UNIVERZITET U BEOGRADU

FAKULTET ORGANIZACIONIH NAUKA

Dragan D. Mladenović

MULTIDISCIPLINARNI ASPEKTI SAJBER RATOVANJA

doktorska disertacija

Beograd, 2016

UNIVERSITY OF BELGRADE

FACULTY OF ORGANIZATIONAL SCIENCES

Dragan D. Mladenović

MULTIDISCIPLINARY ASPECTS OF CYBER WARFARE

Doctoral Dissertation

Belgrade, 2016

Mentor:

dr Mirjana Drakulić, redovni profesor,
Univerzitet u Beogradu - Fakultet organizacionih nauka

Članovi komisije:

dr Dejan Simić, redovni profesor,
Univerzitet u Beogradu - Fakultet organizacionih nauka

dr Slobodan Miladinović, redovni profesor,
Univerzitet u Beogradu - Fakultet organizacionih nauka

dr Branko Kovačević, redovni profesor,
Univerzitet u Beogradu – Elektrotehnički fakultet

dr Danko Jovanović, vanredni profesor,
Univerzitet odbrane – Vojna akademija

Datum odbrane:_____

Zahvalnost i posveta

Ljudi su bića smisla i želje za znanjem. Nauka je put ljudi ka znanju koji traje i ne završava se. Taj put su prešli mnogi, ali ga niko nije okončao. Cilj istraživača nije u dostizanju znanja, jer se ono ne može dostići, već da učini novi korak napred. Od njegove želje i mnogih okolnosti zavisi koliki će taj korak biti. Dostignuto znanje je sadašnjost, prošlost i budućnost. Zato, u skldu sa Bejkonovim rečima, knjige trebaju da prate nauku, a ne nauka knjige.

Moć stvaranja i privlačenja je jača od moći razaranja i prisiljavanja. Stoga odbrana društva ne počiva na fizičkoj snazi, koja je posledica, ne izvor, već u obrazovanju mladih. Porodica i društvo koje propuste da nauče i osposobe svoje mlade da cene znanje, pravdu, rad i svetlost, ne mogu opstati.

Pisana dela su trag prošlosti i odraz stečenog znanja, ali su i iskra budućih ideja i otkrića. Pozivam čitaoca ovog rada, da pročita iskazane misli i ideje, i analizira predstavljene rezultate istraživanja, uz želju da mu oni podstaknu nove ideje o putu i načinu daljeg istrživanja, čiji će rezulatati onda produžiti život ovde napisanih reči. Jednog dana, kada sadašnje znanje, metode i tehnologije budu samo prošlost i uspomena na današnje ljude, vreme i događaje, novo znanje će i dalje biti jednako potrebno i važno. Stoga, znanje, kao i ljubav, unosi nemir i smisao u okean ništavila i praznine, iskru u beskonačni mrak, budi nadu i predstavlja vrednost koja zauvek traje.

Posvećujem ovu disertaciju svom sinu Danilu, koji je moj život i radost, nada i sutrašnjost; svom ocu Danilu, koji me je naučio da poštujem znanje, pravdu i poštenje; svojoj majci Ljubici, koja mi je pružila život, svu ljubav sveta i naučila me veri u pobedu dobrog, upornosti i istrajnosti; i konačno, mojoj voljenoj supruzi Mariji, s kojom delim sve i čija podrška i pomoć su mi omogućili da završim ovaj rad.

Posebno se zahvaljujem mentoru, prof. dr Mirjani Drakulić, na pruženom stručnom znanju, naučnom metodološkom pristupu, posvećenosti mom obrazovanju i razvoju, iskustvu i ljudskom razumevanju kada mi je ono bilo potrebno.

Zahvaljujem se svim autorima čije naučne ideje i otkrića su me dovele do ovog rada i rezultata.

Konačno, izvinjavam se svim dragim ljudima za koje nisam imao dovoljno vremena u prethodnim godinama zbog istraživanja i rada na disertaciji.

MULTIDISCIPLINARNI ASPEKTI SAJBER RATOVANJA

Sajber ratovanje je ratovanje u sajber prostoru, zasnovano na primeni informaciono-komunikacionih tehnologija. Ono predstavlja specifičan oblik međunarodnih sukoba, koji se od tradicionalnih formi ratovanja razlikuje po sredstvima, metodama i učesnicima. Sajber ratovanje se primenjuje nezavisno od perioda rata i mira. Po tehnikama, metodi i procesu napada, ono se tehnološki značajno ne razlikuje od kriminalnih, špijunskih ili terorističkih aktivnosti.

Potencijal ovog, tehnološki zasnovanog oblika sukoba, raste sa zastupljenošću i uticajem informacionih tehnologija na nacionalnom i globalnom nivou. Međunarodna praksa sukoba u sajber prostoru je stvarna i dinamična. Države izdvajaju rastuća budžetska sredstva za vođenje sukoba u sajber prostoru, razvijaju kapacitete i organizacione strukture za preduzimanje operacija u sajber prostoru i usvajaju doktrine i strategije njihove primene i razvoja. Pojedine države su proglasile sajber prostor petim područjem izvođenja vojnih dejstava, ravnopravan sa kopnom, morem, vazduhom i svemirom.

Međutim, međunarodna zajednica ima prirodnu potrebu da međunarodnopravno reguliše sve sukobe, uključujući i sajber ratovanje. Prirodan put da se to učini je primenom postojećeg prava oružanih sukoba i analogije sa odgovarajućim situacijama oružanih sukoba u fizičkom prostoru. Uprkos kratkom periodu razvoja doktrina, metoda i sredstava za vođenje operacija u sajber prostoru, savremena naučna i stručna literatura je bogata radovima koji se bave mogućim načinima primene pomenute analogije u svrhu regulisanja sajber ratovanja. Posebno mesto u toj literaturi ima primena prava na osnovu efekata sajber napada. Taj pristup je prihvatila većina međunarodnih pravnih stručnjaka, uključujući i autore Talinskog priručnika za sajber ratovanje. Uprkos ovakvom teorijskom pristupu, situacije i posledice izvođenja sajber napada na međunarodnom nivou ostaju nerešene i neregulisane u praktičnom pogledu. U praksi države izvode operacije u sajber prostoru, koristeći okolnost da je napade teško otkriti dok se ne manifestuju njihove očigledne posledice; da je najčešće nemoguće izvršiti identifikaciju i atribuciju napadača, odnosno praktično utvrditi odgovornost neke države za preduzeti napad i njegove posledice u skladu sa pravilima, normama i principima Međunarodnog prava oružanih sukoba.

Imajući u vidu značaj sajber sukoba i ratovanja u savremenim međunarodnim odnosima, i očekivani rast njihovog značaja u skladu sa budućim razvojem informacionih tehnologija, kao i nemogućnost praktičnog regulisanja situacija primenom tradicionalnog prava oružanih sukoba, predmet istraživanja ove disertacije je međunarodnopravna regulacija sukoba u sajber prostoru. Cilj istraživanja je utvrđivanje prirode sajber ratovanja i sukoba u sajber prostoru, radi predlaganja načina njegovog budućeg regulisanja. Taj cilj je dostizan tokom istraživanja kroz analizu pretnji od sukoba u sajber prostoru; njegovih najvažnijih specifičnosti, prirode, vrsta i sadržaja; procenu primenljivosti tradicionalnog prava na nove situacije sukoba u sajber prostoru, i izgradnju osnove za buduća teorijska i praktična istraživanja u oblasti sukoba u sajber prostoru.

Imajući u vidu ograničenja koja proističu iz tehnološke prirode informaciono-komunikacionih tehnologija i sajber prostora, i brzu i dinamičnu primenu tih tehnologija u svrhu vođenja sukoba između država u sajber prostoru, polazna hipoteza u toku istraživanja je bila da ne postoji teorijska osnova za dugoročno predviđanje i samim tim razumevanje prirode sajber ratovanja, niti za njegovo međunarodnopravno regulisanje. S obzirom na promenljivu prirodu sajber ratovanja i sukoba, i na potrebu istovremene i kompleksne analize predmeta istraživanja u kontekstu više raznorodnih naučnih disciplina, poput računarskih, pravnih, vojnih i sociooloških nauka, kao i dosadašnje vojne teorije i prakse i prakse informacione bezbednosti, prihvaćen je multidisciplinarni i parcijalno interdisciplinarni pristup istraživanju.

U cilju pružanja naučnog objašnjenja ključnih kategorija, fenomena i pojmova od značaja za istraživanje, poput sajber prostora, sajber napada, sajber oružja, sajber ratovanja i sukoba u sajber prostoru, izvršena je sveobuhvatna analiza i sistematizacija dosadašnjih znanja, prakse i iskustava iz oblasti sajber sukoba i ratovanja. Cilj tog postupka je bila sinteza navedenih ključnih pojmova od značaja za razumevanje prirode sajber ratovanja i njegovog međunarodnopravnog regulisanja.

Rezultati istraživanja su pokazali da je sajber ratovanje tehnološki zavisan oblik sukoba koji se odvija u sajber prostoru i koji se konceptualno razlikuje od svih tradicionalnih formi sukoba u fizičkom okruženju. Ključni elementi sukoba u sajber prostoru, poput sredstava sukoba (oružja), učesnika i metoda ratovanja se po svojoj prirodi značajno razlikuju od situacija tokom tradicionalnih oružanih sukoba. Ključni problemi

međunarodnopravne regulacije sajber ratovanja je česta nemogućnost otkrivanja sajber napada, identifikacije i atribucije napadača i utvrđivanja odgovornosti država za napad. Ovi problemi imaju poreklo u tehnološkoj prirodi i stoga se ne mogu efikasno rešiti isključivim pravnim regulisanjem, bez primene odgovarajućih tehnoloških rešenja. U nekim područjima, poput izvođenja sajber napada sa direktnim učešćem ljudi van javnih i zatvorenih računarskih informacionih mreža, ključne aktivnosti za primenu prava se ne mogu praktično ostvariti.

U radu je izvršena sveobuhvatna analiza velikog broja relevantnih izvora pojmova, definicija i koncepata na osnovu kojih su utvrđene ključne karakteristike sajber prostora i vođenja sukoba u njemu. Po rezultatima analize, sajber prostor je okruženje u kome se stvaraju, čuvaju, obrađuju, razmenjuju i uništavaju podaci i informacije primenom računarskih sistema za koje je karakteristično postojanje ili mogućnost uspostavljanja umreženosti sistema, procesa i ljudi na nivou podataka.

Ova disertacija se posebno bavi problemima primene tradicionalnog Međunarodnog prava oružanih sukoba na sukobe u sajber prostoru, vrši analizu ključnih pojmova, koncepata i fenomena od značaja za sajber ratovanje između država i nudi predlog kao posledicu utvrđenih rezultata istraživanja koji se odnosi na buduće ponašanje država u cilju izgradnje sposobnosti za sajber odbranu od napada u sajber prostoru i međunarodno pravnu akciju na budućem regulisanju sukoba u sajber prostoru.

Za razliku od tradicionalnih sukoba u fizičkom okruženju koji predstavljaju organizovanu primenu ekskluzivnog i specifičnog naoružanja, odnosno sredstava za vođenje sukoba, sajber ratovanje je proces, a ne upotreba „sajber oružja“. Taj proces predstavlja namerno narušavanje informacione bezbednosti napadnutog sistema u sajber prostoru u vojne svrhe. Načelno, svaki proces sajber napada se sastoji od otkrivanja ranjivosti ciljanog sistema, utvrđivanja njegove prirode, iskorišćavanje ranjivosti radi neovlašćenog pristupanja sistemu i izvršenje dejstva napada. Ovaj proces primarno zavisi od tehnologije računarskih sistema i informacione bezbednosti, a ne od vojne veštine i prakse. Pa ipak, bez obzira što ga ne moraju izvoditi vojnici, što u postupku sajber napada nema primene specifičnog, vojnog naoružanja i što se može izvoditi u miru kao i tokom rata, u okviru ili van konteksta političkog sukoba, prikriveno, odloženo i decentralizovano, sajber

napadi imaju potencijal da ostvare značajne vojne efekte i ciljeve na taktičkom, operativnom i strategijskom nivou.

Imajući u vidu specifičnu, tehnološki zasnovanu prirodu sajber ratovanja, ono se treba shvatiti u najširem konceptu, ne kao sukob u stanju rata ili vojna aktivnosti u toku vojnih operacija u fizičkom okruženju, već kao veliki broj mogućih aktivnosti koje se odvijaju na fizičkom, logičkom i kognitivnom nivou sajber prostora. Logički nivo sajber prostora, zasnovan na logičko-matematičkim pravilima i instrukcijama je osnova sajber prostora, koja povezuje njegov uticaj na živi i neživi svet u fizičkom okruženju preko podataka, računarskih sistema koji ih obrađuju i značenja informacija koje ti podaci nose. Široka primena informaciono-komunikacionih tehnologija u sajber prostoru u svrhu vođenja sukoba na međunarodnom nivou je posledica njihove velike zastupljenosti u svim segmentima ljudskog života i rada. Pri tome se iste tehnologije i principi njihovog rada primenjuju u mirnodopskom i vojnom okruženju. Ta činjenica, a ne obim i sadržaj efekata sukoba u sajber prostoru, čini ovu vrstu sukoba i ratovanja perspektivnim u budućnosti i daje ima sposobnost brzog razvoja i menjanja forme, primene i posledica.

Cilj ove disertacije je sadržan u identifikaciji prirode sajber sukoba i ratovanja, njihovih izvora i odnosa između vojne, međunarodnopravne, socijalne i informaciono-bezbednosne prakse. Iz tog cilja proističe i praktičan doprinos disertacije, koji se ogleda u zaključcima njenog istraživanja. Jedan od zaključaka disertacije je da sajber ratovanje ima široku budućnost primene, koja primarno zavisi od razvoja informaciono-komunikacionih tehnologija, a ne od sposobnosti međunarodne zajednice da na tradicionalan način međunarodnopravno reguliše sukobe u sajber prostoru. Ostali zaključci se odnosi na pravce izgradnje kapaciteta za sajber ratovanje na nacionalnom nivou, kao i na jedini moguć pravac praktične regulacije sajber sukoba na međunarodnom nivou. U disertaciji je ukazano da osnove za izgradnju nacionalnog sistema sajber odbrane ne leže u posedovanju i primeni tehničkih sistema za izvođenje operacija u sajber prostoru, već u upravljanju specifičnim znanjem u oblasti primenjene informacione bezbednosti u sajber prostoru na nacionalnom nivou. Takođe, utvrđeno je da međunarodnopravna regulacija sajber ratovanja nije moguća isključivom primenom tradicionalnog Međunarodnog prava oružanih sukoba, pa čak ni izgradnjom novih pravnih sistema, ukoliko su oni zasnovani samo na tradicionalnim pravnim rešenjima, bez

istovremenog uključivanja i primene tehnoloških rešenja na osnovnom nivou savremenih informaciono-komunikacionih tehnologija.

Zaključak analize je da će razvoj novih tehnologija vrlo brzo doneti razvoj novih sposobnosti za sajber ratovanje. U radu je zaključeno da je jedini način praktične regulacije sajber ratovanja na međunarodnom nivou, i ujedno ograničavanja njegovih negativnih posledica, sadržan u mogućoj bilateralnoj i multilateralnoj saradnji zainteresovanih strana u međunarodnoj zajednici. Sukobi u sajber prostoru se ne izvode samo tokom stanja rata, i ne samo primenom vojnih ofanzivnih operacija, pa se i rešenje za njihovu regulaciju ne može naći isključivo u Međunarodnom pravu oružanih sukoba, već mora biti sveobuhvatan pristup koji sadrži brojne mogućnosti i aktivnosti vojnog i mirnodopskog ispoljavanja nacionalne moći. Rešenje za ograničavanje sajber sukoba je u kombinovanoj primeni diplomatskih, političkih, ekonomskih, vojnih, pravnih informacionih i drugih napora i aktivnosti.

Ključne reči: sajber prostor, sajber ratovanje, sajber napadi, sajber oružje, sukob u sajber prostoru, međunarodno pravo oružanih sukoba, međunarodno pravo

Naučna oblast: multidisciplinarne, interdisciplinarne, računarske i pravne studije

Uža naučna oblast: pravne i računarske studije

UDK broj: 004.738.5:343

MULTIDISCIPLINARY ASPECTS OF CYBER WARFARE

Cyber warfare is warfare in cyberspace, based on application of information communication technologies. It represents a specific form of international conflict, differing from the traditional warfare forms in means, methods and participants. Cyber warfare is applied independently from war and peace periods. It is not significantly technologically different in its techniques, methods and attack processes from criminal, espionage or terrorist activities.

The potential of this, technologically based conflict form, grows with prevalence and influence of information technologies at the national and global level. International practice of cyber space conflict is real and dynamic. States allocate growing budget funds for conducting cyberspace conflict, they develop capacities and organizational structures for operations in cyberspace and adopt doctrines and strategies for their application and development. Some states declared cyberspace the fifth domain of military activities, equal with land, sea, air, and space.

However, international community has got a natural tendency to regulate all conflicts, including cyber warfare. The natural way to do this is through application of the existing law of armed conflict and analogy with appropriate armed conflict situations in physical space. Despite brief period for development of doctrines, methods and means for cyberspace operations, modern scientific and professional literature is rich in papers dealing with possible ways of application of the said analogy for the purpose of regulation of cyber warfare. Special place in this literature belongs to application of law based on cyber attack effects. This approach was accepted by most international legal experts, including authors of Tallinn Manual for cyber warfare. Despite such a theoretical approach, situations and consequences of conducting cyber attacks at international level remain unresolved and unregulated in practice. States execute operations in cyberspace, using the circumstance that attacks are difficult to discover until their obvious consequences are manifested; that most often it is impossible to perform identification and attribution of attackers, i.e. to practically determine responsibility of a state for an attack and its consequences in accordance with the rules, norms and principles of International law of armed conflict.

Having in mind the significance of cyber conflict and warfare in modern international relations and expected growth of their importance in line with future development of information technologies, as well as the inability of practical regulation of situations through application of traditional armed conflict law, subject matter of this dissertation is international legal regulation of conflict in cyberspace. The research objective is to determine the nature of cyber warfare and cyberspace conflict in order to propose a way to regulate it in the future. The objective was achieved during the research through analysis of conflict threats; its dominant specifics, nature, types and content; estimate of applicability of traditional law to new conflict situations in cyberspace, and building of foundation for future theoretical and practical research in the field of cyberspace conflict.

Having in mind limitations stemming from technological nature of information-communication technologies and cyberspace and a fast and dynamic application of such technologies for the purpose of leading conflicts between states in cyberspace, the beginning hypothesis during research was that there was no theoretic basis for long-term prediction and consequently understanding of cyber warfare nature, as well as for its international legal regulation. Given the changeable nature of cyber warfare and conflict and the need of simultaneous and complex analyses of the research matter in the context of various scientific disciplines, such as computer, legal, military and sociological sciences, as well as the existing military theory and information security practice, a multidisciplinary and partially interdisciplinary research approach was adopted.

For the purpose of providing a scientific explanation of key categories, phenomena and concepts significant for research, such as cyberspace, cyber attacks, cyber weapons, cyber warfare and cyberspace conflict, a comprehensive analysis and systematization of the existing knowledge, practice and experiences in the cyber conflict and warfare domain was performed. The goal of this procedure was synthesis of the key concepts significant for understanding the nature of cyber warfare and its international legal regulation.

Research results show that cyber warfare is a technologically dependent form of conflict taking place in cyberspace which is conceptually different from all traditional forms of conflict in the physical environment. Key elements of cyberspace conflict, such as conflict means (weapons), participants and methods of warfare are in their nature significantly different from situations during traditional armed conflict. Key problems of

international legal regulation of cyber warfare is frequent inability to discover cyber attacks, to perform attacker identification and attribution and determining state responsibility for attacks. These problems originate in technological nature and therefore, cannot be efficiently resolved by exclusive legal regulation, without application of suitable technological solutions. In some domains, such as performing cyber attacks with direct participation of people outside of public and closed computer information networks, key activities for law application cannot be practically achieved.

The dissertation offers a comprehensive analysis of a large number of relevant sources of notions, definitions and concepts, based on which key characteristics of cyberspace and conflicts within cyberspace are determined. According to the analysis results, cyberspace is an environment where data and information is created, kept, processed, exchanged and destroyed by application of computer systems characterized by existence or possibility of establishing systems, processes and people network at the level of data.

This dissertation especially covers the problems of application of traditional International Law of Armed Conflict to conflicts in cyberspace, analyses key notions, concepts and phenomena important for cyber warfare between states and offers a proposal as a consequence of determined research results relating to future behavior of states for the purpose of building capabilities for cyber defense from cyberspace attacks and international legal action in future regulation of cyberspace conflicts.

Unlike traditional conflicts in physical environment representing organized application of exclusive and specific armament, i.e. means for conduct of conflict, cyber warfare is a process, not use of „cyber weapons“. This process represents intentional violation of information security of an attacked system in cyberspace for the military purposes. In general, every cyber attack process consists of discovery of targeted system's vulnerability, determining its nature, utilization of vulnerability for unauthorized access to the system and execution of attack. This process primarily depends on computer systems technology and information security, not military skill and practice. However, regardless of the fact that soldiers need not conduct the attack, that there is no application of specific, military armament, and that it can be conducted both during peace and war, or within or outside of a political conflict context, covertly, postponed and decentralized,

cyber attacks have the potential to achieve significant military effects and goals at tactical, operational and strategic level.

Having in mind the specific, technologically based nature of cyber warfare, it should be understood in the widest context, not as a conflict in the state of war or a military activity during military operations in the physical environment, but as a large number of possible activities taking place at the physical, logical and cognitive level of cyberspace. Logical level of cyberspace, based on logical-mathematical rules and instructions is the basis of cyberspace, connecting its influence on the living and non-living world in the physical environment through data, computer systems processing them and meaning of information carried in those data. Wide application of information-communication technologies in cyberspace for the purpose of leading conflicts at international level is a consequence of their increasing incidence in all segments of human life and work. Whereas the same technologies and principles of their work are applied both in peace time and military environment. This fact, not the scope and content of cyberspace conflict effects, promises development of this type of conflict and warfare in the future and gives them capability for fast development and changing of form, use and consequences.

The goal of this dissertation is in identification of cyber conflict and warfare nature, their sources and relations between military, international legal, social and information security practice. This goal provides the practical contribution of the dissertation, reflected in conclusions of its research. One of the conclusions is that cyber warfare application has a future, primarily depending on development of information communication technologies, not the capability of international community to legally regulate cyberspace conflicts in a traditional way. Other conclusions relate to ways of cyber warfare capacity building at national level, as well as to the only possible direction for cyber conflict practical regulation at international level. Dissertation points out that the bases for building a national cyber defense system are not in possessing and application of technical systems for conducting operations in cyberspace, but in managing specific knowledge in the field of applied information security in cyberspace at national level. Also, it is determined that international legal regulation of cyber warfare is not possible through exclusive application of traditional International Law of Armed Conflict, not even through building of new legal; systems, if they are based only on traditional legal solutions, without

simultaneous inclusion and application of technological solutions on the basic level of modern information communication technologies.

Conclusion of analysis is that development of new technologies will quickly bring about development of new cyber warfare capabilities. The dissertation offers a conclusion that the only way of practical cyber warfare regulation at international level, and at the same time limitation of its negative consequences, is contained in the possible bilateral and multilateral collaboration of interested parties in international community. Conflicts in cyberspace do not take place only during state of war, and not only through application of military offensive operations, so the solution for their regulation cannot be found exclusively in International Law of Armed Conflict, but be a part of a comprehensive approach encompassing many possibilities and activities of military and peacetime exercise of national power. Solution for limiting cyber conflicts lies in the combined application of diplomatic, political, economic, military, legal, information and other efforts and activities.

Key words: cyberspace, cyber warfare, cyber attack, cyber weapon, cyberspace conflict, LOAC, international law

Scientific field: Multidisciplinary, Interdisciplinary, Computer and Law studies

Narrow scientific field: Law and Computer studies

UDC number: 004.738.5:343

SADRŽAJ

SPISAK SKRAĆENICA

AI	Artificial Intelligence
AKUF	Arbeitsgemeinschaft Kriegsursachenforschung
ARPA	Advanced Research projects Agency
ATIS	Alijanse za rešenja iz oblasti telekomunikacionih industrija
AVACS	Automatic Verification And Analysis of Complex Systems
BGP	Border Gateway Protocol
BSI	Federal Office for Information Security
CCDCOE	Cooperative Cyber Defence Centre of Excellence
CCIS	Center for Cyber and Information Security
CENTRIX	Combined Enterprise Regional Information eXchange System
CFBLNet	Combined Federated Battle Laboratories Network
CHAMP	Counter-electronics High-powered Microwave Advanced Missile Project
CIA	Central Intelligence Agency
CNA	Computer Network Attack
CPU	Central Processing Unit (centralna procesorska jedinica)
CSIS	Center for Strategic and International Studies
DARPA	Defense Advanced Research Project Agency
DDoS	Distributed Denial of Service Attack
DHS	Department of Homeland Security
DI2E	Defense Intelligence Information Enterprise
DIA	Defense Intelligence Agency
DNK	Dezoksiribonukleinska kiselina
DNS	Domain Name System
DoS	Denial-of-service

ENISA	Agencija Evropske Unije za mrežnu i informacioni bezbednost
ENISA	European Union Agency for Network and Information Security
EWI	EastWest Institute
FISMA	Federal Information Security Management Act of 2002
GCHQ	Government Communications Headquarters
GCTF	Global Counter-Terrorism Force
GFP	Global Fire Power
GGE	Group of Governmental Experts
GIG	Global Information Grid
GII	Global Innovation Index
GRIFFIN	Globally Reaching Interconnected Fully Functional Information Network
HDI	Human Development Index
ICJ	International Court of Justice
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IKT	Informaciono-komunikacione tehnologije
IoT	Internet of Things
IP	Internet Protocol
ISIL	Islamic State of Iraq and the Levant
ISO	International Organization for Standardization
IT	Informacione tehnologije
ITC	International Telecommunication Convention
ITIL	Information Technology Infrastructure Library
ITU	International Telecommunications Union
JIE	Joint Information Environment
LTE	Long-Term Evolution

MIT	Massachusetts Institute of Technology
MLAT	Mutual Legal Assistance Treaty
NATO	The North Atlantic Treaty Organization
New START	Treaty Between The United States of America and The Russian Federation on Measures for the Further Reduction and Limitation of Strategic Offensive Arms
NFC	Near Field Communication
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSANet	National Security Agency Network
NSL	oN-Line System
OEBS	Organizacija za evropsku bezbednosti saradnju
OECD	Organisation for Economic Cooperation and Development
OTI	Open Technology Institute
PrEP	Propagation, exploit, payload
PRIO	Peace Research Institute Oslo
QR Code	Quick Response Code
RFID	Radio Frequency Identification
SAD	Sjedinjene Američke Države
SALT I	Treaty Between The United States of America and The Union of Soviet Socialist Republics on the Limitation of Strategic Offensive Arms
SALT II	Treaty Between The United States of America and The Union of Soviet Socialist Republics on the Limitation of Strategic Offensive Arms, Together With Agreed Statements and Common Understandings Regarding the Treaty
SCI	Strategic Computing Initiative
SOFA	Status of Forces Agreements
SRJ	Savezna Republika Jugoslavija

START I	Treaty Between The United States of America and The Union of Soviet Socialist Republics on the Reduction and Limitation of Strategic Offensive Arms
ŠOS	Šangajska organizacija za saradnju
TAO	Tailored Access Operations
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
UCDP	The Uppsala Conflict Data Program
UKUSA	United Kingdom – United States of America Agreement
UNCLOS	The United Nations Convention on the Law of the Sea
UNDP	United Nations Development Programme
UNIDIR	United Nations Institute for Disarmament Research
UNODA	UN Office for Disarmament Affairs
USCYBERCOM	United States Cyber Command
USSTRATCOM	United States Strategic Command
VoIP	Voice over IP

SPISAK ILUSTRACIJA

SPISAK TABELA

1. UVOD

Sajber ratovanje je nov i kompleksan fenomen, koji se odnosi na upotrebu informacionih tehnologija za vođenje sukoba. On podrazumeva primenu novog koncepta sukoba, koji koristi drugačija sredstva ratovanja i koji se primenjuje bez obzira da li je stanje mira ili rata. Njegovi učesnici ne moraju biti uniformisani vojnici. Za njega nisu usvojena nova pravila ratovanja, a postojeća pravila su teško primenjiva u praksi.

Sukobi prate razvoj ljudskog društva. Oni su faktor na koji utiče ljudska priroda i koji stvara ljudsku prirodu. Ratovi su najintenzivniji oblik društvenih sukoba. Sukobima i ratovima ljudi brane sopstvene društvene zajednice, ali i ostvaruju zajedničke interese kroz nasilje prema drugim društvenim grupama. O uzrocima sukoba među ljudima postoje različite teorije i mišljenja. Istorija nam, na žalost, pokazuje da se celokupna epoha ljudske vrste može istovremeno posmatrati i kao istorija razvoja novih znanja i veština, i kao istorija sukoba.[1] Svaki sukob predstavlja isti proces: jedna društvena grupa koristi instrumente moći, primenjuje silu ili preti silom drugoj društvenoj grupi, prisiljavajući je da učini ono, što ta druga grupa ne želi. Ratovanje predstavlja sukob interesa koji se ostvaruje primenom instrumenata moći, primarno oružanom borbom, koja se razvija paralelno sa razvojem tehnologije.

Tehnologija predstavlja veštinu primene znanja. Najnaprednije tehnologije se po pravilu prvo koriste u svrhu odbrane nacije i ostvarivanje nacionalnih interesa. Tokom istorije čovečanstva metode, tehnike i sredstva ratovanja evoluiraju zajedno sa ljudima i postaju efikasnije. Međutim, evoluira i društvena svest, etika i moral, koje ograničavaju primenu tehnologije u svrhu sukoba. Metode i tehnike ratovanja karakteristične za srednji vek u savremenom društvu nisu prihvatljive. Sukobi sami po sebi nisu cilj, niti sredstvo za ostvarivanja interesa, već metoda kojim se ti interesi ostvaruju, koji i sam evoluira, postaje efikasniji, tehnološki savremeniji i etički prihvatljiviji.

Po završetku velikih sukoba, u međunarodnoj zajednici se po pravilu javlja izražena svest i potreba da se budući sukobi ograniče po negativnim posledicama i da postanu humaniji.

[1] Doyne Dawson, "The Origins of War: Biological and Anthropological Theories," *History and Theory* 35, no. 1 (February 1996): 1-28.

Jedini praktičan i ujedno formalan način da se to postigne, jeste primena prava kojim se dostignute civilizacijske norme, principi i osećaji pravičnosti i pravednosti primenjuju na ljudsko ponašanje. Međutim, pravo predstavlja prihvatljiv prosek zajedničkih stavova elemenata zajednice. Ono ima i ograničenja. Najveće od svih je to, što zabranjuje i kažnjava samo one aktivnosti koje spadaju u skup formalno zabranjenih, dok ostale dozvoljava. Navedena okolnost predstavlja praktičan problem u primeni novih tehnologija vođenja sukoba, koje se upotrebljavaju za dobrobit pojedinaca i društva, pri čemu prethodno nisu pravno regulisane, ali isto tako mogu biti i zloupotrebljene na štetu društva.

Regulisanje svih novih područja, tehnika i metoda ratovanja do sada je zahtevalo primenu analogije u odnosu na postojeće pravo, odnosno stvaranje novih propisa. Međutim, u sajber sukobima postoje tehnološke specifičnosti i ograničenja koja značajno otežavaju praktičnu primenu pozitivnog prava na odnose nasilja u sajber prostoru u oba navedena pravca. Ta ograničenja se ogledaju u nemogućnosti pravovremene i potpune detekcije sajber napada, nemogućnosti atribucije napadača i nemogućnosti određivanja državne odgovornosti za napad. Pored toga, informaciono-komunikacione tehnologije uvode potpuno novo okruženje u područje sukoba i njegove regulacije – sajber prostor.

Uticaj informaciono-komunikacionih tehnologija i sajber prostora na celokupno društvo je istovremeno revolucionaran i disruptivan. Revolucionaran je po kvalitativnom uticaju koji ove tehnologije ostvaruju na čovečanstvo. Ipak, osnovni principi i arhitektura računara na čijim osnovama su izgrađeni i savremeni računari su kreirani još tokom Drugog svetskog rata. Prva poruka Internetom je poslata 1969. godine, što znači da je savremeni sajber prostor u svojoj petoj deceniji postojanja. Do značajnog unapređenja naučnih principa i tehnologije doveo je uporan i istrajan rad mnoštva inženjera i naučnika. Savremeni ljudi svoj život teško mogu zamisliti bez svakodnevne upotrebe informaciono-komunikacionih tehnologija. Njihova očekivanja od budućih tehnologija su još veća. Retke su oblasti ljudskog života u kojima ove tehnologije ne pružaju presudan kvalitativni i kvantitativni doprinos. Tako je i sa vođenjem sukoba. Sposobnost sajber napada da ostvare posledice sve ozbiljnije prirode raste sa rastom značaja tehnologija.

Sajber ratovanje ima specifičnu prirodu, formu i primenu. Sajber ratovanje menja pristup sukobima i ratovanju, ne samo u kvantitativnom, već pre svega u kvalitativnom pogledu.

Ono je skoncentrisano oko i u vezi primene informaciono-komunikacionih tehnologija. Dešava se u sajber prostoru, pa ipak, ima posledice i na fizičko okruženje, ljude, tehničke sistema, kao i na medijsko, psihološko i društveno područje. Način na koji se ostvaruje dejstvo sajber napada se menja u skladu sa brzim razvojem i sposobnostima informaciono-komunikacionih tehnologija. Retko koja druga oblast ljudske prakse i znanja se razvija brže od oblasti računarstva i informacionih tehnologija.

Kao novi predmet međunarodnog prava, regulisanje sukoba u sajber prostoru prate mnogobrojni problemi. Oni proističu iz prirode sajber napada i sajber prostora. Njihova specifičnost dovodi do dileme, da li u cilju praktičnih rezultata, sajber sukobe regulisati primenom analogije sa tradicionalnim pravom, uz mnogobrojne generalizacije i prilagođavanja, ili stvoriti potpuno nov pravni sistem regulacije, koji bi više odgovarao tehnologiji sajber sukoba. Međutim, tehnološki dometi i sposobnosti nisu statični. Tehnologija se menja i razvija, tako da postoji realna opasnost da nova pravila međunarodnopravne regulacije sukoba u sajber prostoru ubrzo i sama postanu zastarela. Pored toga, način na koji nastaje međunarodno pravo onemogućava takav pristup.

Primena umreženih informaciono-komunikacionih tehnologija u okruženju sajber prostora zahteva razumevanje ključnih elemenata na kojima počiva tradicionalno pravo. Mala je verovatnoća da će sukobi u sajber prostoru prestati da postoje i prestati da budu relevantni. Naprotiv, svi trendovi razvoja informaciono-komunikacionih tehnologija pokazuju da će njegov kapacitet i značaj u međunarodnim odnosima rasti u budućnosti, a da će njihove savremene sposobnosti biti višestruko prevaziđene. Primena jednostavne, linearne analogije od početka doživljava poteškoće u području analize i razumevanja granica i nadležnosti državnih suvereniteta, procesa primene sile nad protivnikom, utvrđivanja identiteta i odgovornosti za učinjena dela, odsustva klasičnog naoružanja kojim se napad izvodi, proceni prirode ostvarenih efekata dejstva i sličnih. Jedini moguć pristup rešavanju tih i drugih problema se može naći u temeljnoj analizi prirode osnovnih kategorija i fenomena od značaja za istraživanje, u primeni te prirode u analizi savremenih sukoba i ratovanja i tek onda, u sagledavanju mogućeg rešenja.

Ova disertacija obrađuje probleme primene tradicionalnog prava na sukobe u sajber prostoru i daje predlog praktičnih aktivnosti za države u njihovim pokušajima da regulišu sajber sukobe.

Međunarodno pravo oružanih sukoba[2] je stvoreno u cilju regulisanja tradicionalnih sukoba koji se odvijaju isključivo u fizičkom okruženju. Posledica toga je da tradicionalno pravo često nije u praksi primenljivo na situacije sukoba koje se vode u potpuno drugačijem okruženju sajber prostora. Zbog toga, tumačenje pravila, principa i normi međunarodnog prava nekada se mora prilagodilo meri sajber sukoba. To dovodi do situacije u kojoj primena istih, objektivnih pravila može dovesti do različitih ishoda u zavisnosti od okruženja i svojstva objekta.

Po teoriji relativnosti, vreme u fizičkom svetu je relativno u odnosu na brzinu kojom se objekat kreće, a prostor, zajedno sa dimenzijama, u odnosu na masu objekta. Međutim, relativnost u oblasti prava ugrožava važnost opštih principa na kojima je pravo zasnovano. Različiti događaji kršenja zakona, koji po posledicama predstavljaju isti prekršaj, počinjen sa istom namerom i na isti način, ali u različitim situacijama, primenom prava mora biti tretiran na isti način. Međutim, realnost pokazuje da u slučaju primene informaciono-komunikacionih tehnologija to ne važi uvek. Primena prava u sajber prostoru često više zavisi od situacija koje stvara tehnologija, nego od pravnog sistema. Informacija istovremeno može biti u nadležnosti svih i nijednog suvereniteta. U sajber prostoru je sve više *non liquet* situacija u kojima međunarodno pravo nije primenjivo.

Na primer, tehnološka nejednakost između uključenih aktera stvara razliku u sposobnosti upravljanja informacijama. Mnogi subjekti u međunarodnom okruženju jednostavno nemaju tehnološke sposobnosti da otkriju, razumeju i poseduju informacije o učinjenom prekršaju prava koje su posledica sajber napada. Izreka da „pravo govori svima jednim ustima“[3] u sajber prostoru često ne važi. U sajber prostoru primena prava zavisi od sposobnosti da se ovlada informacijama, detektuju aktivnosti i posledice sajber napada i od sposobnosti razvoja i primene informaciono-komunikacionih tehnologija.

[2] Međunarodno pravo oružanih sukoba je oblast međunarodnog javnog prava koje se odnosi na regulisanje odnosa između međunarodnopravnih subjekata u stanju oružanog sukoba, a naziva se i Međunarodno humanitarno pravo ili Ratno pravo.

Joan Policastri and Sergio D. Stone, "International Humanitarian Law," *American Society of International Law (ASIL) https://www.asil.org/sites/default/files/ERG_International%20Humanitarian%20Law%20(test).pdf* (2013).

[3] Lat. *Lex uno ore omnes alloquitur*

Međutim, temeljni principi i izvori međunarodnog prava su univerzalno isti, bez obzira na okruženje i sredstva vođenja sukoba. Zbog toga je pravu u visokotehnološkom okruženju potrebna podrška u vidu rezultata i metoda iz drugih oblasti ljudskog znanja. Dakle, regulacija sukoba u sajber prostoru zahteva istovremenu primenu znanja i veština iz više različitih oblasti. To su računarske nauke, informatika, kibernetika, elektronika, matematika, logika, pravo, vojne nauke, sociologija, ekonomija, bezbednosti i informaciona bezbednost, psihologija i antropologija, pri čemu spisak uključenih nauka ne treba ograničiti. Sve te discipline, veštine i oblasti znanja, u skladu sa sopstvenim područjima i metodama istraživanja, na drugačiji način vide različite pojmove i elemente sukoba u sajber prostoru. To se odnosi čak i na fundamentalne pojmove i kategorije kao što su „sajber oružje“, „sajber napad“, „sajber borci“, „agresija u sajber prostoru“, „sajber rat“, „sajber ratovanje“, koji mogu imati različito značenje posmatrano sa aspekta različitih naučnih disciplina.

U zamagljenom svetu sajber sukoba između nacija često se dešavaju situacije u kojima su okolnosti i motivi samo naizgled jasni, ali je malo toga materijalno ili forenzički dokazivo u razumno prihvatljivom vremenu, da bi bilo moguće regulisati sukob i sprečiti njegovu eskalaciju. U takvim situacijama nominalne definicije pojmova nastale u dugoj tradiciji regulisanja tradicionalnih sukoba često nisu saglasne sa deskriptivnim i preskriptivnim definicijama nastalim u različitim područjima istraživanja sajber sukoba, nisu relevantne u drugim područjima ili nisu u praksi primenjive na širok skup stvarnih situacija. Posledica toga je da se istraživanje sajber ratovanja, zasnovano na znanju i primeni tradicionalnih metoda jedne naučne discipline ne može efikasno ostvariti zbog problema ontološke, epistemološke, metodološke i metodičke prirode. Rezultat toga je da se, u praktičnom smislu, teško može jednoznačno i precizno i odgovoriti iz ugla jedne specifične discipline na sledeća pitanja:

- Šta je sajber ratovanje, njegov sadržaj i predmet?
- Kako doći do naučne istine u oblasti sukoba u sajber prostoru koja se može potvrditi na naučno prihvatljiv način?
- Koje su to naučne istine u vezi sajber ratovanja koje mogu dovesti do njegove pravno prihvatljive i sprovodljive regulacije?

- Kakve procedure istraživač treba da primenjuje u procesu istraživanja prirode i zakonitosti sajber ratovanja?
- Da li je u postupku istraživanja sajber ratovanja dovoljna primena kvalitativnih metoda istraživanja i da li je istraživanje zasnovano na preovlađujućoj primeni kvantitativnih metoda uopšte relevantno za odabranu oblast istraživanja?

Pored ontološkog, u procesu istraživanja premeta sajber sukoba postoje i epistemološki i metodološki problemi. Epistemološki problem se prvenstveno ogleda u činjenici da je sajber ratovanje veoma tehnološki zavisno i zasnovano. U pogledu razvoja tehnologije ne postoje zakonitosti. Studija Kadtkea i Velsa[4] o izazovima ubrzanja tehnoloških izazova u oblasti bezbednosne politike tvrdi da se sajber prostor i svi aspekti informaciono-komunikacionih tehnologija razvijaju tako brzo, da je buduće sposobnosti aktera u toj oblasti vrlo teško predvideti čak i u kratkoročnom periodu. Pri tome, čak ni postojeća predviđanja nisu zasnovana na naučnoj metodologiji, već su profesionalne pretpostavke zasnovane na iskustvu, kao u slučaju predviđanja trenda unapređenja procesorske moći računarskih informacionih sistema, popularno nazvanog „Murovim zakonom“[5]. Ali, „Murov zakon“ nije naučni zakon, niti je teorija. On čak nije ni naučna hipoteza. Da bi imao karakter hipoteze, inicijalne etape u naučnom metodu otkrivanja sistema znanja, ovaj koncept mora pokazati svoju valjanost, održivost i postojanost u vremenu, a rezultati mu moraju biti zasnovani na naučnom pristupu istraživanju. To „Murov zakon“ nije u stanju da pruži, iako su se njegove pretpostavke pokazale tačnim u periodu od pedeset godina.[6] Bez primene naučne metode u istraživanju, postupak predstavlja projekciju, uočenu konstataciju o karakteru posmatranog fenomena.[7]

Oraničavanje na primenu jedne metode i discipline u pogledu istraživanja sukoba u sajber prostoru ne može da omogući valjane rezultate. Čak i uz primenu objedinjenog, holističkog pristupa koji uključuje istovremenu primenu metoda i rezultata formalnih, društvenih i prirodnih nauka, kao i primenjenih veština i područja znanja, i dalje postoje

[4] James Kadtke and Linton Wells II, *Policy Challenges of Accelerating Technological Change: Security Policy and Strategy Implications of Parallel Scientific Revolutions* (Washington, DC: Center for Technology and National Security Policy, National Defense University, 2003), 23.

[5] Gordon E. Moore, "Cramming More Components onto Integrated Circuits," *Electronics* (April 19, 1965), 114-117.

[6] "The Law That's Not A Law," *IEEE Spectrum* 52, no. 4 (April 2015): 38-57.

[7] "Law That's Not A Law," *IEEE Spectrum* .

brojni problemi različite prirode, koji zahtevaju pažljivu primenu indukcije u postupku istraživanja. Na primer, sajber ratovanje je specifična primena znanja i veština iz oblasti informacione bezbednosti. U stručnoj profesionalnoj zajednici, informaciona bezbednost se, još uvek, smatra praksom. Stoga su i njeni krajnji uvidi samo rezultati „najbolje prakse“, a ne naučna teorija, a pogotovo ne naučni zakon.

1.1. Izbor discipline

Problemi metodološkog pristupa istraživanju sajber sukoba proističu iz mnoštva mogućih pristupa istraživanju. Ograničavanje na jednu metodu istraživanja može:

- pružiti tačne, ali u praksi neprimenjive rezultate [8];
- stvoriti situaciju u kojoj se jedna teorija objašnjava drugom;
- dovesti do preterane generalizacije ili specijalizacije rezultata;
- dovesti do neželjene redukcije karakteristika predmeta i sadržaja istraživanja.

Od mnoštva potencijalno primenjivih naučnih disciplina i veština u postupku istraživanja primene prava na sukobe u sajber prostoru ključni značaj imaju one discipline, koje na najprirodniji način omogućavaju ostvarivanje uvida u karakter sajber sukoba, njegovih elemenata i uzrok nastanka. S obzirom da se radi o pravnom regulisanju primene informacionih tehnologija, to su pre svega, informaciona i sajber bezbednost, javno pravo, Međunarodno pravo oružanih sukoba, vojna teorija i praksa i računarske nauke. Navedene oblasti predstavljaju sistematizovan korpus ljudskog znanja i iskustva u specifičnim oblastima koje se mogu dovesti u vezu sa vođenjem međunarodnih sukoba. Međutim, ni za jednu od navedenih oblasti se ne može eksplicitno tvrditi da poseduje karakter i formu

[8] Ernest Nejgel, *Struktura nauke: problemi logike naučnog objašnjenja* (Beograd, Srbija: Nolit, 1974), 293.

naučne discipline koja se zasniva na primeni univerzalnih naučnih metoda i tehnika istraživanja prirodnih nauka u postupku otkrivanja naučne istine [9, 10, 11, 12].

U sajber sukobima se dešava uticaj na društvene odnose primenom tehnologije u cilju vođenja sukoba zasnovanog na znanju. Zbog kompleksnosti uzročno-posledičnih odnosa u okviru predmeta istraživanja i nemogućnosti preduzimanja egzaktnih i eksperimentalnih naučnih metoda u procesu istraživanja, utvrđivanje zakonitosti u području istraživanja i sposobnost predviđanja zasnovanog na utvrđenim zakonima gotovo da nisu moguće. Između navedenih disciplina postoji razlika u tradiciji primene specifičnih pristupa istraživanju, kao i u iskustvu stečenom na osnovu dosadašnjeg istraživanja. Vojna (ratna) veština je stara koliko i čovečanstvo. Ona predstavlja primenu iskustva i znanja radi postizanja vojnog uspeha. Ne postoji formula niti naučni zakon po kome se može ostvariti vojnička pobeda u ratu. Moderno Međunarodno pravo oružanih sukoba primenjuje pravne principe koji su nastali još u vreme Rimskog carstva i rimskog prava.[13] S druge strane, praksa sajber bezbednosti postoji u kratkom periodu od svega par decenija.[14] Međutim, navedene razlike ne znače da područja istraživanja ovih oblasti nisu područja znanja, niti da se naučna metoda istraživanja ne može primeniti u postupku regulisanju sukoba u sajber prostoru.[15] Ipak, nauku ne čini samo njen predmet, već i način istraživanja. Konačno, znanje je uvek potrebno tamo gde ga nema.

Čak ni nedostatak naučne zasnovanosti u oblasti primenjene sajber bezbednosti ne znači da praktičan napredak u njegovoj praksi, zasnovan na znanju, ne može biti učinjen.[16] To

[9] Fred B. Schneider, „Blueprint for a Science of Cybersecurity," *The Next Wave*, 19, no. 2 (2012): 47-57, https://www.nsa.gov/research/tnw/tnw192/articles/pdfs/TNW_19_2_Web.pdf (preuzeto 28. jula 2015).

[10] Radomir Lukić, „Da li je pravo nauka?" (predavanje, 29. januar 1966. Reči u vremenu – zvučni zapisi predavanja na Kolarcu, DVD – Video, Zadužbina Ilije M. Kolarca, Centar za izdavačku delatnost, Beograd, 2007).

[11] Peter Lodewyckx, „Nauka odbrane: Da li postoje?" *Vojno delo* (2011): 78-82.

[12] Peter J. Denning, "Is Computer Science Science?" *Communications of the ACM* 48, no. 4 (2005): 27-31.

[13] Cherif M. Bassiouni, „International Crimer: The Ratione Materiae of International Criminal Law." in *International Criminal Law. Vol. 1, Sources, Subjects, and Contents*, ed. Bassiouni M. Cherif (Leiden, Netherlands: Martinus Nijhoff Publishers, 2008).

[14] Carl E. Landwehr, „Cybersecurity: From Engineering to Science", *The Next Wave*, 19, no.2 (2012), 2-5, https://www.nsa.gov/research/tnw/tnw192/articles/pdfs/TNW_19_2_Web.pdf (preuzeto 28. jula 2015).

[15] Lukić, „Da li je pravo nauka?"

[16] Landwehr, „Cybersecurity: From engineering."

se posebno odnosi na postupak utvrđivanja karaktera, zahteva i posledica različitih pristupa međunarodnog pravnog regulisanja sajber sukoba. Bez obzira na brzinu izmene prirode sajber sukoba, pri njegovom istraživanju je moguće učiniti potrebne opservacije predmeta istraživanja, postaviti ključna pitanja od značaja, razviti pretpostavke, formulisati hipoteze, prikupiti podatke od značaja za istraživanje i razviti opštu teoriju.

Međutim, ono što nije moguće učiniti u konkretnom razmatranju modela međunarodne pravne regulacije sukoba u sajber prostoru je njegovo testiranje u praksi. Nije moguće preduzeti eksperiment, niti izvesti kvantitativno istraživanje koje može predvideti ponašanje pojedinaca, grupa, država i čovečanstva u pogledu primene i regulisanja sajber ratovanja u budućnosti. Eksperiment je naučna metoda istraživanja u prirodnim naukama. Tokom eksperimenta se stvara model predmeta istraživanja, kojim istraživač manipuliše u željenom pravcu radi sticanja novog saznanja. Eksperimentalna saznanja se mogu sistematizovati i predstaviti naučnim zakonima, ukoliko su potvrđena naučnim dokazivanjem ili teorijama, odnosno hipotezama, ukoliko pružaju naučno prihvatljiv odgovor. Sa metodološkog stanovišta, osnovni razlog za primenu eksperimenta je veličina potrebnog modela. Zbog etičkih, praktičnih i organizacionih problema, u oblasti društvenih nauka metoda eksperimenta se može sprovoditi samo u ograničenoj meri po obimu i predmetu istraživanja.[17]

U području sajber sukoba još uvek nije u praksi potvrđena istinitost ni jedne hipoteze na metodološki prihvatljiv način. Međunarodni sukobi predstavljaju odnose između nacija. Na tom nivou ne postoje predvidljivi obrasci ponašanja pojedinaca i grupa u sličnim ili različitim situacijama. To čak i jednostavne društvene probleme i situacije podiže na nivo problema kompleksnih sistema. Primena klasičnih metoda društvenih nauka na situacije međunarodnih sukoba u sajber prostoru vodi nužno u područje kompleksnosti, koje odudara od potreba međunarodnopravnog regulisanja sukoba, koje teži jednostavnosti i primenljivosti.

[17] Neil F. Johnson, "Chapter 1: Two's Company, Three is Complexity," *Simply complexity: A clear guide to complexity theory* (London, UK: Oneworld Publications, 2009) 3.

Postavlja se pitanje izbora odgovarajućeg disciplinarnog pristupa u procesu istraživanja sukoba u sajber prostoru, kao i pitanje odnosa između različitih naučnih disciplina. Taj problem se može sažeti u pitanju, da li je pogodnija primena naučne metode (istraživanja) u kontekstu jedne naučne discipline, multidisciplinarnim, interdisciplinarnim, unakrsno-disciplinarnim, transdisciplinarnim ili potpuno vandisciplinarnim pristupom?

Pitanje se postavlja i u vezi izbora primarne metode istraživanja. Na primer, pojedine društvene nauke, poput sociologije, ekonomije, a u poslednje vreme, čak i prava, zahvaljujući primeni informacionih tehnologija i statistike, doživele su revoluciju u primeni metoda formalnih logičkih nauka u okviru svog primarnog područja istraživanja. Primena statistike i kvantitativni doprinos računarskih tehnologija u tom procesu stvaraju nove kvalitativne uvide u predmet naučnog istraživanja. Iako je primena statistike u mnogim slučajevima opravdana, u praksi naučnog istraživanja se mogu sresti slučajevi njene nepotrebne i neopravdane primene, kao težnje istraživača da na veštački način pruže doprinos kvalitetu i vrednosti ostvarenih rezultata. U tom pogledu nameće se niz pitanja. Da li se statističkom analizom dosadašnjih napada u sajber prostoru može predvideti kada, i na koji način će biti preduzet sledeći napad? Da li je moguće stvoriti ikakvo naučno prihvatljivo predviđanje o načinu mogućeg regulisanja sukoba koje je zasnovano isključivo na logici i formalnim odnosima, a ne na nacionalnom interesu i nacionalnoj moći? Istorija govori da se ratovi pokreću kao posledica odnosa između nacija i njihovih interesa. Pa ipak, ratovi se još od antičkog doba i Trojanskog rata pokreću nekada i na osnovu potpuno iracionalnih razloga. Da pojedine nacije nisu pokretale ratove, ne bi dolazilo do njihovog sloma i opšteg poraza kao posledica tih ratova u periodima kada su imale najveću nacionalnu moć, na primer, u slučaju nacističke Nemačke tokom Drugog svetskog rata ili Austrougarske monarhije pred Prvi svetski rat. Odluke o ratovima i savezima su donošene iznenada, neočekivano, pod uticajem unutrašnjih i spoljnih faktora racionalne i iracionalne prirode. Statističko obrađivanje događaja pokrenutih na osnovu iracionalnih odluka ne može pružiti naučno valjane rezultate, niti pokazati prirodnu zakonitost u sledu događaja. Pored toga, stavovi, ideje, uverenja i emocije ljudi nisu podložne matematičkim logičkim operacijama na način koji pruža egzaktno predviđanje budućeg ishoda.

Po Čomskom[18], primena čiste statističke metode u opisivanju pojava u svetu, bez napora da se razume smisao, predstavlja samo formalno oponašanje tih pojava, a ne suštinsko razumevanje, čak i u onim područjima u kojima se tradicionalno koriste metode formalnih nauka, kao što je lingvistika. Međutim, to ne znači da statističke metode nemaju moć da ostvare suštinske uvide u pogodnim specifičnim oblastima naučnog istraživanja, [19] niti da ih treba izbegavati zbog prethodnog ubeđenja.

Međutim, primer morfogeneze, fraktala[20] i nekada iznenađujućih rezultata numeričke analize prirodnih pojava, pokazuju da veza između haosa, prirodnih i društvenih nauka možda i nije slučajna, već suštinska, pri čemu je moguće da logičke zakonitosti formalnih nauka predstavljaju jedinu zajedničku vezu koja uopšte i postoji između navedenih oblasti. Ista matematička logika stoji u osnovi formalnih procesa na osnovu kojih rastu biljke[21], formira se klima[22], obrazuje se DNK lanac[23] ili nastaju ratovi[24]. Ukoliko je tako, formalne nauke mogu predstavljati ključnu sponu između prirodnih i društvenih nauka i instrument u borbi za savladavanje izazova haosa, koji je posledica nekontrolisane i rastuće kompleksnosti sistema, kako su to, svaki na svoj način, videli Poenkare[25], Tjuring[26] i Mandelbrot[27]. Najl navodi cilj takve primene formalnih nauka u okviru rešavanja problema kompleksnosti: „Sveti gral kompleksnosti je razumevanje, predviđanje i kontrola takvih specifičnih dolazećih fenomena, poput mogućih

[18] Noam Chomsky, „The Golden Age: A Look at the Original Roots of Artificial Intelligence, Cognitive Science, and Neuroscience," Keynote Panel, *Symposium: „Brains, Minds and Machines,*" MIT - Massachusetts Institute of Technology, delimički transkript preuzet sa http://languagelog.ldc.upenn.edu/myl/PinkerChomskyMIT.html (preuzeto 30. marta 2016).

[19] Peter Norvig, „On Chomsky and the Two Cultures of Statistical Learning," http://norvig.com/chomsky.html (preuzeto 30. marta 2016).

[20] Benoit B. Mandelbrot, *The Fractal Geometry of Nature* (New York, NY: W. H. Freeman and Company, 1982): 35.

[21] Alan Mathison Turing, "The Chemical Basis of Morphogenesis," *Philosophical Transactions of the Royal Society of London B: Biological Sciences* 237, no. 641 (1952): 37-72.

[22] Benoit B. Mandelbrot, "The Fractals and the Geometry of Nature," (1982), http://users.math.yale.edu/~bbm3/web_pdfs/encyclopediaBritannica.pdf (preuzeto 5. avgusta 2015).

[23] Yu B. Rumer, "Translation of 'Systematization of Codons in the Genetic Code [III]'by Yu. B. Rumer (1969)," *Philosophical Transactions of the Royal Society A* 374, no. 2063 (2016): 20150448.

[24] Neil F. Johnson, "Chapter 1: Two's Company, Three is Complexity," *Simply Complexity: A Clear Guide to Complexity Theory* (London, UK: Oneworld Publications, 2009), 5. http://www.uvm.edu/rsenr/nr385se/readings/complexity.pdf

[25] Henri Poincaré, *Science and hypothesis* (New York, NY: Science Press, 1905).

[26] Turing, "The Chemical Basis."

[27] Mandelbrot, *The fractal geometry*.

katastrofičnih masovnih efekata kao što su berzanski lomovi, saobraćajne gužve pojave bolesti, ljudski sukobi i promene prirodne okoline. Da li su one na bilo koji način predvidive, ili jednostavno nastaju niotkuda bez upozorenja? Da li one mogu biti kontrolisane, upravljane ili čak izbegnute“ [28].

Međutim, u osnovi svake kompleksnosti leži jednostavnost, a pravilo koje multiciplira tu jednostavnost, dovodi do beskonačne složenosti. Na primer, jednačina Mandelbrotovog skupa:

$$f_c(z) = z^2 + c$$

opisuje zatvoren (povezan) skup vrednosti *c* u kompleksnoj ravni (tačaka čija pozicija se može odrediti na osnovu njihove realne i imaginarne vrednosti), kod koje se rezultat vrednosti funkcije njenim neprekidnim ponavljanjem nalazi u skupu povezanih tačaka, [29] odnosno fraktala[30]. Tjuring[31] i Rumer[32] su odvojeno pokazali da je čak i uređenje gena u okviru DNK[33] sistematično definisano jednostavnim matematičko-logičkim pravilima.

U tom pogledu korisno može biti pravilo koje je postavio Fajerbou u vezi sa istraživanjem u oblasti sociologije, a koje je primenjivo na širi skup društvenih nauka, posebno onih koje teže primeni statističkih metoda u istraživanju: “Neka metod bude sluga, ne gospodar“[34]. U praksi istraživanja sajber sukoba i ratovanja, primena navedenog pravila prvenstveno se odnosi na davanje prioriteta predmetu istraživanja, onome što jeste na izvoru nastanka fenomena, što ga gradi i uslovljava mu prirodu razvoja. Razumevanje suštine elemenata i njihovih odnosa, uključujući i sile koje ih pokreću, je jedini put istraživanja celine. Poštujući navedeni princip, jasno je da pristup istraživanju mora biti višedisciplinarne prirode, pre svega multidisciplinaran, a u mnogim delovima i interdisciplinaran. Ovakav izbor je razumljiv, pošto je i sama priroda sukoba u sajber

[28] Johnson, " Two's Company.“

[29] Robert L. Devaney, Peter B. Siegel, and A. John Mallinckrodt, „A First Course in Chaotic Dynamical Systems: Theory and Experiment,“ *Computers in Physics*, 7, no.4 (1994): 416-417.

[30] U najkraćem, fraktali su prirodno-matematički fenomen koji predstavlja skup ponavljajućih obrazaca koji se ponavljaju na svakom nivou.
Mandelbrot, "The Fractals."

[31] Turing, "The Chemical Basis."

[32] Rumer, "Systematization of Codons."

[33] Dezoksiribonukleinska kiselina

[34] Glenn Firebaugh, *Seven Rules for Social Research* (Princeton, NJ: Princeton University Press, 2008).

prostoru takva, istovremeno sačinjena delovanjem raznorodnih faktora koje proučavaju različite i raznorodne naučne discipline.

Na sličan način se mogu prikazati i društvene interakcije između ljudi i zajednica. Na primer, i ratovi i terorizam mogu biti shvaćeni kao „kolektivne, nasilne aktivnosti koje vode različite grupe ljudi koje su u sukobu za kontrolu određenih resursa"[35]. U tom slučaju nije važan pravni status učesnika. Ono što sukobe čini tako kompleksnim, nije logična i razumljiva ideja o njihovom izvornom uzroku (nadmetanju za ostvarivanje vlastitih interesa), već način na koji se to čini (struktura i forma sukoba). Primenjena tehnologija čini da se priroda sukoba menja od linearnih ka nelinearnim, povećavajući stepen njihove kompleksnosti.

Dakle, proces istraživanja (međunarodnih) sukoba u sajber prostoru u smislu primene Međunarodnog prava oružanih sukoba se sastoji od dva važna nivoa:

- utvrđivanja suštinske prirode elemenata i okruženja sajber sukoba i
- razumevanja njegove kompleksne primene u međunarodnim odnosima.

Ovakav proces zahteva primenu različitih metoda naučnog istraživanja, pri čemu je redosled njihove primene podjednako značajan kao i sam izbor.

1.2. Problemi

Predmet i problemi područja istraživanja pravne regulacije međunarodnih sukoba u sajber prostoru se tiču specifičnog karaktera digitalnih informacionih tehnologija i njihove informacione bezbednosti. Informaciona bezbednost predstavlja bezbednosnu praksu koja je nastala iz razvoja i upotrebe informaciono-komunikacionih tehnologija i nema veze sa političkim kontekstom sukoba u sajber prostoru. Ona je neutralna u odnosu na političku volju država i nasilne načine njenog ostvarivanja. Na njenu suštinu utiču različiti faktori poput ljudi, tehničkih i organizacionih sistema i procesa. Njihova interakcija stvara virtuelne, dinamične, nehomogene i nestalne društveno-tehničke sisteme ljudi, softvera i hardvera. To dovodi do situacija u kojima se složeni i sistematični napori za dostizanje

[35] Johnson, "Two's Company."

željenog nivoa informacione bezbednosti mogu lako poništiti iskorišćavanjem skrivenih internih i eksternih ranjivosti sistema.

Sajber bezbednost se odnosi na informacionu bezbednost u sajber prostoru[36, 37, 38, 39, 40,41]. Njen konačni cilj je stvaranje sposobnosti korisnika i/ili vlasnika informacija i informacionih sistema za odbranu od svih vrsta sajber napada,[42] bez obzira da li su napadi otkriveni ili nisu, da li je napadač poznat ili nije, i da li je za napad odgovorna država ili nedržavna organizacija, grupa ili čak pojedinac. Kako navodi Šnajder, branioci razvijaju metode i tehnike za odbranu od napada koji su im poznati, najviše iz razloga što raspolažu sa ograničenim resursima, što za posledicu ima povećanje verovatnoće da će nove vrste napada koje razvijaju napadači biti uspešne.[43] U sajber bezbednosti, napadaču je dovoljno da iskoristi jednu ranjivost branjenog sistema da bi prošao kroz sistem zaštite ili ga zaobišao, dok branilac mora da zaštiti i osigura sve moguće ranjivosti koji omogućavaju napad. Time se ističe značaj ofanzivnih aktivnosti u sajber prostoru.

Međunarodno pravo oružanih sukoba potencira miroljubivo rešavanje sporova, sprečavanje i kontrolu oružanih sukoba. Međutim, ono se odnosi na agresiju, upotrebu sile ili pretnju silom, kao i na upotrebu oružane sile isključivo u odnosima između međunarodnih subjekata, a ne na kriminalne aktivnosti pojedinaca, grupa, pa čak ni na

[36] International Organization for Standardization, ISO/IEC Glossary of IT Security Terminology, ISO/IEC, 2013, http://www.jtc1sc27.din.de/cmd?level=tpl-bereich&menuid=64540&languageid=en&cmsareaid=64540

[37] International Telecommunication Union, ITU-T X.1205 (04/2008), 2008, 3.2.5, Termite 6L - Terminology of Telecommunications - V.7, Updated 2014, http://www.itu.int/online/termite/index.html

[38] Government of Israel, Resolution No. 3611: Advancing National Cyberspace Capabilities, 2011, 1 http://www.pmo.gov.il/English/PrimeMinistersOffice/DivisionsAndAuthorities/cyber/Documents/Advancing%20National%20Cyberspace%20Capabilities.pdf

[39] Совет Федерации, Федералыного Собрания Российской Федерации, *Концепция стратегии кибербезопасности Российской Федерации - Проект*, (10 января 2014), 2, http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf (preuzeto 5. januara 2016).

[40] United States of America, Committee on National Security Systems, National Information Assurance Glossary, 2010, 22, http://www.ncix.gov/publications/policy/docs/CNSSI_4009.pdf

[41] Richard Kissel, National Institute of Standards and Technology Glossary of Key Information Security Terms, U.S. Department of Commerce, 2013, 58, http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

[42] Schneider, „Blueprint for Cyber Security."

[43] Ibid, 47.

aktivnosti država ukoliko se ne mogu oceniti aktima agresije ili primene (oružane i druge) sile.

Mogućnost napada (primene sile) u sajber sukobima ne zavisi od raspolaganja oružjem, već znanjem. Postojanje ranjivosti u sistemima dovodi do narušavanja bezbednosti sistema, čak i na nacionalnom nivou, što se ne može potpuno kontrolisati i bezbednosno je nepredvidivo. U sukobu u sajber prostoru stoga nema poznate zakonitosti koje se odnose na to ko, kada i kako primenjuje silu, niti je put do nje očigledan. Takođe, ne može se ni utvrditi zakonitost ukoliko je nema. Konačno, ni svi sadržaji, elementi, odnosi ili procesi unutar područja istraživanja se ne mogu dugoročno predvideti, s obzirom da se i razvoj novih tehnologija odvija u nepredvidivom sledu.[44]

Imajući u vidu ove probleme i ograničenja, postavlja se opravdano pitanje: da li je moguće utvrditi naučno zasnovanu zakonitost u području regulisanja sukoba u sajber prostoru, odnosno da li je moguća primena naučne metodologije u pronalaženju optimalnog modela međunarodnopravnog regulisanja sukoba u sajber prostoru, i ukoliko jeste, primenom kog metodološkog pristupa?

Bez obzira što su sukobi u sajber prostoru nova oblast aktivnosti, o primeni Međunarodnog prava oružanih sukoba na sajber sukobe postoji široka literatura. Pri tome, većina istraživača se bavi analogijom između tradicionalnih situacija u fizičkom okruženju i novih situacija u sajber prostoru. Pri tome se polazi od osnovnih principa međunarodnog prava, pošto se radi o pravno orjentisanoj analizi i istraživanju. Takav pristup stvara potrebu za uspostavljanjem ontološkog sistema znanja i verovanja o pitanju šta konstituiše regulaciju sajber ratovanja.

1.2.1. Logička reprezentacija fenomena i pojmova

U području predmeta istraživanja postoji često preklapanje u značenju različitih pojmova koji predstavljaju različite fenomene u različitim područjima, ali koji se primenom računarskih tehnologija i kroz računarske tehnologije u praktičnom smislu svode na isto područje aktivnosti. Na primer, svi ti fenomeni su zasnovani na informacijama, računarskim tehnologijama i komunikacionim sistemima; odnose se na specifične,

[44] Kadtke and Wells, *Policy Challenges*.

odnosno elementarne pojmove, na sisteme, procese ili čak na celokupna okruženja i koncepte. To preklapanje značenja se odnosi na pojmove iz skupa informacionih, računarskih i komunikacionih tehnologija.

Pored toga, navedeni fenomeni i koncepti imaju različito značenje u odnosu na ugao posmatranja. Na primer, sajber napad nema isto značenje u pogledu vojne veštine, sajber bezbednosti i međunarodnog prava. Upotrebom istih termina za označavanje različitih pojmova i različitih termina za iste pojmove povećava se mogućnost greške u ontološkom definisanju fenomena od značaja za sukobe u sajber prostoru. To se posebno odnosi na skup opštih pojmova kao što su „informacioni", „informatički", „računarski" i „sajber", i izvedenih pojmova, kao što su „sajber sukob", „sajber rat", „agresija u sajber prostoru", „sajber napad" i drugi. Neusaglašena terminologija osnovnih i izvedenih pojmova u oblasti sajber sukoba postoji čak i u praksi jedinstvenih nacionalnih kultura,[45] a to može voditi pogrešnoj ontološkoj predstavi.

Razvoj tehnologije nameće potrebu razlikovanja računarskih nauka i informaciono-komunikacionih tehnologija. Računarske nauke predstavljaju primenu naučnog pristupa u cilju sveobuhvatnog bavljenja računarskim sistemima, principima njihove upotrebe, tehnologijom, automatskom obradom podataka, inteligentnim sistemima, softverskim inženjerstvom, arhitekturom računarskih sistema, programskim jezicima, operativnim sistemima i drugim područjima računarstva. To podrazumeva razvoj teorije i metoda čuvanja, obrade i distribucije podataka i informacija u računarskim sistemima, dizajn softvera i hardvera i sveobuhvatnu primenu računarstva povezujući teoriju i praksu njihovog razvoja i upotrebe. Dakle, računarske nauke se bave primenom naučnog pristupa u istraživanju računarstva, odnosno fenomena koji okružuju i kreiraju računare.[46] Po Deningu[47], one obuhvataju sveobuhvatno angažovanje matematičara, naučnika iz

[45] Iako je pojam „sajber rat" potekao iz jedinstvenog anglosaksonskog govornog područja, tačnije iz SAD, najpoznatija enciklopedija na engleskom jeziku, „Britanika", navodi da se za ovaj složeni pojam naizmenično primenjuju termini sa različitim smislom i oblikom reči: „cyberwar" (sajber rat), koji se često piše i kao odvojena reč „cyber war", i „cyberwarfare" (sajber ratovanje), koji se takođe često piše i odvojeno kao „cyber warfare". http://www.britannica.com/topic/cyberwar

[46] Allen Newell and Herbert A. Simon, "Computer science as empirical inquiry: Symbols and search," *Communications of the ACM* 19, no. 3 (1976): 113-126.

[47] Peter J Denning, "Is computer science science?," *Communications of the ACM* 48, no. 4 (2005): 27-31, 28

područja prirodnih nauka i inženjera, čime povezuju informaciono-komunikacione tehnologije, matematiku i prirodne nauke, ujedno povezujući teoriju i praksu.

Tehnologija se odnosi na veštinu upotrebe sredstava, procesa i metoda u praktičnoj primeni nekih znanja (do kojih dolazi iskustvo ili nauka). Ključne tehnologije (i tehnički sistemi zasnovani na njima) u području koji gradi sajber prostor su informacione, računarske i komunikacione tehnologije. Svaka of navedenih grupa tehnologija ima svoje sopstveno područje primene. Informacione tehnologije predstavljaju „svaku opremu ili povezane sisteme ili podsisteme opreme za obradu, prenos, prijem, slanje i razmenu podataka i informacija“[48] Oksfordski rečnik definiše informacione tehnologije kao „izučavanje ili upotrebu sistema (posebno računarskih i telekomunikacionih) za čuvanje, dobijanje i slanje informacija“[49]. Meriam-Vebster definiše informacione tehnologije kao: „tehnologije koje uključuju razvoj, održavanje i upotrebu računarskih sistema, softvera i mreža za obradu i distribuciju podataka“[50]. Dakle, informacione tehnologije se odnose na podatke i informacije i predstavljaju sredstva, tehnike i metode njihovog kreiranja, obrade, razmene i reprezentacije.

Pojam informaciono-komunikacionih tehnologija se u praksi najčešće koristi u najširem smislu u odnosu na informacione, komunikacione i računarske tehnologije, kao „tehnologije i oprema za rukovanje (na primer, pristup, kreiranje, prikupljanje, slanje, primanje i širenje) informacija i komunikacija.“[51] To znači da ovaj pojam obuhvata i informacione i komunikacione tehnologije, uključujući razna sredstva masovne komunikacije, kao što su radio, televizija, telefonija, Internet; računarske sisteme poput

[48] National Initiative for Cybersecurity Careers and Studies, U.S. Department of Homeland Security, *Explore Terms: A Glossary of Common Cybersecurity Terminology*, http://niccs.us-cert.gov/glossary

[49] *Oxford Dictionaries*, s.v. „information technology,“ http://www.oxforddictionaries.com/definition/english/information-technology?q=information+technology

[50] *Merriam-Webster*, s.v. „information technology,“ http://www.merriam-webster.com/dictionary/information%20technology

[51] International Telecommunication Union, ITU Terms and Definitions, Updated 2014, ITU-T K.58 (02/2014), 2014, 3.2.1, http://www.itu.int/ITU-R/index.asp?redirect=true&category=information&rlink=terminology-database&lang=en&adsearch=&SearchTerminology=exploit&collection=both&sector=all&language=all&part=abbreviationterm&kind=anywhere&StartRecord=1&NumberRecords=50 (preuzeto 10. novembra 2015).

hardvera i softvera; pa čak i komunikacionu infrastrukturu poput kablovskih i satelitskih sistema.[52]

Međutim, bez obzira na pojam informacionih i komunikacionih tehnologija, u pogledu izgradnje i funkcionisanja sajber prostora, one uvek moraju istovremeno biti i računarske tehnologije. Računarski sistemi su uređaji ili programi koji se koriste za izvođenje operacija nad podacima na automatizovan, numerički način. Podaci ulaze u računarske sisteme, koji ih obrađuju primenom matematičkih operacija, podeljenih u logičke sekvence (programe), i zatim izlaze sa promenjenom vrednošću koja zavisi od vrste izvedenih operacija.[53] Sve informacione i informaciono-komunikacione tehnologije koje primenjuju računarske tehnologije učestvuju u stvaranju sajber prostora. Računarske tehnologije se u savremenoj praksi se uglavnom odnose na digitalne tehnologije, odnosno digitalne podatke, ali je moguće da to budu i analogni, kvantni ili čak biološki računarski sistemi i tehnologije, kao i svi drugi budući računarski sistemi koji omogućavaju kreiranje, skladištenje, obradu, razmenu i reprezentaciju podataka. Dakle, računarski sistemi i tehnologije svojim funkcionisanjem i umrežavanjem sačinjavaju sajber prostor, a tehnološki razvoj je doveo do situacije u kojoj su informacione i informaciono-komunikacione tehnologije i sistemi u najvećoj meri zasnovane na računarskim tehnologijama, sposobnim za automatsku obradu podataka.

Međutim, osim računarskih tehnologija, postoje i računarske nauke, koje su orjentisane ka praktičnom aspektu i tehnički su vrlo bliske području tehnologija. Pored računarskih postoje i informacione nauke. Oksfordski rečnik definiše informacione nauke kao „izučavanje procesa čuvanja i dobijanja informacija“[54], a Meriam-Vebster rečnik kao: „prikupljanje, klasifikaciju, čuvanje, dobijanje i širenje zabeleženog znanja“[55]. Dakle, moguće je praktično preklapanje značenja pojmova računarski i informacioni, kao i sadržaja odgovarajućih nauka i tehnologija koje se bave njihovim predmetom i sadržajem

[52] Austria, Bundeskanzleramt Osterreich, „Austrian Cyber Security Strategy“ Federal Chancellery of the Republic of Austria, 2013, 22, http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world

[53] Oxford University, *A Dictionary of Computing*, (New York, NY: Oxford University Press, 2004), 102

[54] *Oxford Dictionaries,* s.v. „information science,“ http://www.oxforddictionaries.com/definition/english/information-science

[55] *Merriam-Webster*, s.v. „information science,“ http://www.merriam-webster.com/dictionary/information%20science

proučavanja. Ipak, između informacionih i računarskih nauka, kao i tehnologija postoji razlika. Dok računarske nauke proučavaju automatsku obradu podataka i principe rada računarskih sistema, informacione nauke proučavaju informacije i načine na koji informacije koriste ljudi i obrađuju računarski sistemi.

Tehnološki razvoj digitalnih sistema i njegovo uključivanje u sve informacione, komunikacione i računarske tehnologije i sisteme dodatno približava predstave navedenih pojmova. Većina savremenih informacija i podataka veštačkog porekla je digitalnog karaktera, a većina savremenih informacionih tehnologija (koje mogu biti analogne i digitalne) su računarskog porekla. Svi informacioni sistemi nisu ujedno i računarski, ali trend digitalizacije vodi ka tome da postanu. Skup računarskih sistema čini podskup informacionih sistema, pošto svi računari koriste podatke (informacije sa značenjem) za izvršavanje svoje osnovne funkcije. Imajući to u vidu, najbliži termin za označavanje tehnologija koje izgrađuju i razvijaju sajber prostor je „računarske informacione tehnologije“, pošto se atributi-termini „računarski“ i „informacioni“ ne mogu uzajamno zamenjivati, niti se treba smatrati da su nauke samo „računarske“, a tehnologije samo „informacione“.[56] Istovremeno, imajući u vidu konvergenciju između računarskih, informacionih i komunikacionih tehnologija u vidu digitalnih tehnologija, najobuhvatniji termin za označavanje tehnologije koje stvaraju sajber prostor je „informaciono-komunikacione tehnologije“.

1.2.2. Taksonomski problemi

Tehnologija se razvija na fizičkom nivou, pošto se odnosi na realne fenomene koji postoje u fizičkom svetu. Koncepti predstavljaju tehnološke, društvene, vojne i pravne pojave i rešenja i mogu dolaziti iz različitih sistema vrednosti, reprezentacija i područja aktivnosti. Nastojanje da se ostvari sistematičan i dosledan pristup istraživanju zahteva stabilnu naučnu klasifikaciju, kako po sadržaju, tako i po odnosu dela prema celini. Brz razvoj informaciono-komunikacionih tehnologija donosi promene postojećih fenomena istraživanja, i do pojave novih. Visoka dinamika razvoja dovodi do neusklađenosti značenja koncepata koji te fenomene označavaju, do pojave nejasnoća na nivou njihove

[56] S tim u vezi neće biti u potrebi uobičajeni termin „računarske nauke i informacione tehnologije“ u smislu označavanja jedinstvenog skupa tehnologija relevantnih za primenu sukoba u sajber prostoru i naučnih znanja na kojim se zasnivaju.

lingvističke reprezentacije - pojmova, i pogrešne upotrebe odgovarajućih jezičkih izraza - termina.

U oblasti primene informaciono-komunikacionih tehnologija često dolazi do mešanja značenja osnovnih i izvedenih pojmova. Na primer, u javnosti i medijima je čest slučaj da se sajber ratovanje meša sa sajber kriminalom i njegovim posebnim oblicima, sajber špijunažom i sajber terorizmom.[57] Takve situacije mogu stvoriti ne samo lingvističke i epistemološke probleme, već i probleme političke i pravne prirode.[58] Međutim, problemi taksonomije fenomena u oblasti sukoba u sajber prostoru su posledice, a ne uzrok njegove nedefinisane prirode. Bez znanja o suštini prirode sukoba u sajber prostoru i njenih karakteristika, nije moguće ni izvršiti njihovu međunarodnopravnu regulaciju. U tu svrhu neophodno je uspostaviti univerzalni sistem ključnih pojmova u području sukoba u sajber prostoru. Svrha tog specifičnog i opšteg definisanja je objektivno utvrđivanje njihove prirode i međusobnog odnosa.

Pri izgradnji ontološko-taksonomskog sistema moguće je primeniti materijalistički ili idealistički pristup. Primer prvog bi bilo shvatanje da je sajber napad usmeren na ostvarivanje efekata na cilj napada koji su po posledicama ekvivalentni napadu u fizičkom okruženju. Primer drugog bi predstavljao pristup iz ugla dominacije jednog specifičnog prava nad drugima, na primer, Međunarodnog prava oružanih sukoba, i posmatranje i procenu objektivne stvarnosti kroz prizmu njegove strukture.

1.2.3. Sistemski pristup

Opšti pojam sukoba ima široko značenje. Na primer, „oružani sukob“ ili „vojni sukob“, koji se odnose na primenu oružane ili vojne sile u sukobu, su podskup šireg pojma „sukob“, koji pored vojnih, koristi i ekonomske, političke, diplomatske, kulturne i druge metode i sredstva.[59] I vođenje sukoba u sajber prostoru se može posmatrati u užem i širem kontekstu u odnosu na različite kriterijume. Prethodna analiza je pokazala da su informaciono-komunikacione tehnologije ključni faktor koji omogućava i utiče na sukobe

[57] *Encyclopaedia Britannica,* s.v. „cyberwar,“http://www.britannica.com/topic/cyberwar

[58] Jarno Limnéll, „The Danger of Mixing Cyberespionage with Cyberwarfare,“ *Wired,* http://www.wired.com/insights/2013/07/the-danger-of-mixing-cyberespionage-with-cyberwarfare/ (preuzeto 25. februara 2016).

[59] Herbert Lin, "Cyber conflict and international humanitarian law," *International Review of the Red Cross* 94, no. 886 (2012): 515-531, 517.

u sajber prostoru. U skladu sa tim, uži kontekst sajber sukoba obuhvata suštinske karakteristike sukoba u sajber prostoru, koje su nezavisne od načina primene i okruženja i primarno zavise od informaciono-komunikacionih tehnologija. Širi kontekst prirode sukoba u sajber prostoru čine sve izvedene karakteristike koje su posledica specifične primene, aktivnosti i okruženja. Te karakteristike se tiču vojnog, pravnog, sociološkog, ekonomskog, organizacionog aspekta, kao i šireg tehnološkog apsekta. Zbog toga je potrebno u toku istraživanja utvrditi prirodu sukoba u sajber prostoru u užem i u širem smislu. Pod tom prirodom se smatra sistem znanja koji sadrži podatke, informacije, utvrđene zakonitosti i obrasce ponašanja i odnose između uključenih elemenata od značaja za sajber sukobe; praksu i trendove razvoja, na osnovu kojih se mogu opisati, objasniti, razumeti, planirati, organizovati i predvideti okolnosti od značaja za sajber ratovanje i za sukobe u sajber prostoru. To razumevanje treba da obuhvati i dva ključna aspekta:

a) razvoj, planiranje, organizovanje i vođenje vojnih operacija u sajber prostoru;
b) nacionalno i međunarodnopravno regulisanje sajber ratovanja/sukoba u sajber prostoru.

Imajući u vidu zastupljenost informaciono-komunikacionih tehnologija u svim ljudskim aktivnostima, obim i brzinu njihovog razvoja, ovakav poduhvat je zahtevan i ne može se rešiti u okviru jedne naučne discipline.

Razlog za to je sam koncept sajber sukoba. Informacioni sistemi sadrže ranjivosti koje su podložne zloupotrebi, omogućavajući napadačima preduzimanje sajber napada. Po Hačinsu, Klopertu i Aminu[60]; Heru[61]; Čoseku i Podinsu[62] i kompaniji Gartner[63], zajedničke faze postupaka koje napadači preuzimaju u cilju izvršenja sajber napada načelno su:

[60] Eric M. Hutchins, Michael J. Cloppert, and Rohan M. Amin, "Intelligence-driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," *Leading Issues in Information Warfare & Security Research* 1 (2011): 80.

[61] Trey Herr, "PrEP: A Framework for Malware and Cyber Weapons," *Proceedings of the International Conference on Information Warfare & Security*, 2014: 84-91.

[62] Christian Czosseck and Karlis Podins, "A Vulnerability-Based Model of Cyber Weapons and its Implications for Cyber Conflict," *Proceedings of the European Conference on Information Warfare and Security* (Academic Conferences, Limited, 2012): 246.

[63] "Selecting Security Monitoring Approaches by Using the Attack Chain Model," *Gartner*, https://www.gartner.com/doc/2816617?ref=clientFriendlyURL (preuzeto 18. marta 2016).

a) pronalaženja ranjivosti u drugim informacionim sistemima;
b) iskorišćavanja otkrivenih ranjivosti u cilju pristupa i narušavanja nekog svojstva informacione bezbednosti napadnutog sistema;
c) izvršenja planiranog dejstva kojom se čini šteta/agresija nad napadnutim sistemom.

Sajber napadi predstavljaju ispoljavanje agresije nad drugom stranom primenom znanja iz oblasti informacione bezbednosti. Na napadaču je odluka o izboru ranjivosti i načinu dejstva na cilj. Različiti napadači će stoga izvršiti sajber napade na isti cilj na potpuno različite načine. Osnovni resurs za preduzimanje napada su znanje i veština napadača, koji postoje objektivno kao sistem znanja koji proučavaju računarske nauke i primenjuju informaciono-komunikacione tehnologije i informaciona, odnosno sajber bezbednosti, i subjektivno, kao znanje karakteristično za napadača. Znanje neophodno za preduzimanje sajber napada nema apsolutnu destruktivnu moć, već je svojstveno konkretnom napadaču. Ti sukobi se mogu odvijati u toku tradicionalnog, oružanog rata, ali još češće se odvijaju u nevojnim oblicima asimetrične ili hibridne agresije između subjekata međunarodnog prava. Dakle, na njihovu regulaciju utiče i kontekst primene. Posledice sajber napada mogu biti trenutne, ali i odložene. Motivi napadača mogu biti političke prirode, ali mogu biti i posledica sticanja tehničkih uslova za preduzimanje napada, na primer, poznavanje i pristup ranjivosti nekog važnog sistema, bez ikakvih političkih motiva. Efekti sajber napada mogu biti direktni i indirektni i mogu se osećati odvojeno ili istovremeno na različitim nivoima: fizičkom, logičkom i društveno-kognitivnom. Sajber napadi imaju inherentno svojstvo da se mogu preduzimati prikriveno, da se napadači mogu sakriti, i da se istovremeno mogu preduzimati u različitim modelima sukoba.

U navedenim okolnostima istraživanje se velikim delom odnosi na posmatranje i analizu specifičnosti predmeta u kompleksnom, međuzavisnom okruženju. Iako to kompleksno okruženje samo po sebi nije jedinstven i egzaktan sistem, jer ne predstavlja organizaciju entiteta i fenomena koji imaju zajedničku svrhu ili cilj,[64] ono se sastoji od mnoštva međupovezanih i međuzavisnih sistema različite prirode. Zbog toga je u istraživanju fenomena sajber ratovanja važno primeniti proces sistemskog razmišljanja u cilju rešavanja problema, na način koji je po formi sličan procesu sistemskog razmišljanja u

[64] *Merriam-Webster*, s.v. „system," http://www.merriam-webster.com/dictionary/system

prirodnim i društvenim naukama.[65] Raznorodni faktori koji utiču na prirodu sajber ratovanja kreiraju strukture i procese koji zajedničkim delovanjem stvaraju povoljno ili nepovoljno okruženje za vođenje sajber ratovanja. Iako je ovo okruženje kompleksno, ono nije i haotično okruženje u kome se delovi ponašaju nezavisno jedni od drugih, pošto okruženje ograničavanjem, iniciranjem i usmeravanjem utiče na elemente (agente)[66] sistema, dok istovremeno elementi utiču na sistem vlastitom funkcijom.

1.3. Predmet istraživanja

Predmet istraživanja ove disertacije je međunarodnopravna regulacija sukoba u sajber prostoru. Informaciono-komunikacione tehnologije su od ključnog značaja za sva društva i nacije. Njihova primena u vođenju sukoba je specifična, karakteristična i revolucionarna, a mogućnosti ostvarivanja vojnih efekata na cilj su sve značajniji. Efekti sajber napada po kvalitetu, više nego po kvantitetu, dostižu mogućnosti tradicionalnih formi sukoba koji se vode u fizičkom okruženju. Sredstva, kapaciteti i praksa razvoja vojnih sastava koji su namenjeni za izvođenje operacija u sajber prostoru u mnogim državama pokazuju da nacije doživljavaju vođenje sukoba u sajber prostoru kao značajnu pretnju, ali istovremeno i kao potencijal za ispoljavanje vlastite vojne moći pri ostvarivanju nacionalnih interesa. Sve veći broj država razvija institucionalne kapacitete, vojne strategije i doktrine za vođenje sajber ratovanja. Istovremeno, sajber prostor je već proglašen petim područjem izvođenja vojnih operacija u SAD, a u drugim državama se kao takav praktično i operativno prihvata. Sukobi u sajber prostoru i odbrana su predmet pregovora vodećih država i sporazuma vodećih vojno-političkih saveza. Sposobnost za vođenje sukoba u sajber prostoru dobija sve veći značaj, a priroda ove vojne aktivnosti postaje sve složenija. Istovremeno, pretnje iz sajber prostora koje ugrožavaju nacionalnu bezbednost i odbranu su višedimenzionalne i sve ozbiljnije, kao i posledice napada.

Međunarodno pravo oružanih sukoba reguliše opšte situacije ovih sukoba i primenjuje se na sve oblike agresije i primene sile između država. Ipak, priroda sukoba u sajber prostoru je specifična i zavisi od primenjenih informaciono-komunikacionih tehnologija. Ona se u velikoj meri razlikuje od tradicionalnih formi sukoba u fizičkom okruženju. S druge

[65] Peter Senge, *The Fifth Discipline: The Art and Science of the Learning Organization* (New York, NY: Currency Doubleday, 1990).

[66] Ključne elemente sistema u teoriji sistema.

strane, vrlo je slična nevojnim oblicima agresije u sajber prostoru, poput sajber špijunaže, terorizma i kriminala, što potvrđuje njena visoka tehnološka zasnovanost.

Sukobi u sajber prostoru se vode nevezano za stanje rata i mira. Sajber napade ne moraju preduzimati naoružani i uniformisani pripadnici vojnih jedinica, već i civili ili unajmljeni napadači. Ciljevi sajber napada često imaju civilnu ili dvostruku namenu. Napadi mogu imati trenutan ili vremenski odložen efekat. Napade u sajber prostoru je teško otkriti, napadače je još teže identifikovati i izvršiti njihovu atribuciju, što za posledicu ima otežano utvrđivanje odgovornosti države za sajber napad, kao akt agresije, u prihvatljivom vremenskom okviru.

U međunarodnoj zajednici ne postoji jedinstveni stav o prirodi sajber sukoba, niti o mogućem načinu njihove regulacije. Tri najveće međunarodne organizacije za bezbednost, odbranu i saradnju, NATO[67], Organizacija za evropsku bezbednosti saradnju (OEBS) i Šangajska organizacija za saradnju (ŠOS) imaju različite stavove o prirodi i pristupu regulisanju sukoba u sajber prostoru. One na različit način vide pretnje po odbranu iz sajber prostora, kao i primenu međunarodnog prava na agresiju iz sajber prostora. Takođe, u međunarodnoj zajednici ne postoji potreban nivo međusobnog poverenja između nacija po pitanju nacionalnih aktivnosti u sajber prostoru. Rezultat su česte međusobne optužbe za razne agresivne aktivnosti koje vodeće države međusobno preduzimaju jedna prema drugoj. Nivo globalne saradnje nije uspostavljen u dovoljnoj meri u sprečavanju agresivne primene sajber napada. Jedino u čemu se države slažu jeste stav o potrebi za što bržom izgradnjom kapaciteta za sajber odbranu i za preduzimanje obaveštajnih aktivnosti. Praksa primene sajber napada u međunarodnim okvirima je sve obimnija. Napadi su sve češći, imaju sve ozbiljnije posledice, a njihovi počinioci ostaju prikriveni.

U predmetu istraživanja koji se tiče primene prava na sukobe između država u sajber prostoru, utvrđivanje naučne istine predstavlja složen zadatak. Razloga za to ima više, a osnovni problemi se tiču otežanog normativnog formulisanja ključnih pojmova i

[67] Eng. *The North Atlantic Treaty Organization*

kategorija od značaja, izbora pogodnog metodološkog pristupa istraživanju, i same specifične, višedimenzionalne prirode sajber napada.

Problemi formulisanja ključnih kategorija od značaja nastaju kao posledica kompleksne prirode sukoba u sajber prostoru. Ta priroda je predmet istovremenog istraživanja više različitih naučnih disciplina, čije su osnovne metode istraživanja nesrodne. Ključne nauke i discipline za razmatranje sukoba u sajber prostoru se mogu svrstati u skup tehničkih, formalnih i društvenih nauka, koje primenjuju različite metode, tehnike i pristupe predmetu istraživanja. Konačno, zbog brze evolucije same prirode predmeta istraživanja (pod uticajem razvoja veštine i primenjenog znanja, odnosno tehnologije), značenje tih pojmova i kategorija se brzo menja u odnosu na vreme i okruženje. Stoga u oblasti sajber sukoba ne postoje kategorije čiji je sadržaj i oblik konačno formiran, nepromenljiv i trajno definisan.

Predmet istraživanja ove disertacije su tehnički orjentisana priroda sukoba u sajber prostoru i mogućnost njihove međunarodnopravne regulacije. Pristup istraživanju je multidisciplinarni, što se ogleda u analizi i sintezi iz ugla različitih naučnih disciplina i primenjenih veština od značaja za istraživanje predmeta istraživanja: prava, računarskih nauka, informaciono-komunikacionih tehnologija, informacione bezbednosti, vojne teorije i veštine, sociologije, političkih i organizacionih nauka.

1.4. Cilj istraživanja

Opšti cilj istraživanja je multidisciplinarna analiza elemenata sajber sukoba i njihova sinteza u cilju definisanja ključnih kategorija od značaja za istraživanje predmeta sajber ratovanja, kao i predlog modela njegove međunarodnopravne regulacije. Posebni ciljevi istraživanja su:

- sagledavanje pretnji od sukoba u sajber prostoru;
- utvrđivanje najvažnijih aspekata sukoba u sajber prostoru, vrste i sadržaja njegovih posebnih oblika;
- utvrđivanje tehnoloških specifičnosti, prirode i karakteristika sajber sukoba i ratovanja;

- analiza primenljivosti postojećeg sistema međunarodnog prava na sukobe u sajber prostoru;
- utvrđivanje mogućnost primene Međunarodnog prava oružanih sukoba na sajber ratovanje;
- obezbeđivanje osnove za buduća teorijska i praktična istraživanja u oblasti sukoba u sajber prostoru.

1.5. Hipoteze istraživanja

Opšta hipoteza istraživanja je sledeća:

Razvoj sajber ratovanja se ne može predvideti u dužem vremenskom periodu, niti se može regulisati primenom tradicionalnog Međunarodnog prava oružanih sukoba.

Posebne hipoteze su sledeće:

- Sajber ratovanje je specifičan koncept sukoba koji se po uzrocima, izvođenju i rešavanju značajno razlikuje od koncepata sukoba u fizičkom okruženju.
- Sajber ratovanje se ne može praktično i efektivno regulisati primenom međunarodnog prava oružanih sukoba po principu analogije sa tradicionalnim ratovanjem.
- Sajber ratovanje se primarno zasniva na upravljanju znanjem i na organizaciji strukture na nacionalnom nivou, a ne na posedovanju materijalnih resursa za vođenje borbe.
- Zbog tehnološkog ograničenja u primeni sajber ratovanja bez greške napadača nije moguće pouzdano otkriti tok i proces napada, identitet napadača i utvrditi odgovornost države za sajber napad.
- Neregulisana praksa sukoba u sajber prostoru ugrožava mogućnost za njegovu mirnodopsku primenu, i narušava odbranu i bezbednost svih nacija.
- Primena sajber napada u svrhu vođenja sukoba je karakteristična podjednako u stanju mira, kao i rata. Efektivno rešenje regulisanja sukoba u sajber prostoru mora imati sposobnost primene podjednako u stanju rata kao i u stanju mira.

– Zbog složene prirode i višedimenzionalnosti sukoba u sajber prostoru fokus naučnog istraživanja održivog modela njegove regulacije mora bit pomeren sa monodisciplinarnog na multidisciplinaran i interdisciplinarni pristup.

1.6. Metode istraživanja

Sukobi u sajber prostoru su realnost, iako se odvijaju u obliku koji se razlikuje od tradicionalnih sukoba, primenom drugačijih sredstava i metoda i vođeni su od strane karakterističnih učesnika. U tim specifičnim situacijama, formalna primena metoda koje se koriste u istraživanju tradicionalnih vrsta sukoba često ne predstavlja praktičan put do rešenja problema, niti je takav postupak dovoljan za ispitivanje predmeta istraživanja, ma koliko rigorozno se istraživači pridržavali formalnog pristupa i produbljivali područje svog istraživanja. S druge strane, područje koje sadrži mnoštvo nepoznanica i u kome nije izgrađen čak ni ontološki sistem kvalitativnih vrednosti podložno je čestim i značajnim greškama u zaključivanju. One lako mogu dovesti do rezultata koji nisu proverljivi, ponovljivi ili tačni. Takvi rezultati nemaju naučnu vrednost i ne mogu se primenjivati u naučnom postupku. Odbrana i bezbednost spadaju u grupu prioritetnih funkcija za svaku naciju. Od njih zavisi sam opstanak nacije. Naučno objašnjene jedne, specifične forme sukoba između nacija stoga je od kritične važnosti za sve pojedinačne subjekte međunarodne zajednice, uključujući i samu zajednicu. S obzirom na multidisciplinarnost pristupa u ovom istraživanju primenjeno je više naučnih metoda:

(a) **Analiza** prikupljenih informacija, definicija, stavova, modela i postojećih međunarodnopravnih konvencija, ugovora i sporazuma je primenjena tokom celog istraživanja. Poseban predmet analize su definicije ključnih kategorija i pojmova od značaja za sukobe, kao i odgovarajućih konvencija međunarodnog prava. Analiza je izvedena nad predmetom istraživanja kao celinom, po pojedinačnim svojstvima, u svim vremenskim periodima i po posebnim studijama slučaja. S obzirom na kompleksnu i međusobno zavisnu prirodu posebnih kategorija od značaja za sajber prostor, sajber napad i sajber ratovanje primenjena je eksplikativna analiza radi boljeg razumevanja sajber ratovanja, njegovog objašnjenja i otkrivanja pravilnosti i zakonitosti.

Za specifična posebna pitanja primenjena je parcijalna analiza:

- Analiza sadržaja je upotrebljena za istraživanje definicija, pisanih materijala, dokumenata i informacija. Cilj ove analize je razgraničavanje medijske predstave sajber sukoba od akademske (teorijske) i vojne (praktične).
- Strukturalna analiza predmeta istraživanja je primenjena za sagledavanje celokupnosti područja sajber bezbednosti pri utvrđivanju karakterističnih svojstava.
- Funkcionalna analiza je korišćena za utvrđivanje aktivnosti i odnosa (veza i međuzavisnosti) unutar predmeta istraživanja, kao i odnosa sajber ratovanja i njegovog šireg okruženja.
- Komparativna analiza je imala primenu u poređenju različitih definicija istog predmeta/fenomena a u cilju utvrđivanja ključnih svojstava sajber sukoba.
- Generička analiza primenjena je u istraživanju okolnosti nastanka i razvoja sajber ratovanja kao savremenog koncepta bezbednosti i odbrane država.

(b) **Apstrakcija** i **konkretizacije** su upotrebljene za razumevanje globalnog sistema sajber bezbednosti, povezivanja problema i karakteristika sajber ratovanja sa pravnim sistemima i primenom postojećih odredbi i pravila ratovanja na sajber ratovanje.

(c) **Specijalizacija** je korišćena u svim fazama istraživanja, a posebno u funkciji klasifikacije vrsta sajber napada i pojmova od posebnog značaja za istraživanje.

(d) **Induktivno–deduktivna metoda** je primenjena u toku i nakon analize sajber ratovanja za ocenu postavljenih hipoteza istraživanja i formiranje zaključaka neophodnih za ostvarivanje cilja istraživanja (utvrđivanje okolnosti i karakteristika neophodnog međunarodnog pravnog sistema regulacije sajber ratovanja i područja njegove primene na nacionalnom nivou).

(e) **Sinteza** rezultata istraživanja je primenjena prilikom multidisciplinarno orjentisanog definisanja prirode ključnih kategorija i pojmova.

(f) Metoda **studije slučaja** je primenjena u cilju prikupljanja podataka, analize i utvrđivanja najbolje prakse i trendova razvoja nacionalnih i međunarodnih modela sajber odbrane.

2. SUKOBI I RATOVI

Sajber sukob je, pre svega, sukob. Sukobi se ne posmatraju izolovano od ljudske prirode i interesa društvenih zajednica. Da bi se pravilno razumela priroda sajber sukoba, analiza treba da počne od karakteristika sukoba, kao inherentnog svojstva ljudske civilizacije, a ne od sajber prostora, kao tehnološkog koncepta postavljenog na osnovu društvenih odnosa.

2.1. Koncept međunarodnih sukoba

Sukobi između širih društvenih zajednica nastaju zbog nejednakosti u prirodi zajednica, razlika u dostupnim resursima i suprotstavljenih interesa. Karakter sukoba određuje mnoštvo elemenata, poput uzroka, učesnika, metoda i sredstava za vođenje sukoba, ciljeva i načina rešavanja sukoba. Sukobi kao društvena pojava su pratilac čovečanstva od njegovog nastanka i karakteristični element ljudske civilizacije. Po Gumploviču[68] i Milsu[69], ljudska civilizacije je oblikovana sukobima između društvenih grupa zbog interesa i resursa. Po Gumploviču[70], sve velike i složene društvene zajednice su nastale iz nekog sukoba.

2.1.1. Uzroci sukoba

Kao inherentna karakteristika svakog društva i čovečanstva, sukobi ne predstavljaju nužno znak nestabilnosti odnosa unutar ili između društvenih zajednica. Sukobi mogu imati i pozitivne karakteristike u odnosu na moć društvene zajednice, pre svega nacije: vode ka društvenim promenama, mogu da stimulišu inovacije i da jačaju moć centralnog autoriteta tokom izloženosti tradicionalnoj ratnoj pretnji koja dolazi izvan zajednice ili od dela zajednice[71].

[68] Ludwig Gumplowicz, *Outlines of Sociology*, trans. Frederick W. Moore, (New Yok, NY: Arno Press, 1975).

[69] Charles Wright Mills, *Power, Politics, and People: The Collected Essays of C. Wright Mills* (Oxford University Press, USA, 1963).

[70] Ibid.

[71] Lewis A. Coser, *The Functions of Social Conflict*. Vol. 9 (London, UK: Routledge, 1956).

Vard[72] tvrdi da uzroci sukoba unutar i između društvenih zajednica leže u samoj prirodi čoveka, iz koje se reflektuju na šire društveno okruženje. Takav stav potvrđuju antropolozi Šagnon[73], Haris[74], Feguson[75] i Sponsel[76], koji su decenijama odvojeno proučavali primitivno amazonsko pleme Jamomani, koje živi u konstantnom stanju rata sa drugim plemenima. Moguće je da su koreni sukoba i dublji, i da se nalaze u spremnosti inteligentnih primata na agresivno ponašanje[77]. Prateći najstarije istorijske izvore, može se zaključiti da ni jedan pripadnik ljudske vrste nije živeo u dobu u kome u nekom delu čovečanstva nije vođen sukob. Po Šou i Vongu[78], svega 8% ljudske istorije u prethodnih 3.400 godina je proteklo bez ratova. Po Kendeu[79], u periodu između 1945. do 1970. godine, u svetu je svakog pojedinačnog dana vođeno u proseku 10,49 ratova.

U skladu sa teorijom sukoba[80], moć je u osnovi svih društvenih odnosa, uključujući i odnose sukoba. Interesne grupe se bore međusobno da bi stekle preimućstvo jedne nad drugom u sukobu nad resursima. Po Koseru sukob predstavlja „borbu oko vrednosti i prava nad ograničenim statusom, moći i resursima u kojima je cilj svake strane u sukobu da neutrališe, onesposobi ili eliminiše rivala“ [81]. Kada dominantna grupa, koja raspolaže sa najviše moći od značaja za odnose među grupama, ostvari nadmoć nad ostalima,

[72] Citirano u James MacGregor Burns, Transforming leadership: A new pursuit of happiness, Vol. 213. Grove Press, 2003, 189.

[73] Napoleon A. Chagnon. "Life Histories, Blood Revenge, and Warfare in a Tribal Population," *Science* 239, no. 4843 (1988): 985-992.

[74] Marvin Harris, "Animal Capture and Yanomamo Warfare: Retrospect and New eEidence," *Journal of Anthropological Research* (1984): 183-201.

[75] R. Brian Ferguson, *Yanomami Warfare: A Political History* (Santa Fe, NM: School of American Research Press, 1995).

[76] Leslie E Sponsel, "Yanomami: An Arena of Conflict and Aggression in the Amazon," *Aggressive Behavior* 24, no. 2 (1998): 97-122.

[77] Jill D. Pruetz and Paco Bertolani. "Savanna Chimpanzees, Pan Troglodytes Verus, Hunt with Tools." *Current Biology* 17, no. 5 (2007): 412-417.

[78] R. Paul Shaw and Yuwa Wong, *Genetic Seeds of Warfare: Evolution, Nationalism, and Patriotism*, (Boston: Unwin Hyman, 1989). Nađeno u knjizi Chris Hedges, *What Every Person Should Know About War* (New York, NY: Free Press, 2003), 1.

[79] Istvan Kende, „Twenty-Five Years of Local Wars,“ *Journal of Peace Research*, 8, no. 1 (1971): 5-22. http://www.jstor.org/stable/422559 (preuzeto 15. avgusta 2015), 8.

[80] Teorija sukoba je sociološka teorija nastala sredinom ’50-tih godina dvadestog veka radom Luisa Kosera (Lewis Coser) and Ralfa Darendorfa (Ralph Dahrendorf), pod uticajem ideja Marksa, Vebera i Simela.

[81] Coser, *Functions of Social Conflict*, 10.

nastupa stabilnost u odnosima među grupama. Maks Veber[82] definiše moć kao sposobnost da se utiče na volju druge strane, čak i kada ima drugačije ciljeve. Po njemu, stabilnost društvene zajednice zavisi od odnosa autoriteta, koji su nosioci legitimne društvene moći u odnosu na stav većine i distribucije moći u zajednici. Kada se pod dejstvom unutrašnjih ili spoljnih faktora naruši verovanje većine u pravo autoriteta da bude nosilac legitimne političke moći (u savremenim društvima zasnovanom na pravnom sistemu društva) nastaje osnova za unutrašnji konflikt u zajednici.

Ostvarivanje nacionalnih ciljeva država u međunarodnoj zajednici je prirodan, ali i prinudan proces. Čak i ukoliko sukob ne postoji, u skladu sa ljudskom prirodom, postoji velika verovatnoća da će on nastati, ukoliko se ljudi i društvene organizacije nađu u okruženju koje ima ograničene resurse. Po teoriji antropologa Hardina[83] o "tragediji zajedničkog dobra" neograničen pristup opštem dobru od strane neke zajednice nužno vodi do njegove propasti usled nekontrolisane eksploatacije. U takvoj situaciji pojedinci nastoje da za sebe prigrabe resurse zajedničkog, neregulisanog i nezaštićenog dobra i brzo ih troše u međusobnoj konkurenciji.. Usled intenzivne eksploatacije nastaje neodrživa situacija u kojoj dolazi do propasti zajedničkog dobra na štetu svih. Poznati primer, svakako ne jedini, koji potvrđuje ovu teoriju je slučaj nestale civilizacije na tihookeanskim Uskršnjim ostrvima[84] koja je nestala usled konstantnog uništenja drveća eksploatacijom od strane konkurentnih klanova.

Po Hardinu, jedini način za očuvanje zajedničkih dobara je uspostavljanje centralnog suvereniteta koji se brine o zajedničkim interesima. Osnovni cilj zajedničke baštine čovečanstva je očuvanje prirodnih potencijala neke oblasti ili prostranstva za dobrobit celokupnog čovečanstva i sprečavanje njegovog uskogrudog i samovoljnog eksploatisanja od strane bilo koje pojedinačne države ili grupe država. Zato su usvojeni međunarodni sporazumi koji predstavljaju presek zajedničkih stavova čime obezbeđuju da se eksploatacija zajedničkih dobara vrši na dobrobit svih (većine) na globalno prihvatljiv način, odnosno da „ničija" i „svačija" prirodna dobra ne postanu predmet

[82] Isidor Wallimann, Nicholas Ch. Tatsis, and George V. Zito. "On Max Weber's definition of power."*Journal of Sociology* 13, no. 3 (1977): 231-235.

[83] Garrett Hardin, "The Tragedy of Commons" , *Science*, 162, no. 3859 (1968):1243-1248, http://www.sciencemag.org/cgi/content/full/162/3859/1243 (preuzeto 5. septembra 2015).

[84] Danas u sastavu države Čile.

otimačine i neetične eksploatacije. Taj proces se posebno odvija na nacionalnom nivou, pri čemu državna vlast odlučuje o balansu kontrole nad nekim resursom društva i slobodi pojedinaca. [85]

Jedan od najpoznatijih savremenih primera je sajber prostor, nad kojim ne postoji jedinstvena zakonska regulativa o nadležnosti zakona, već vladaju nacionalni zakoni sa ograničenim jurisdikcijama (u skladu sa unutrašnjim pravom i međunarodnim sporazumima na koje su se obavezale države) i sa različitom moći država da ostvare vlastite nacionalne interese u svim mogućim okruženjima sajber prostora: fizičkom, logičkom i informacionom. Međunarodnu regulaciju u velikoj meri zamenjuje zajednička tehničko-tehnološka organizacija, koja se ipak odnosi samo na jedan deo sajber prostora, Internet.

2.1.2. Način ispoljavanja moći u međunarodnim odnosima

Važan doprinos savremenoj analizi sukoba mogu dati rezultati naučne misli političkog realizma u međunarodnim odnosima iz sredine 20. veka. Po ovom pravcu, država je centralni oblik društvene organizacije, od ključnog uticaja na društvene odnose, pa i na razvoj specifičnih društvenih vrednosti, poput tehnologije. U osnovi društvenih odnosa, uključujući i sukobe, su objektivni zakoni čiji izvor se nalazi u ljudskoj prirodi. Može se zaključiti da su u svim slučajevima, uključujući i sukobe u sajber prostoru, uzroci sukoba uvek isti. Jedina razlika između navedenih vrsta sukoba su sredstva napada, agresije ili primene sile u sajber ratovanju, odnosno priroda sajber oružja i sajber napada. Akteri sukoba ispoljavaju svoje interese kroz sajber prostor primenom moći, na identičan način kao i u fizičkom okruženju.

Predstavnik političkog realizma[86], američki politikolog Morgentau, navodi: "I iznad svega, uvek imajte na umu da je ne samo politička neophodnost, već i moralna obaveza

[85] Nekada ta kontrola može imati ekstremni oblik, ali je ipak u interesu zajednice u skladu sa stavom centara moći. Na primer, ograničavanje rađanja u Kini je pokazalo značaj kontrole rađanja za održivi ekonomski napredak.

[86] Politički realizam (eng. *Political Realism*) je pravac u međunarodnim odnosima, političkim naukama i političkoj filozofiji, koji predstavlja teorijsko-metodološki koncept po kome je interes nacije vrhunski razlog preduzimanja akcija, a manifestacija moći je prirodan završetak svake političke akcije, na međunarodnom ili unutrašnjem planu. Predstavlja savremeni oblik opšteg pravca u međunarodnim političkim odnosima čiji su istaknuti oblici nemački *realpolitik*, italijanski *makijavelizam* ili opšti *pragmatizam*. Ključni principi političkog realizma, po Morgentau su: 1. Politika se rukovodi objektivnim zakonima (nepromenljivim i nezavisnim od političke svesti) koji imaju korena u samoj

nacije da u odnosima sa drugim nacijama uvek sledi jednu zvezdu vodilju, jedan standard u mislima, jedno pravilo za akciju: nacionalni interes"[87] Istorija je pokazala da nacije u međunarodnim, ali i unutrašnjim odnosima uvek preduzimaju svoje akcije u skladu sa vlastitom moći, kao i da je moć uvek centralni stub njihove politike.[88] Područje bezbednosti i odbrane je primarno pitanje za svaku naciju.[89] Ispoljavanje nacionalne moći u procesu ostvarivanja nacionalnih interesa između država je prirodan proces.[90]

Iako su postulati realizma kritikovani tokom novije istorije, istorijska praksa je potvrdila mnogo puta tačnost stavova ovog pravca o prioritetima nacionalnog interesa u kriznim vremenima u međunarodnoj zajednici kada je bezbednost nacija bivala ugrožena u velikoj meri.[91, 92] Na primer, savremeni politički predstavnici demokratskih društava teže za uspostavljanjem civilizacijskih vrednosti i okupljanjem društvenih zajednica oko tih vrednosti, poput deklarisanih kosmopolitskih vrednosti Ujedinjenih Nacija ili Evropske Unije. Multikulturalizam, jednakosti prava svih socijalnih slojeva društva, nacionalna, rodna i verska jednakost, humanost u odnosu na izbeglice iz drugih regiona, sloboda kretanja bez obzira na religijsko, nacionalno i socijalno poreklo i druge moralno prihvatljive ideje i stavovi su očit primer takvih vrednosti. Međutim, te vrednosti po pravilu ne važe u vreme sukoba između nacija, niti u vreme kriza. Istorija je pokazala da, kada je ugrožen neki segment nacionalne bezbednosti, ideje političkog realizma su gotovo

ljudskoj prirodi; 2. Nacionalni interes se uvek ostvaruje primenom nacionalne moći; 3. Nacionalna politika i akcije se uvek odvijaju u skladu sa nacionalnim interesima, koji su uvek promenljivi; 4. Apstraktni moralni principi ne mogu uspešno biti primenjeni u politici (uz napomenu da moralni principi mogu uticati na politiku u skladu sa njihovim značajem); 5. Moralni principi bilo koje nacije nisu univerzalni moralni principi (moralni principi bilo koje nacije ne mogu biti nametani svetu) i 6. Međunarodni odnosi predstavljaju samostalnu naučnu disciplinu, nezavisnu od politike.

Hans J. Morgenthau, *Politics Among Nations: The Struggle for Power and Peace*, Fifth Edition, Revised, (New York, NY: Knopf, 1978): 4-15, https://www.mtholyoke.edu/acad/intrel/morg6.htm (preuzeto 9. septembra 2015).

[87] Hans J. Morgenthau, *In Defense of the National Interest: A Critical Examination of American Foreign Policy* (New York, NY: Knopf, 1951).

[88] Morgenthau, *Politics Among Nations.*

[89] Morgenthau, *In Defense of the National Interest*, 241–242.

[90] Morgenthau, *Politics among nations*.

[91] Nacionalni interes se prvenstveno ogleda u osiguranju vladavine nacionalne moći kroz područje ekonomije i vojne sile da ostvari vlastite ciljeve u međunarodnim okvirima.

[92] To se ogleda u brzom reagovanju naoružavanjem, podizanjem vojne spremnosti, sklapanjem međudržavnih sporazuma sa drugim nacijama o odbrani u slučaju pretnje ratom, ekspresnim podizanjem granica radi zaštite vlastitog društva od političkih i ekonomskih izbeglica, uvođenjem diplomatskih, ekonomskih i političkih mera protiv onih država koje im ugrožavaju nacionalne interese i sličnim merama.

po pravilu preovladavale, a moralno prihvatljive ideje su odbacivane ili odlagane za drugo vreme, čak i po cenu narušavanja nacionalnog interesa nad moralnim vrednostima u svakom vremenu i svakom regionu sveta. [93, 94, 95, 96, 97, 98, 99, 100, 101]

U međunarodnim odnosima, u kojima države imaju centralno mesto, moć predstavlja sposobnost države da usmerava odluke i radnje drugih država. Po Frimenu[102], moć države potiče od njene snage i volje da je upotrebi u skladu sa sopstvenom strategijom, dok snaga nastaje transformacijom nacionalnih resursa u nacionalne sposobnosti. Ključne aktivnosti koje država koristi da manifestuje svoju moć su vođenje sukoba (primenom oružane sile),

[93] Asaf Hussain, Bill Law, and Tim Haq, *Engagement with Cultures: From Diversity to Interculturalism* (Leicester: University of Leicester, Institute of Lifelong Learning, 2006).

[94] U savremenim okolnostima, ti primeri se ogledaju u istupanju evropskih nacionalnih lidera u vreme finansijske krize u Evropskoj Uniji, poput izjava nemačke kancelarke Angele Merkel i britanskog premijera o nestanku ideje multikulturalizma u Evropi, u podizanju ograda na granicama evropskih država u cilju zaštite vlastite nacionalne bezbednosti od nekontrolisanog dolaska izbeglica iz regiona Bliskog Istoka u Evropu, u odbijanju mnogih evropskih država da prime migrante sa Bliskog istoka druge veroispovesti, u praktičnoj zabrani ulaska pripadnika neke nacije ili religije na teritoriju države pod izgovorom borbe protiv terorizma i sličnih.

[95] Ministerium für Inneres und Kommunales des Landes Nordrhein-Westfalen (Ministarstvo unutrašnjih poslova i lokalne uprave pokrajine Severne Vestfalije), "Bericht des Ministeriums für Inneres und Kommunales über die Übergriffe am Hauptbahnhof Köln in der Silvesternacht" (Izveštaj Ministarstva unutrašnjih poslova i lokalne uprave o napadima na Centralnoj stanici u Kelnu tokom Novogodišnje noći), 10. januar 2016,

http://www.mik.nrw.de/fileadmin/user_upload/Redakteure/Dokumente/Themen_und_Aufgaben/Schutz_und_Sicherheit/160111ssia/160111berichtmik.pdf (preuzeto 22. februara 2016).

[96] „Prosecutor: Most Cologne New Year's Suspects are Refugees", *Associated Press*, February 15, 2016, http://news.yahoo.com/cologne-prosecutor-majority-suspects-asylum-seekers-135156726.html (preuzeto 23. februara 2016).

[97] Matthew Weaver, „Angela Merkel: German Multiculturalism Has 'Utterly Failed," *The Guardian*, October 17, 2010 http://www.theguardian.com/world/2010/oct/17/angela-merkel-german-multiculturalism-failed (preuzeto 23. februara 2016).

[98] Laura Kuenssberg, "State Multiculturalism Has Failed, Says David Cameron," *BBC News*, February 5, 2011, http://www.bbc.com/news/uk-politics-12371994 (preuzeto 23. februara 2016).

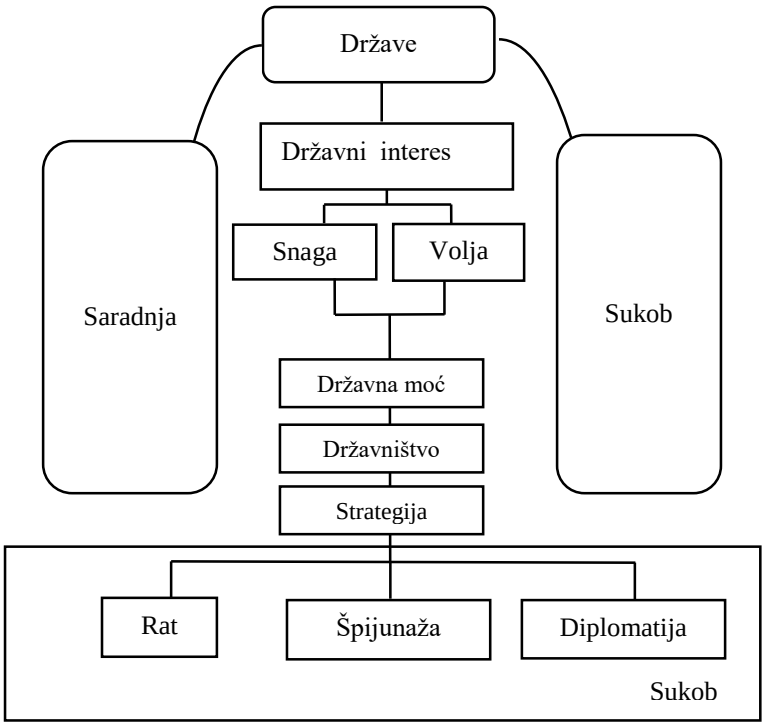
[99] „Migrants Crisis: Slovakia 'Will Only Accept Christians'," *BBC News*, August 19, 2015, http://www.bbc.com/news/world-europe-33986738 (preuzeto 23. februara 2016).

[100] „Growing Number of EU States Say They Prefer Non-Muslim Refugees," *Times of Israel*, September 8, 2015, http://www.timesofisrael.com/eu-states-increasingly-say-they-prefer-non-muslim-refugees/ (preuzeto 23. februara 2016).

[101] „Checkpoints, Physical Obstructions, and Forbidden Roads," *B'Tselem*, January 16, 2011, updated May 20, 2015, http://www.btselem.org/freedom_of_movement/checkpoints_and_forbidden_roads (preuzeto 23. februara 2016).

[102] Charles W. Freeman, Jr., *Arts of Power: Statecraft and Diplomacy* (Washington, DC: United States Institute of Peace, 1997), 3.

obaveštajnim aktivnostima (pribavljanjem i upravljanjem informacijama prikrivenim putem) i diplomatijom (ubeđivanjem, uticajem na svest i proces donošenja odluka).[103]



Slika 1. Šema modela ispoljavanja državne moći po Frimenu[104]

Nacionalna moć se ne ogleda isključivo u sposobnosti primene vojne sile na organizovan način uz upotrebu naoružanja.

Po Naju, državni ciljevi u međunarodnim odnosima se ostvaruju primenom kapaciteta „tvrde moći" (ekonomija i vojna sila), „meke moći" [105] (diplomatija, mediji, sajber prostor i međunarodni ugled) i „pametne moći"[106, 107] (kombinovanjem prethodna dva instrumenta u cilju optimalnog dejstva).[108] Osnovu moći nacije, takozvanu "tvrdu moć" čini sposobnost njene vojske (oružana sila) i ekonomije (sankcije i pritisak) da izvrši

[103] Charles W. Freeman, Jr., *Arts of Power*, 3-4.

[104] Ibid. Model je sačinjen na osnovu stavova autora.

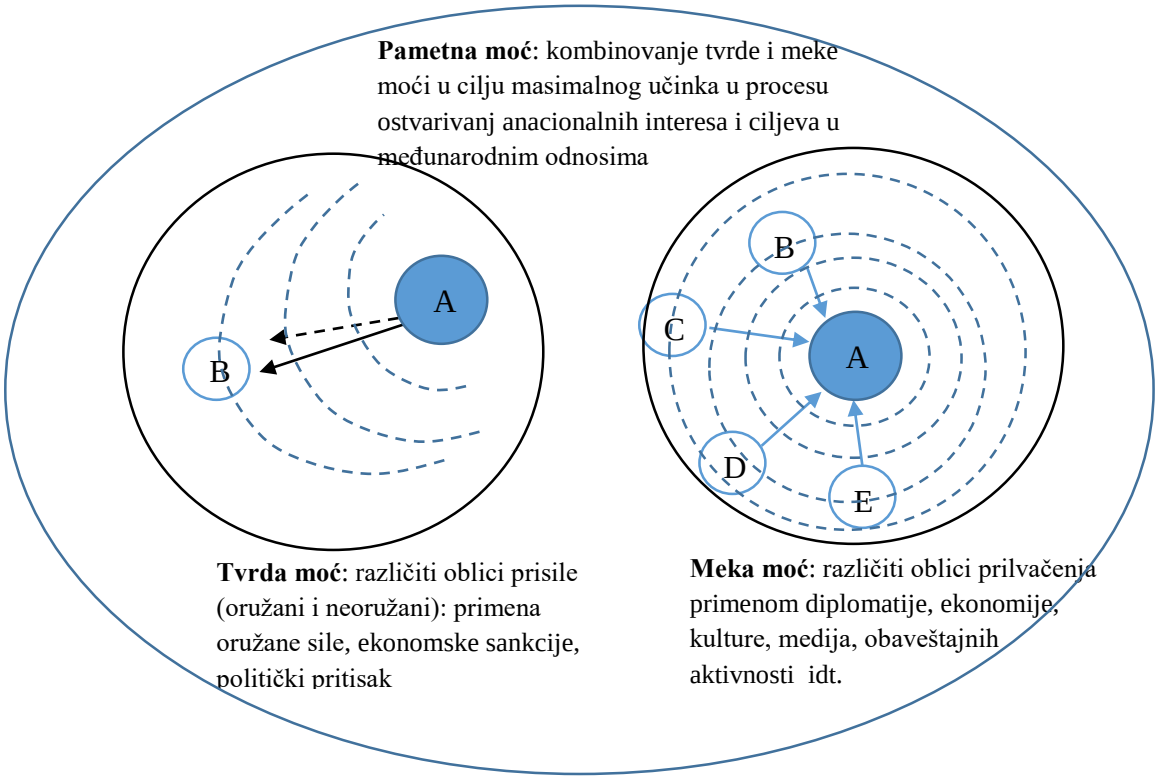
[105] Joseph S. Nye, „Soft Power," *Foreign policy* 80 (1990): 153-171.

[106] Center For Strategic & International Studies, *Smart Power Initiative*, http://csis.org/program/smart-power-initiative (preuzeto 5. septembra 2015).

[107] Joseph S. Nye, *The future of power* (New York, NY: PublicAffairs, 2011).

[108] Joseph S. Nye, „Combining Hard and Soft Power," *Foreign Affairs*, (July/August 2009), https://www.foreignaffairs.com/articles/2009-07-01/get-smart (preuzeto 5. septembra 2015).

željeni uticaj na okruženje prisilom u cilju ostvarivanja nacionalnih interesa. Koncept "meke moći" nacije čini sposobnost da ostvari interese i uticaj na okruženje privlačenjem, bez manifestacije prinude, primenom diplomatije, kulture, ekonomije, medijsko-informacionih aktivnosti i drugim odgovarajućim sredstvima.[109] Konačno, "pametnu moć" predstavlja sinhronizovana kombinacija "tvrde" i "meke" moći čime im se uzajamno pojačava dejstvo u ostvarivanju nacionalnih ciljeva. Pošto "pametna moć" predstavlja "pristup koji naglašava neophodnost postojanja jake vojske, ali takođe i jakog investiranja u sklapanje saveza, partnerstava i institucija na svim nivoima sa ciljem da se širi američki uticaj i uspostavi legitimnost američke akcije"[110] (u svetu).



Slika 2. Šema primene tvrde, meke i pametne moći po Naju[111].

[109] Nye, "Soft Power."

[110] Richard L. Armitage and Joseph S. Nye, Center for Strategic and International Studies (CSIS), *CSIS Commission on Smart Power: A Smarter, More Secure America*, http://csis.org/files/media/csis/pubs/071106_csissmartpowerreport.pdf (preuzeto 24. februara 2016).

[111] Ibid.

U pogledu primene sajber ratovanja, jasno je da se ono može upotrebi u svim navedenim područjima koje navodi Naj: kao meka moć (kroz diplomatiju, medijsko-propagandni uticaj i u sferi kulture u sajber prostoru), kao tvrda moć (kroz tehnički/fizički uticaj na protivničke sisteme i/ili njihovo uništenje primenom sajber napada) i kao pametna moć, kroz kombinaciju svih navedenih elemenata. Ključni faktor za ostvarivanje uticaja i efekata na sva tri nivoa je izgradnja osnove onoga što predstavlja logički nivo sajber ratovanja: ljudi, procesi i sistemi, sa svojim sposobnostima i ranjivostima.

Međutim, sukobi se razlikuju ne samo po područjima u kojima se vode, već i po vrsti i sadržaju dejstava između strana u sukobu, po intenzitetu agresivnih aktivnosti i njihovim posledicama. U tom pogledu može se utvrditi suštinska razlika između koncepta „sukoba“ i koncepta „ratovanja“ u međunarodnim odnosima.

2.1.3. Odnos sukoba i rata

Najagresivniji oblik sukoba je rat. U ratu strane u sukobu nanose štetu protivničkoj zajednici, njenim sposobnostima i resursima primenom oružane sile sa ciljem da je prisile da prihvati volju pobednika ili da dođe u stanje u skladu sa tom voljom. Iako rat predstavlja agresivnu primenu oružane sile nad drugom stranom, to nužno ne znači i da je primena oružane sile uvek i najefikasnije vođenja sukoba, niti da efikasnost primene sile zavisi isključivo od intenziteta i obima primene sile. Na primer, u okviru pravca koji je doveo do savremene vojne misli o potrebi i značaju izgradnje kapaciteta za sajber ratovanje u okviru Ministarstva odbrane SAD, često su citirane ideje drevnog kineskog vojnog stratega Sun Cua koji ističe značaj sveobuhvatnog sagledavanja situacije u kojoj se sukob odvija, vlastitih i protivničkih snaga, kao i značaja pravilne primene znanja i veština: „Stoga, boriti se i pokoriti u svim tvojim bitkama nije vrhovna odlika; vrhovna odlika se sastoji u slamanju neprijateljskog otpora bez borbe“[112]. Po Sun Cuu, ali i Klauzevicu, Makijaveliju i Žominiju, znanje, kako o vlastitim sposobnostima i stanju, tako i o neprijateljskom i o okruženju, je osnovni faktor za uspeh u svakom ratu.[113]

[112] Sun Tzu, *The Art of War*, trans. Lionel Giles, http://classics.mit.edu/Tzu/artwar.html.

[113] Sun Tzu, General Carl von Clausewitz, Niccolo Machiavelli, and Baron De Jomini, *The Complete Art of War* (New York: Start Publishing LLC, 2012).

U međunarodnom pravu ne postoji jedinstvena definicija rata. U međunarodnim odnosima, pojam „rat“ je u užem smislu shvaćen kao oružani sukob između dve ili više država/nacija koje su međusobno jedna drugoj zvanično objavile rat[114]. Međutim, opisana situacija sve manje odgovara praksi savremenih međunarodnih odnosa. Ratovi se formalno sve ređe zvanično objavljuju između država u sukobu, a strane u sukobu sve ređe su države. Ipak, rat ima svoje karakteristike koje ga bliže određuju.

Po Klauzevicu[115], rat je:

- nasilna aktivnost primene oružane sile, usmerena prema protivniku sa ciljem da mu se potčini volja prisiljavanjem da postupa po pobednikovoj zamisli;
- organizovana aktivnost koja se nikada ne izvodi samostalno, uvek je neophodna druga strana;
- sukob u kome suprotstavljene strane izvode recipročne akcije manifestacije sile nad protivnikom zbog čega rat stalno stremi ka ekstremnom intenzitetu i stanju neprijateljstva između protivnika;
- upotreba sile, simbolizovane u oružju i vojnim jedinicama;
- rat nije izolovana aktivnost, već je nastavak politike drugim sredstvima.

Po Klauzevicu, navedene karakteristike rata se nisu menjale nikada tokom istorije civilizacije i ratovanja. Međutim, od Klauzevicevog doba do danas, društvene okolnosti u kojima se vode ratovi su se značajno izmenile. U skladu sa njima, evoluirala je i priroda sukoba u odnosu na tradicionalnu formu klasičnog sukoba između dva „tabora“ zaraćenih država. Sve češće se dešavaju nove, specifične vrste oružanih sukoba:

- pobune dela stanovništva prema vladama;
- sukobi između etničkih i religioznih grupa ili političkih frakcija unutar država sa oslabljenom centralnom vlašću;

[114] Pojedini istraživači Una primer Ištvan Kende) smatraju da rat se rat može viditi između dva entiteta od kojih je najmanje jedan država, pri čemu ne mora biti formalno objavljen rat.

[115] Carl von Clausewitz, *On War*, trans. J.J. Graham (London, UK: Nicholas Trubner, 1873), Book I, Chapter 1, p. 18, http://www.gutenberg.org/files/1946/1946-h/1946-h.htm#link2HCH0001 (preuzeto 22. avgusta 2015).

- sukobi nadnacionalnih saveza protiv nenacionalnih teroristično-paravojnih grupa[116] i druge.

Tokom vremena izmenio se i pristup naučnog istraživanja uzroka i prirode ratovanja, idući od kvalitativne ka kvantitativnoj analizi sukoba. Tokom perioda Hladnog rata, veći broj istraživača i timova širom sveta je razvilo posebne okvire za utvrđivanje uzroka i karaktera rata na osnovu analize oružanih sukoba koji su se odigrali u dužem vremenskom periodu[117]. Kao rezultat njihovog rada razvijene su različite definicije rata u okviru utvrđenih oblika sukoba i u skladu sa kriterijumima po kojim se neki sukob može svrstati u ratne sukobe u skladu sa međunarodnim pravom. Iako su sve bile zasnovane na rezultatima empirijskih istraživanja, težište njihove metodologije se kretalo od kvantitativno-statističke analize do kvalitativno orjentisanih metoda sinteze i indukcije.
Mađarski istraživač sukoba, Ištvan Kende[118] je, u vreme vrhunca hladnog rata, na osnovu analize 97 ratnih sukoba u svetu, koji su vođeni u periodu od 1945. do 1969. godine, naveo sledeće kriterijume koje svaki oružani sukob treba da ispuni da bi imao status rata:

- borbe se izvode između najmanje dve oružane grupacije, od kojih bar jednu čine regularne vojne ili policijske snage neke države;
- na svakoj strani u sukobu mora biti prisutan određen stepen organizovane kontrole nad borbom od strane nadležnog centralnog autoriteta, čak i u slučaju kada se borba manifestuje isključivo radi odbrane ili jednostavnih dejstava;
- sukobi koji imaju karakter rata imaju kontinuitet u oružanom dejstvu, odvijaju se po jedinstvenoj strategijsko-taktičkoj zamisli i karakteriše ih organizaciona koherentnost između pojedinačnih aktivnosti[119], bez obzira na stepen sporadičnosti borbenih operacija, da li se operacije vode na vlastitoj teritoriji ili van nje i na vreme njihovog trajanja.

Već na prvi pogled može se uočiti da izbor i redosled kriterijuma koje je postavio Kende posebno podseća na specifične vrste oružanih sukoba koji su se odvijali u svetu u vreme

[116] Karakterističan primer za ove sukobe je rat u Avganistanu vođen između NATO i široke alijanse saveznika i grupacije Talibana sa terorističkom nadnacionalnom organizacijom Al-Kaida, zasnovanoj na sunitskom verskom fundamentalizmu.

[117] Singer sa Univerzitet Mičigen, Ištvan Kende, UPSALA, Hajdelberg Univerzitet, AKUF i drugi.

[118] Kende „Twenty-Five Years."

[119] Dakle, nije reč o sporadičnim i nezavisnim sukobima.

nastanka tih kriterijuma.[120] Međutim, daljom analizom se može uočiti da su navedeni kriterijumi jednako primenjivi i na savremene sukobe u informacionom dobu. Kende je pažljivo odabrao kriterijume prema njihovom odnosu na prirodu i suštinu univerzalnog koncepta rata, odbacujući one kriterijume koji se odnose na kvantitativno određenje rata. Ključni kvalitativni kriterijumi koje Kende uzima u obzir su: postojanje aktivnog oružanog dejstva regularnih snaga bar jedne države u sukobu, postojanje uređene organizacije borbenog delovanja i jedinstvene strategije, kao i postojanje povezanosti svih aktera na svakoj strani u sukobu. Nasuprot tome, izbegao je kriterijume poput mesta i trajanja sukoba, broja učesnika i žrtava.[121] Okolnost da li su oružani sukobi vođeni između unutrašnjih entiteta neke države ili između entiteta koji su u različitim državama nije od uticaja na odluku da li se radi o ratnom sukobu, već samo na klasifikaciju vrste sukoba.

Kendeova metodologija za praktično razlikovanje rata od ostalih oružanih sukoba je aktuelna i danas, široko je prihvaćena i poslužila je kao osnov za veliki broj naučnih dela, knjiga i istraživačkih projekata, uključujući i istraživanje *Radne grupe za istraživanje uzroka rata* (AKUF)[122] sa Hamburškog Univerziteta.[123] Ona je primenjiva i danas, na sukobe u sajber prostoru. Analizirajući kriterijume koje je postavio Kende, jasno je da je su ključni faktori koji dodatno razlikuju tradicionalne sukobe od sukoba u sajber prostoru:

- procena da li je sajber sukob oblik borbe između strana u sukobu;
- da li se može detektovati;
- da li se učesnici sukoba mogu identifikovati, i
- da li se može utvrditi državna odgovornost za preduzete sajber napade.

[120] Reč je o gerilskim, nacionalno-oslobodilačkim, revolucionarnim i kontrarevolucionarnim pokretima u postkolonijalnim društvima „Trećeg sveta“ u vreme „Hladnog rata“, tokom koga su dva velika vojno-politička bloka indirektno bila u sukobu podržavajući neku od strana u tim sukobima. Takođe, odnosi se i na, tada aktuelne, spoljne vojne intervencije velikih sila na unutrašnje društvene tokove malih zemalja u njihovom području interesa.

[121] Kao primer Kende navodi slučaj Arapsko-Izraelskog sukoba 1967. godine, koji je trajao svega šest dana i koji efektivno pokazuje da ne mora postojati direktna uzročno-posledična veza između trajanja, nivoa pretnje i posledica rata. Kende „Twenty-Five Years.“

[122] Arbeitsgemeinschaft Kriegsursachenforschung AKUF, http://www.wiso.uni-hamburg.de/en/fachbereiche/sozialwissenschaften/forschung/akuf/akuf/ (preuzeto 13. septembra 2015).

[123] Arbeitsgemeinschaft Kriegsursachenforschung (AKUF), „Definition and Typology of War,“ http://www.wiso.uni-hamburg.de/en/fachbereiche/sozialwissenschaften/forschung/akuf/akuf/kriegsdefinition-und-kriegstypologie/#c84532 (preuzeto 13. septembra 2015).

Pri tome, za ocenu prirode sukoba u sajber prostoru je od ključnog značaja pitanje koje se odnosi na samu primenu sile, odnosno oružane sile. U tom pogledu, odnosi sukoba se mogu kategorisati u nekoliko različitih oblika, koje se razlikuju po sadržaju, intenzitetu i nivou, kao što su borba, boj, bitka, rat, oružani sukob. S obzirom da se radi o pojmovima koji predstavljaju složene društvene fenomene, čiju genezu, tok i ishode nije moguće egzaktno kvantitativno predstaviti, za njihovo opisivanje i predviđanje manifestacije teško je utvrditi objektivne naučne zakonitosti. Iako su opšte poznati i široko prisutni, njihove pojedinačne definicije se razlikuju u odnosu na širi društveni i kulturni kontekst, kao i u odnosu na stavove iskazane od strane pojedinih istraživača, teoretičara i odgovarajućih nacionalnih dokumenata koji su se bavili njihovim fenomenima. U stručnom pogledu, njihove definicije su usvojene iz potrebe normativnog uređenja vojnih doktrina i strategija, i ne moraju nužno biti zasnovane na rezultatima naučnog istraživanja, već su stvar praktičnog pristupa i stručne konvencije.

Po Mačkiću, Milkovskom i Ostojiću, termin „oružana borba“ je izraz novijeg porekla, čije značenje je užeg karaktera od značenja pojmova „rat“ i „oružani sukob“, koji označava proces izvođenja borbenih dejstava upotrebom oružja i predstavlja „sukob dveju strana upotrebom oružja,…odnos dejstava u jednom sukobu“[124]. Po navedenim autorima, pojam „borba“ je opštijeg karaktera od pojma „oružana borba“ i ujedno je manje precizan po značenju. Značenje pojma „borba“ nije precizno i kreće se od osnovnog nivoa oružane borbe (na taktičkom nivou), ograničenog po vremenu, prostoru, broju učesnika i cilju, do apstraktnog koncepta procesa oružane borbe,[125] odnosno opšteg oružanog sukobljavanja između naoružanih snaga, bez obzira na veličinu, brojnost, ciljeve i pravni status[126]. Oružana borba je osnovni, ali ne i jedini sadržaj rata.

Pojmovi „boj“ i „bitka“ se po neposrednom cilju, obimu i nivou sukoba razlikuju, ali imaju i zajedničke karakteristike. Boj predstavlja nivo oružanog sukoba, odnosno oblik borbenih dejstava na taktičkom ili operativnom nivou, koji izvode vojni sastavi pod jedinstvenom komandom. U taktičkom pogledu, „boj“ je nivo oružane borbe koji je viši

[124] Ranko Mačkić, Vangel Milkovski, Miroslav Ostojić, „Međusobni odnos, razlike i uticaj pojedinih termina ratne veštine na rzvoj vojne doktrine“, *Vojno delo*, maj 2015, 265-276, 267.

[125] Ibid, 270.

[126] *Merriam-Webster*, s.v. “combat,“ http://www.merriam-webster.com/dictionary/combat (preuzeto 24. marta 2016).

od pojma „borba“ kada se on shvata u užem, specifičnom smislu. Bitka predstavlja najviši nivo oružane borbe,[127] dakle, predstavlja oružanu borbu na strategijskom nivou. Bitka, načelno, može obuhvatati više pojedinačnih borbi i bojeva.

U odnosu na boj, bitku, oružanu borbu i borbu, pojam „rat“ ima značenje stanja oružanog sukoba ili perioda njegovog vođenja između država ili između grupa unutar države[128], bez obzira da li je to stanje zvanično proglašeno (lat. *de iure*) ili je faktično (lat. *de facto*). Po Blekovom pravnom rečniku, rat predstavlja:

> „neprijateljski sukob sredstvima oružanih snaga, preduzet između nacija, država, ili vladara, ili nekada između strana unutar iste nacije ili države; period takvog sukoba;…stanje rata može takođe postojati bez oružanog sukoba; na primer, sporazum koji je formalno okončao stanje rata u Drugom svetskom ratu između Sjedinjenih država i Japana je potpisan sedam godina nakon što su borbe okončane 1945. godine“[129].

Po Bledšou i Bočeku, rat je:

> Status ili stanje oružanog neprijateljstva između dve ili više država. Rat nastaje bilo (1) formalnom deklaracijom; (2) ili aktima koje predstavljaju primenu oružane sile počinjenim od strane države ili grupe država protiv druge države ili grupe država sa impliciranom neprijateljskom namerom (ili bez takve namere, ali tretiran kao rat od strane te druge države ili grupe država); ili (3) aktima oružane sile između dve strane, dovoljno ozbiljnim i produženim do proglašenja rata, iako obe strane negiraju bilo kakvu neprijateljsku nameru…[130].

Dakle, rat je suštinsko stanje oružanog neprijateljstva, ili deklarisani status neprijateljstva, čak i ukoliko sami akti neprijateljstva primenom oružane sile ne postoje.

Što se u analizi oblika suprostavljenosti između strana dalje ide ka opštim oblicima, njihovo definisanje postaje sve teže, jer je i opseg njihovog značenja sve širi. Tako, na primer, sukob podrazumeva najširi mogući skup aktivne suprotstavljenosti, od nesaglasja, do samog vođenja rata. Po vrsti sredstava koje sukobljene strane koriste za neprijateljstva,

---

[127] Mačkić, Milkovski, Ostojić, „Međusobni odnos, razlike i uticaj pojedinih termina ratne veštine na rzvoj vojne doktrine“, 273.

[128] *Merriam-Webster*, s.v. “war,“ http://www.merriam-webster.com/dictionary/war (preuzeto 24. marta 2016).

[129] Black’s Law Dictionary, Ninth Edition, s.v. „war“, Bryan A. Garner, Editor in Chief, (St. Paul, US: West, Thompson Reuters, 2010), 1720.

[130] Robert L. Bledsoe and Boleslaw A. Boczek, The International Law Dictionary. (Santa Barbara, CA: ABC-CLIO, 1987), 343.

sukobi mogu biti oružani i neoružani. Po Kendeu, rat je oblik oružanog sukoba koji uključuje angažovanje naoružanih snaga neke vlade, kome se suprotstavlja nekakav oblik organizovane borbe suprotstavljene strane i uz određeni kontinuitet u oružanim borbama.[131] Dakle, sukob je šireg karaktera od rata, koga karakteriše intenzivna upotreba oružane sile, i predstavlja primenu i drugih, neoružanih oblika neprijateljstva koji se izvode sa istim ili sličnim ciljem kao i oružani sukobi.

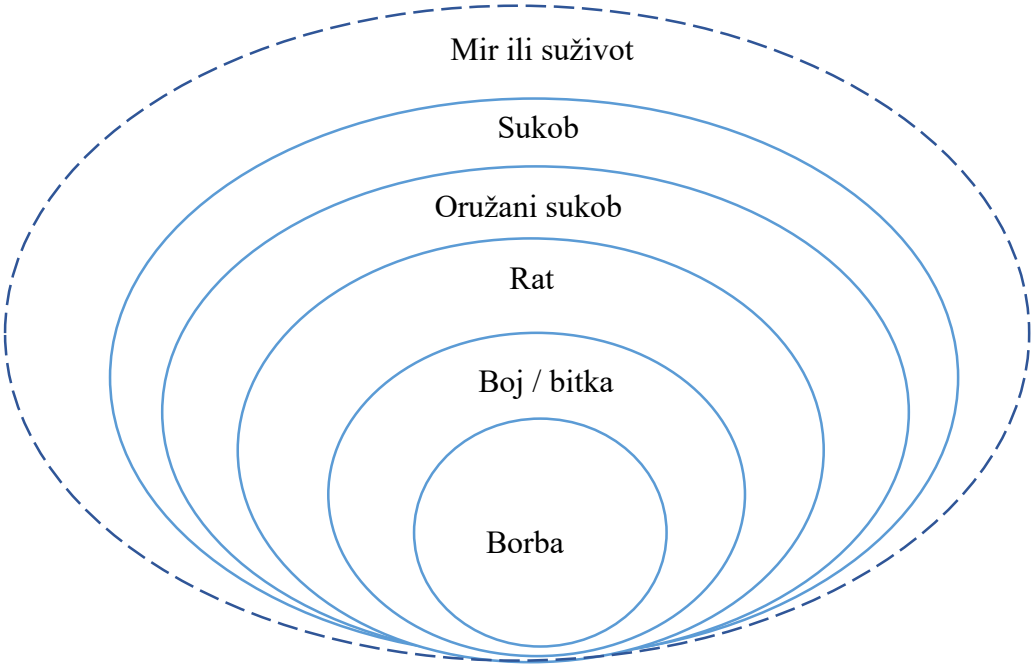
Na osnovu dosadašnje vojne prakse i društvenog iskustva na praćenju dosadašnjih sukoba i ratova, opšte je prihvaćeno stanovište da (organizacione) forme ispoljavanja sile u međunarodnim odnosima stoje u sledećem međusobnom odnosu (Slika 3):

- borba je neposredna primena oružane sile između strana u sukobu;
- boj i bitka su vojni pojmovi i predstavljaju viši stepen organizacije strana u oružanom sukobu;
- rat je širi pojam, koji se sprovodi u dužem vremenskom periodu i u kontinuitetu, pri čemu nije neophodno da bude međunarodnopravno deklarisan, i čiji osnovni, ali ne jedini sadržaj je oružana borba;
- oružani sukob je širi pojam od rata, koja se od rata razlikuje u skladu sa ispunjenošću principa i uslova koje rat mora da ispunjava, na primer, po trajanju, intenzitetu, odnosno okolnosti da li bar jedan učesnik oružanog sukoba ima međunarodnopravni subjektivitet; Međunarodno pravo oružanih sukoba se primenjuje i na rat i na oružani sukob, jer ih oba karakteriše upotreba oružane sile, pri čemu je uslov subjektivitet učesnika sukoba;
- sukob je najširi oblik suprotstavljanja agresijom ili primenom sile između dva ili više međunarodnopravnih subjekata, koji može obuhvatati oružane i neoružane oblike primene sile, pri čemu se Međunarodno pravo oružanih sukoba odnosi samo na oružane oblike primene sile, i
- stanje mira ili suživota u kome nema sukoba, ali u kome postoje odnosi konkurencije interesa, netrpeljivosti između subjekata i suprotstavljenih stavova i pozicija.

Ključna razlika između navedenih formi neprijateljstava u međunarodnim odnosima je ona između rata, oružanog sukoba i sukoba. Načelno, svi ovi oblici imaju isti cilj i mogu

[131] Frank Barnaby, "Arms and the Third World."*New Scientist,* 7 April, vol. 74 no.1046 (1977): 30-31.

se ostvariti u istoj perspektivi. Takođe, mogu se odvijati u unutrašnjim ili međunarodnim odnosima. Ipak, oni se razlikuju po intenzitetu, sadržaju i obimu, što ih čini različitim u pogledu primene Međunarodnog prava oružanih sukoba.



Slika 3. Odnos organizacionih formi sukoba u međunarodnim odnosima

Sukob predstavlja najširi oblik neprijateljstva između politički nezavisnih faktora. On se može manifestovati u jednom području delatnosti ili u više njih istovremeno (na primer, vojni, ekonomski, politički, rasni, religijski, etnički, politički, revolucionarni ili opšti društveni sukob). Sukobi mogu biti ograničeni po trajanju ili postojani u dugom vremenskom periodu, čak vekovima. Sukobi ne moraju nužno biti ostvareni na nacionalnom ili međunarodnom nivou, već se mogu manifestovati i u okviru specifičnih društvenih grupa, bez obzira na stepen njihove kohezije. Po Nikolsonu[132], u svim tim slučajevima sukob predstavlja rezultat nastojanja strana u sukobu da ostvare sopstvene interese i predstavlja svesno nastojanje svake strane da se uzrok sukoba reši putem

[132] Nicholson, Michael. *Rationality and the analysis of international conflict*. Vol. 19. Cambridge University Press, 1992, 12.

manifestacije neprijateljstva, nanošenjem štete drugoj strani. Međutim sukob može biti sporadičan, neorganizovan od strane organa centralne moći. Sukob se ne odvija nužno na međunarodnom nivou, već može i na organizacionom, čak i na grupnom i individualnom. S druge strane, rat podrazumeva organizovanu pripremu društvene zajednice da ga vodi. Na primer, u svakom društvu se pred rat izvode vojne pripreme, donose specifični zakoni, vrši se mobilizacija trupa, priprema vojnih jedinica i naoružanja. Po Rumelu[133], koncept sukoba je multidimenzionalan, pa stoga razvija mnoštvo različitih oblika. Rumel definiše sukob kao „balansiranje vektora moći, sposobnosti da proizvode efekte“[134]. Sukob ne nastaje trenutno, on ima svoje izvore i uzroke, kao i proces u kome se generiše i manifestuje. U tom procesu svaka strana preduzima korake koji zavise od ponašanja druge strane. Dakle, sukob je proces u kome se suprotstavljene strane takmiče međusobno u suprotstavljenom odnosu pri ostvarenju vlastitih interesa, primenom sopstvene moći. U pogledu posmatranja sukoba kao balansiranja moći, Rumel razlikuje tri karakteristike sukoba: mogućnost, raspolaganje i manifestaciju.[135] U tom pogledu, sukobi u sajber prostoru se lako mogu razumeti. Oni nisu linearni, odnosno ne nastaju isključivo kao posledica sukoba interesa između međunarodnih aktera, koji se rešavaju primenom sile, odnosno manifestacijom moći nad protivnikom u sajber prostoru. Više nego u drugim područjima, sukobi u sajber prostoru zavise od mogućnosti napadača da napadne drugu stranu. Ta mogućnost je sadržana u stalnom postojanju ranjivosti informacionih sistema u sajber prostoru. Druga strana može raspolagati sa sposobnošću da iskoristi te ranjivosti, ali tu sposobnost ne mora manifestovati. Napadač u sajber prostoru stoga može biti ona strana koja ima sukobljene interese sa napadnutom stranom, ali i ona koja nema sukobljene interese, ali poseduje sposobnost da izvrši napad (ukoliko je stekla informacije o postojanju ranjivosti druge strane i znanje kako da ih efektivno iskoristi). Sukob u sajber prostoru se manifestuje kada se spoje ranjivosti i sposobnosti za izvođenje napada. Pri tome, složenu prirodu sukoba u sajber prostoru stvara tehnička mogućnost napadača da njegove napadačke aktivnosti ostanu prikrivene.

[133] Rudolph Rummel, Understanding Conflict and War, Vol. 2, The Conflict Helix, Beverly Hills, California, Sage Publications, 1976. https://www.hawaii.edu/powerkills/TCH.CHAP26.HTM

[134] Ibid.

[135] Ibid.

Po intenzitetu, oružani sukob predstavlja najintenzivniju formu sukoba. Sukob sadrži oružane i neoružane oblike ispoljavanja sile ili agresije, a oružani sukob se može voditi između grupa koje nemaju međunarodnopravni subjektivitet, pa se u tom području nalazi i granica primene međunarodnog prava. Stoga, u cilju određivanja šta je rat, a šta oružani sukob i sukob, od značaja može biti analiza ratnih sukoba Kendea.

Međutim, treba biti obazriv, jer je Kende naveo razliku između oružanog sukob i rata, a ne između svakog sukoba i rata. Po njegovom mišljenju, rat je oružani sukob koji:

- se vodi između oružanih grupacija (što nije relevantno za problem sajber ratovanja, jer sajber napade mogu izvoditi i neoružane grupe);
- najmanje jedna strana mora biti u nadležnosti države, a organizovana kontrola snaga mora biti prisutna na svakoj strani, na planiran i koherentan način i u kontinuitetu (u ovom uslovu postoji prikriveni problem identifikacije i atribucije sajber napadača, kao i utvrđivanja odgovornosti države za sajber napad), i
- nisu uslovljeni trajanjem i mestom sukoba[136] (što u potpunosti odgovara prirodi sajber ratovanja).

Dakle, da bi neki sukob u sajber prostoru bio podložan primeni Međunarodnog prava oružanih sukoba, mora ispuniti sledeće uslove:

- mora biti oblik primene sile;
- mora ugrožavati teritoriju i suverenitet države, i
- mora biti organizovan, planiran ili naručen od strane ili u ime države protiv nekog drugog entiteta međunarodnog prava (obrnuto nije slučaj, jer je u tom slučaju takav napad kriminalni akt, a ne oružani sukob).

[136] Kende „Twenty-Five Years.“

3. SAJBER PROSTOR I NJEGOVI SLOJEVI

"Mašta je jedino oružje u ratu protiv stvarnosti"
Žil de Gotije[137]

Primena informaciono-komunikacionih tehnologija je kvalitativno unapredila način funkcionisanja ljudskog društva.[138] Ne postoji područje delatnosti čovečanstva u kome njihova primena ne omogućava poboljšanu efektivnost, efikasnost, optimizaciju ili nove mogućnosti. Drastično unapređujući način komunikacije, rada, razmene, obrazovanja i drugih odnosa između ljudi, smanjivanjem razlika u vremenu, prostoru i dostupnosti informacija, servisa i sadržaja, informaciono-komunikacione tehnologije su jedan od ključnih razloga i faktora za nastanak globalizacije u svetu[139]. Neposredno su omogućile stvaranje koncepta informacionog društva,[140] koji je od značaja za sve funkcije savremenog društva, a posebno za bezbednost i odbranu.[141] Sajber ratovanje u opštem smislu predstavlja ratovanje u sajber prostoru. O pojmu „ratovanje" postoje brojni koncepti, definicije i teorije, kao i stručne materije, što nije slučaj sa pojmom „sajber prostor", posebno kada se ima u vidu potreba za njegovim preciznim definisanjem u pogledu međunarodnog prava. Zbog toga ova jednostavna definicija sajber ratovanja zahteva obiman postupak definisanja sajber prostora. Ipak, iako zahtevan, ovakav pristup je praktičan, jer definisanje značenja sajber ratovanja svodi definisanje sajber prostora, odnosno na njegov tehnološki i društveni kontekst. Stoga ovakav pristup analizi ratovanja sajber ratovanja ima potencijal da duže traje, uprkos dinamičnoj promeni njegove prirode, uz istovremeno redukovanje svih drugih faktora koji se vremenom mogu značajno promeniti, dozvoljavajući uključivanje i novih faktora koji mogu doći sa budućim

[137] Fra. *Jules de Gaultier*.

[138] Robert Lee Konsbruck., *Impacts of Information Technology on Society in the New Century* (2002), 1-6.

[139] Manuel Castells, "Information Technology, Globalization and Social Development," United Nations Research Institute for Social Development (UNRISD) Publications, 114 (September 1999): 1-23, http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?id=29033 (preuzeto 11. novembra 2015.).

[140] Frank Webster, *Theories of the Information Society*, (Abingdon, UK: Routledge, 2006), https://cryptome.org/2013/01/aaron-swartz/Information-Society-Theories.pdf

[141] "Strategic Culture: The Impact of Technology on the Military", *7th International Security Forum (ISF)*, Panel chaired by Stephanie Neuman, speakers Stephen Biddle, Jack Treddenick, Kenneth W. Estes, Center for Security Studies (CSS), (Zurich, Switzerland: April 2007), http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?id=30882

razvojem tehnologije, na primer, uključivanje primene sistema veštačke inteligencije u proces vođenja sukoba u sajber prostoru.

3.1. Značenje pojma „sajber“

Iako je uticaj informaciono-komunikacionih tehnologija na celokupno čovečanstvo očigledan i revolucionaran, on je teško kvantitativno merljiv, posebno u opštem smislu. Razlog za to su kompleksnost i širina njihove specifične i opšte primene. Jedan od mogućih posrednih pokazatelja rasta značaja informaciono-komunikacionih tehnologija za savremeno čovečanstvo je analiza učestalosti svakodnevne upotrebe njihovih karakterističnih lingvističkih simbola (reči). Ključni izraz u vezi sa primenom informaciono-komunikacionih tehnologija koji prati ceo njihov razvoj je izraz „sajber“ (eng. *cyber*). Navedeni izraz istovremeno ima svojstvo reči[142], morfeme[143] i lekseme[144] i predstavlja ključni konceptualni simbol savremene upotrebe informaciono-komunikacionih tehnologija u svim oblastima, uključujući i bezbednost i odbranu. Nastao je u kulturi američke nacije, na engleskom jeziku,[145] na osnovu etimološkog korena iz

[142] Reči su glasovni skupovi (i pojedinačni glasovi) (jezičke jedinice) koji imaju određeno leksičko i gramatičko značenje značenje i funkciju (sintaksičku službu). Kao takve, reči su oznake pojmova. Živojin Stanojčić, Ljubomir Popović, Gramatika srpskog jezika, Zavod za udžbenike, Beograd, 1989.

[143] U lingvističkom smislu, morfema je najmanja gramatička jedinica u jeziku koja ima gramatičko značenje. Morfema „sajber“ je korenska (leksička) morfema, kao najmanja jezička jedinica koja je nosilac pojedinačnog (leksičkog) značenja.

[144] Najmanja samostalna leksička jedinica koja obuhvata sva značenja i oblike te reči.

[145] Koncept sajber prostora je nastao u SAD, kao projekat agencije Ministarstva odbrane SAD – ARPA (kasnije DARPA) i odatle se evolucijom razvio i njegova primena i upotreba se proširila na ceo svet u relativno kratkom periodu vremena zajedno sa razvojem i primenom informaciono-komunikacionih tehnologija.

starogrčkog jezika[146] iz koga se u transliterovanom obliku[147] proširio na sve savremene jezike sveta, [148] uključujući i srpski[149]. Zbog univerzalne upotrebe, za njega se može reći da je jedna od najpoznatijih savremenih internacionalističkih leksema[150], koja ima jedinstveno (opšte) značenje i isti oblik u svakom jeziku, naciji i delu sveta. Po statistici specijalizovanog internet servisa za pretraživanje termina u štampanim izvorima, servisu *Google Ngram Viewer*, učestalost pojavljivanja termina „cyber" na engleskom jeziku u periodu od 1985. do 2008. godine se povećala 129 puta. [151] Broj objavljenih članaka u čijem nazivu je termin „cyber" u bazi podataka naučnog agregatora i pretraživača naučnih, akademskih i stručnih radova *ProQuest*, koji su objavljeni u periodu 1980-1989

[146] Termin „sajber" vodi poreklo od etimološkog korena starogrčke reči *kibernetikos* (*κυβερνητικός*), sa značenjem upravljati, rukovoditi ili kormilariti. *Merriam-Webster Online Dictionary*, s.v. „cyber," http://www.merriam-webster.com/dictionary/cybernetic;

Iako je navedena reč upotrebljavana u smislu označavanja procesa upravljanja još u antičkoj Grčkoj, u novije doba, matematičar Andre-Mari Amper je prvi upotrebio reč „kibernetika" (fr. *cybernétique*) u eseju *Essai sur la philosophie des sciences*, u kontekstu upravljanja građanskim društvom. H.S. Tsien, Engineering Cybernetics, Preface vii, 1954 McGraw Hill.

Intenzivno je počeo je da se koristi u području izučavanja kibernetike (*Cybernetics*), nove naučne discipline koja se bavi automatskim upravljanjem sistemima u živom svetu i mehanici, i u njihovoj međusobnoj interakciji, čiji je formalni predvodnik bio matematičar i fizičar Norbert Viner (*Norbert Wiener*), *Cybernetics: or Control and Communication in the Animal and the Machine, The M.I.T. Press,* 1948); U modernu upotrebu ga je uvela grupa američkih autora iz popularno-kulturnog žanra naučne fantastike poznatog pod nazivom sajber pank (*cyberpunk*) pominjanjem u sledećim novelama i kratkim pričama: *Web of Angels* (Džon M. Ford [*John M. Ford*], 1980, *Tor Books*), *True Names* (Vernor Vindž [*Vernor Vinge*], 1981, *Dell*), *Burning Chrome* (Viliam Gibson [*William Gibson*], 1982, *Omni*) i *Neuromancer* (Viliam Gibson, 1984, *Ace*).

[147] Pošto je specifičan, nov, i ne postoji drugi sličan pojam koji opisuje njegovu predmetnu oblast.

[148] Fredrik Hull and Gin Sivanesar. "Introducing Cyber." *Journal Of Business Continuity & Emergency Planning* 7, no. 2 (2013): 97-102, EBSCO*host* (preuzeto 13. junara 2016).

[149] Reč „sajber" je sasvim opravdani anglicizam (reč koja je u srpski jezik došla iz engleskog jezika), kako u srpskom, tako i u drugim jezicima, jer pre njene pojave nije postojala adekvatna reč u tim jezicima.

[150] U nemačkom i slovenskim jezicima (uključujući i srpski jezik), pored morfeme „sajber" u upotrebi je njen morfološki dublet „kiber", koji ima isto etimološko poreklo, kao i značenje, a razlika u obliku mu potiče iz pravila da se transliterovane strane reči čiji koren potiče iz trećih (obično neživih) jezika izgovaraju u skladu izgovorom originalne reči porekla (*kibernetikos* ~ kiber). Međutim, u slučaju reči „sajber", zbog intenzivne i obimne upotrebe na globalnom nivou, koje se povezuje sa mestom njegovog nastanka i njegovim značajem za informaciono-komunikacione tehnologije u čijem slučaju gotovo sve reči imaju poreklo iz engleskog jezika, leksičko značenje ima veći značaj od gramatičkog. Između ostalih, to je jedan od razloga što je navedena reč u kratkom vremenu, kao retko koja druga, dobila identično univerzalno značenje i izgovor u globalnim razmerama.

[151] Google Books, nGram Viewer, https://books.google.com/ngrams/graph?content=cyber&year_start=1800&year_end=2008&corpus=15&smoothing=3&share=&direct_url=t1%3B%2Ccyber%3B%2Cc0 (preuzeto 22. decembra 2015).

iznosi 4.517, dok u periodu 2010-2016 taj broj iznosi 189.024, što predstavlja povećanje od 42 puta.[152]

Takva primena se posebno favorizuje u okviru Ministarstva odbrane SAD i Vojske SAD, ali sa vrlo racionalnim razlogom.[153, 154] Izraz „sajber“ je sastavni deo složenog pojma „sajber prostor“ (eng. *cyberspace*).

Slika 4. Učestalost termina „cyber“ u periodu od 1800 do 2008. godine u štampanim izdanjima na engleskom jeziku. Google Books, nGram Viewer [155]

Oba termina se u savremenoj upotrebi koriste za označavanje novog, posebnog područja u praksi računarskih nauka i primene informaciono-komunikacionih tehnologija u raznim oblastima, uključujući i vođenje vojnih operacija i drugih aktivnosti.[156, 157, 158]

[152] Preuzeto 17.01.2016. godine sa pretraživača ProQuest, http://search.proquest.com

[153] Ibid.

[154] Michael N. Schmitt, ed., *Tallinn Manual On The International Law Applicable to Cyber Warfare,* (Cambridge, Cambridge University Press, 2013), 2011, preuzeto sa http://issuu.com/nato_ccd_coe/docs/tallinnmanual

[155] Google Books, nGram Viewer, https://books.google.com/ngrams/graph?content=cyber&year_start=1800&year_end=2008&corpus=15&smoothing=3&share=&direct_url=t1%3B%2Ccyber%3B%2Cc0 (preuzetp 22. decembra 2015).

[156] „War in the Fifth Domain,“ *The Economist.*

[157] *Information Operations, Joint Publication 3-13*. Washington, DC: U.S. Joint Chiefs of Staff, 2014, preuzeto sa http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf

[158] *Cyberspace Operations: Joint Publication 3-12*. Washington, DC: U.S. Joint Chiefs of Staff, 2013, preuzeto sa http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf

Takođe, široko se upotrebljavaju u cilju ontološkog i semantičkog formiranja više odgovarajućih naziva pojmova u vojnoj primeni: „sajber ratovanje“ (eng. *cyber warfare*), „sajber rat“ (eng. *cyber war* ili *cyberwar*), „sajber sukob“ (eng. *cyber conflict*), „sajber napad“ (eng. *cyber attack*) „sajber oružje“ (eng. *cyber weapon*) i drugih. Uvođenjem jednog pojma (sajber) u jedno novo operativno okruženje zasnovano na tom pojmu (sajber prostor) najlakše se harmonizuje ceo postojeći skup vojni pojmova, aktivnosti, radnji između tradicionalnog sukoba (u fizičkom okruženju) i sukoba u sajber prostoru. U suprotnom, potrebno je uvesti u potrebu i univerzalno usvojiti potpuno nova značenja i definicije pojmova vezanih za sajber prostor, od kojih bi se mnoge po svojoj prirodi drastično razlikovale od odgovarajućih tradicionalnih, zbog specifične prirode sajber prostora. U vojnom okruženju, s obzirom na značaj i moguće posledice, uvek je neophodno precizno i standardizovano izražavanje i jasno razlikovanje pojmova i termina.

3.2. Poreklo sajber prostora

Izraz „sajber prostor“ je nastao i razvijao se u SAD, paralelno sa razvojem i primenom računarskih nauka i informaciono-komunikacionih tehnologija. Prvo javno upotrebljavano značenje izraza „sajber prostor“ razvili su književni, filmski i strip umetnici, kao umetnički i filozofski koncept, u okviru specifičnog, tehnološki orjentisanog, podžanra naučne fantastike, pod nazivom „sajber pank“ (eng. *cyberpunk*)[159] u periodu od šezdesetih do kraja osamdesetih godina dvadesetog veka.[160] Umetničko-filozofska predstava sajber prostora je obuhvatala konceptualno „virtuelno“ okruženje, sačinjeno od digitalnih podataka.[161] Međutim, bilo bi pogrešno smatrati da su umetnici zaslužni za stvaranje i postojanje sajber prostora. Priroda sajber prostora se ne može

[159] „Cyberpunk as a Science Fiction Genre,“ *Information Database, The Cyberpunk Project*, stranica poslednji put modifikovana 12. jula 2004, http://project.cyberpunk.ru/idb/scifi.html (preuzeto 8. novembra 2015).

[160] Annelee Newitz, „The Bizarre Evolution of the Word “Cyber”,” *io9 Gizmodo*, 16. Septembar 2013, http://io9.gizmodo.com/today-cyber-means-war-but-back-in-the-1990s-it-mean-1325671487 (preuzeto 8. Novembra 2015).

[161] Scott Thill, “March 17, 1948: William Gibson, Father of Cyberspace,” *Wired*, March 17, 2009, http://archive.wired.com/science/discoveries/news/2009/03/dayintech_0317 (preuzeto 9. novembra 2015).

pravilno razumeti bez uključivanja vojnog elementa, odnosno mimo uticaja faktora nacionalne bezbednosti i odbrane.

Pregledom postojećih baza podataka termina koji se odnose na pojmove sa prefiksom „sajber“, lako se uviđa da su dokumenti koji se odnose na područje bezbednosti i odbrane izvori većine definicija pojma „sajber prostor“ koji su u zvaničnoj upotrebi na nacionalnom nivou ili u relevantnim međunarodnim organizacijama.[162, 163, 164, 165]

Između sajber prostora i vojnih aktivnosti od početka postoji suštinska povezanost. Informaciono-komunikacione tehnologije, uključujući računare, računarske mreže i sajber prostor, koji je nastao njihovim umrežavanjem, inicijalno su razvijene baš za potrebe vojske i odbrane, u SAD i Velikoj Britaniji.[166, 167, 168] Internet, početna osnova i najveća globalna mreža u konceptu koji se danas naziva „sajber prostorom“, tehnički je razvijan i kreiran u periodu od kraja šezdesetih do početka devedesetih godina 20. veka u više projekata, kojima je u osnovi bio projekt ARPANET Ministarstva odbrane SAD[169],

[162] NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), *Cyber Definitions*, https://ccdcoe.org/cyber-definitions.html;
https://data.opentechinstitute.org/dataset/cyber-security-definitions/resource/c6ab94f6-0323-44a3-970f-549df5da0939, (preuzeto 10. novembra 2015).

[163] European Union Agency for Network and Information Secuirty (ENISA), “National Cyber Security Strategies in the World,” https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world (preuzeto 10. novembra 2015).

[164] International Telecommunication Union (ITU), *ITU Terms and Definitions*, http://www.itu.int/net/ITU-R/index.asp?redirect=true&category=information&rlink=terminology-database&lang=en&adsearch=&SearchTerminology=cyberspace&collection=normative&sector=all&language=all&part=abbreviationterm&kind=anywhere&StartRecord=1&NumberRecords=50 (preuzeto 10. novembra 2015).

[165] Open Technology Institute, *Global Cyber Definitions Data (Updated)*, https://data.opentechinstitute.org/dataset/cyber-security-definitions/resource/c6ab94f6-0323-44a3-970f-549df5da0939 (preuzeto 10. novembra 2015).

[166] Thomas Haigh, "The Tears of Donald Knuth." *Communications Of The ACM* 58, no. 1 (January 2015): 40-44, http://cacm.acm.org/magazines/2015/1/181633-the-tears-of-donald-knuth/abstract (preuzeto 30. januara 2016).

[167] Michael R. Williams, *A History of Computing Technology*. (Wiley-IEEE Computer Society Press, 1997).

[168] Michael S. Mahoney, "The History of Computing in the History of Technology," *Annals of the History of Computing* 10, no. 2 (1988): 113-125, http://www.princeton.edu/~hos/mike/articles/hcht.pdf (preuzeto 30. januara 2016)

[169] Cilj projekta ARPANET, pokrenutog 1969 godine, je bilo kreiranje nacionalne vojne komunikacione mreže sposobne da preživi razaranja mrežne infrastrukture u potencijalnom nuklearnom ratu. Zbog toga je osnova programa bila izgradnja mreže između udaljenih vojnih centara i komandi sa distribuiranim i decentralizovanim čvorištima, sposobne da dinamično menja mrežnu topologiju. Ovaj vojni projekat je doživeo nagli razvoj kada su u njega uključeni predstavnici civilne akademske zajednice, univerzitetski centri na univerzitetima Stenfordu UCLA, MIT, Berkli, Juta i drugim. Od

u okviru koga je radilo više istaknutih pojedinaca[170], uz doprinos naučnika i ustanova iz Velike Britanije[171]. Kreativna moć ovog projekta je proistekla iz činjenice što je pored Ministarstva odbrane SAD, kroz funkcionisanje naučnoistraživačke *Agencije za napredne istraživačke projekte* (eng. *Advanced Research Projects Agency* – ARPA)[172], u njemu aktivno učestvovala naučno-istraživačka zajednica vodećih američkih univerziteta u oblasti računarskih nauka i informaciono-komunikacionih tehnologija.[173] Tako se mirnodopski istraživački potencijal preveo u aktivnosti odbrane od strategijskog značaja uz istovremen interes odbrambene, naučne i industrijske zajednice. [174]

1983.godine, Ministarstvo odbrane SAD je u odvojenom projektu počelo da razvija novu, bezbednu mrežu MILNET, a ARPANET je nastavio život u obliku nove mreže NSFNET, od koga je nastao savremeni Internet početkom devedesetih godina prošlog veka.

Izvor Mladenović „Neslućene mogućnosti novih tehnologija."

[170] Ključni istraživači tadašnje agencije ARPA su bili rukovodioci njenih programa za razvoj računarskih tehnologija, Robert Kan i Vinton Cerf. Rad Kana i Cerfa je doveo do izuma novih protokola umrežavanja koji su poslužili kao osnova za funkcionisanje tehnologije mrežne komunikacije digitalnih podataka.

[171] Britanski naučnik Donald Dejvis je ključni tvorac sistema saobraćaja paketa podataka (eng. *packet switching*).

Internet Hall of Fame, "Donald Davies" http://www.internethalloffame.org/inductees/donald-davies (preuzeto 18. Decembra 2015);

Cade Metz, "Why Do We Call Them Internet Packets? His Name Was Donald Davies," *Wired*, Septembar 10, 2012, http://www.wired.com/2012/09/donald-davies/ (preuzeto 13. Novembr 2015).

[172] ARPA je preteča savremene agencije DARPA (United States Defense Advanced Research Project Agency). Osnovana je 1958. godine, sa ciljem rukovođenja naučnoistraživačkim projektima radi ostvarivanja proboja u postojećim znanjima u oblasti tehnologije i nauke koji su od značaja za odbrambene potrebe. Promenila je ime u Defense Advanced Research Projects Agency (DARPA) 1972. godine. Osnovala ju je Vlada SAD zbog odbrambeno-političkih razloga, kao odgovor na prethodne uspehe Sovjetskog Saveza u razvoju i primeni kosmičke tehnologije, poput uspešnog lansiranja prvog veštačkog satelita Sputnjik u Zemljinu orbitu 1957. godine. DARPA ne izvodi neposredno projekte, već ih planira, organizuje, vodi i finansira. Budžet ove agencije u 2016. godini iznosi 2.94 milijardi američkih dolara. DARPA, Budget, preuzeto 20.01.2016. godine sa http://www.darpa.mil/about-us/budget;

Mladenović, „Neslućene mogućnosti novih tehnologija".

[173] Barry M. Leiner, Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, and Stephen Wolff, „Brief History of the Internet," *Internet Society*, http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet (preuzeto 12. januara 2016).

[174] Jadan od ključnih koraka u razvoju primenjenih informaciono-komunikacionih tehnologija i njihovom praktičnom objedinjavanju u koncept iz koga je nastao Internet, je ostvaren u periodu od 1983. do 1993. godine, za vreme rada agencije DARPA na programu Strategijska računarska inicijativa (eng. Strategic Computing Inititive – SCI). Nedugo po pokretanju ovaj projekat je od strane agencije DARPA nazivan kao Program strategijskog računarstva (*Strategic Computing Program*) ili samo sa *Strategijsko računarstvo* (*Strategic Computing*). Izvor: Alex Roland and Philip Shiman, *Strategic Computing: DARPA and the Quest for Machine Intelligence, 1983-1993*, (Cambridge, MA: The MIT Press, 2002) 333.

Uticaj Ministarstva odbrane SAD na razvoj sajber prostora nije ograničen na iniciranje i usmeravanje razvoja Interneta, već se ogleda i u neposrednom razvoju tehnologija koje su tehnološka osnova savremenog sajber prostora[175]. Taj pristup je kontinuiran i ima dugoročni cilj.[176]

Dakle, Internet, preteča sajber prostora, nastao je radom naučnika i inženjera u okviru projekata agencije DARPA, kao i radom istraživača na vodećim univerzitetima u SAD[177], u okviru inicijative Vlade SAD, čiji primarni cilj je bio da se unapredi sposobnost vojske za odbranu. Samo u svrhu razvoja informaciono-komunikacionih tehnologija, Vlada SAD je uložila više od milijardu dolara finansijskih sredstava, tokom perioda od jedanaest godina trajanja programa *Strategijska računarska inicijativa*.[178]

3.2.1. Evolucija značenja pojma „sajber prostor“

Značenje pojma „sajber prostor“ nije statično, već se neprekidno menja tokom vremena, u skladu sa razvojem tehnologije. Proces razvoja sajber prostora nije bio brz i kratak, već je trajao dugi niz godina. Tokom tog perioda, tehnologija se menjala, i u skladu sa njom, funkcionalne i operativne sposobnosti sistema koji su bili rezultat njene primene. Takođe,

---

[175] ARPA je, između ostalog, tokom svoga postojanja uspešno realizovala i niz razvojno orjentisanih istraživačkih projekata u oblasti računarstva i umrežavanja, čiji rezultati danas predstavljaju osnovu računarstva i informaciono-komunikacionih tehnologija u širokoj upotrebi u svetu, poput: računarskih mreža; ključnih digitalnih internet protokola, kao što su *Transmission Control Protocol* (TCP) i *Internet Protocol* (IP), hipertekst sistema, *oN-Line System* (NSL); grafičkog korisničkog interfejsa; hardverskih komponenti savremenih računara i mreža i drugih.

Defense Advanced Research Projects Agency, „Where the Future Becomes Now“, http://www.darpa.mil/about-us/darpa-history-and-timeline (preuzeto 18. decembra 2015).

[176] Primarni cilj programa *Strategijska računarska inicijativa* je bilo ostvarivanje mašinske inteligencije, odnosno „započinjanje integrisanog plana promocije razvoja dizajna i proizvodnje računarskog procesora, računarske arhitekture i softvera veštačke inteligencije. Ovaj cilj Vlada SAD razvija i danas, uglavnom kroz nove programe agencije DARPA.

Roland and Shiman, *Strategic Computing.*

[177] Kao istraživački projekata podržan od strane ARPA (Defense Department’s Advanced Research Project Agency), inicijalna mreža je uspostavljena između računara na univerzitetima UCLA, Stenford istraživačkom institutu (Stanford Research Institute), Santa Barbara kampu u sastavu Kalifornijskog Univerziteta (UC Santa Barbara) i Univerzitetu Juta (University of Utah), a zatim je ubrzo proširena i na Masačusetski tehnološki institut (M.I.T.), RAND i System Development Corp. u Santa Monici, Berkli (Berkley) kamp Kalifornijskog Univerziteta, Stenford Univerzitet (Stanford University) i Stenford Istraživački Institut (Stanford Research Institute).

Marcel Brown, „World, Meet the Internet“, *This Day in Tech History*, http://thisdayintechhistory.com/07/03/world-meet-the-internet/, (preuzeto 13. aprila 2016).

[178] Ne računajući posebne izdatke ili ulaganja za specijalne tajne operacije, za koje nije postojala zakonska obaveza Vlade SAD da pruža javnosti informacije o budžetskim sredstvima. Izvor: Roland and Shiman, *Strategic Computing*, 333-334.

tokom evolucije dostupnih sadržaja, procesa, servisa i mogućnosti za njihovu praktičnu primenu, razvijala se i svest ljudi, kao i državnih organizacija o shvatanju prirode sajber prostora i o njegovoj mogućoj primeni. To se najbolje vidi na primeru Ministarstva odbrane SAD, koje je često menjalo stav o shvatanju prirode sajber prostora. Izbor navedene institucije kao primera brze evolucije prirode sajber prostora je logičan, s obzirom da je ideja o nastanku sajber prostora, njegova tehnološka osnova i praksa primene u vojne svrhe nastala u navedenoj instituciji.

U *Združenoj publikaciji Vojske SAD broj 2-01.3*, iz 2000. godine, pod nazivom *Združene taktike, tehnike i procedure za združenu obaveštajnu pripremu bojišta*, objavljena je jedna od prvih javno dostupnih vojnih definicija sajber prostora uopšte. Po njoj, sajber prostor je: „Konceptualno[179] okruženje u kome digitalizovane informacije komuniciraju preko računarskih mreža“[180]. Ova definicija je dobila status zvanične definicije sajber prostora u Ministarstvu odbrane SAD objavljivanjem u *Rečniku vojnih i povezanih termina Ministarstva odbrane* iz 2001. godine.[181]

Sedam godina nakon navedene definicije, usvojena je nova definicija sajber prostora u tada klasifikovanoj[182] *Predsedničkoj direktivi u oblasti nacionalne i unutrašnje bezbednosti* (NSPD-54/HSPD-23): „’Sajber prostor’ označava međuzavisnu mrežu infrastruktura informacionih tehnologija, uključujući Internet, telekomunikacione mreže, računarske sisteme i ugrađene procesore i kontrolere u kritičnim industrijama“[183].

Iste godine, nedugo nakon objavljivanja prethodne definicije, u zvaničnoj upotrebi u Ministarstvu odbrane se pojavila i nova, proširena definicija sajber prostora: „Globalno područje unutar informacionog okruženja koje se sastoji od međuzavisnih mreža

[179] U smislu nematerijalnog, zamišljenog.

[180] *Joint Tactics, Techniques and Procedures for Joint Intelligence Preparation of the Battlespace: Joint Publication 2-01.3,* Washington, DC: Joint Chiefs of Staff, 20000, GL-4 – GL-5, http://webapp1.dlib.indiana.edu/virtual_disk_library/index.cgi/4240529/FID521/pdfdocs/jel/new_pubs/jp2_01_3.pdf (preuzeto 22. decembra 2015).

[181] *Department of Defense Dictionary of Military and Associated Terms: Joint Publication 1-02,* Washington, DC: Joint Chiefs of Staff, 2001, 110, http://www.bits.de/NRANEU/others/jp-doctrine/jp1_02%2801%29.pdf (preuzeto 22. decembra 2015).

[182] Navedena direktiva ima dve verzije, javnu i tajnu, koje se neznatno razlikuju i istovremeno su potpisane.

[183] The White House, George Bush, *National Secuirty Presidential Directive/NSPD-54 / Homeland Security Presidential Directive/HSPD-23*, (January 8, 2008), član 7, stav g, str. 3, https://fas.org/irp/offdocs/nspd/nspd-54.pdf (preuzeto 15. novembra 2015).

infrastruktura informacionih tehnologija, uključujući Internet, telekomunikacione mreže, računarske sisteme, i ugrađene procesore i kontrolere“.[184] Ova definicija je usvojena kao zajednička objavljivanjem u dopunjenom izdanju Rečnika od 26. avgusta 2008.[185]

Konačno, nakon pet godina i ova definicija je dodatno proširena, objavljivanjem nove definicije u *Združenoj publikaciji 3-12 (R), Operacije u sajber prostoru*[186]. U njoj su u pojam sajber prostora kao sastavni elementi uključeni i podaci koji postoje u međuzavisnim mrežama infrastruktura informacionih tehnologija. Po toj definiciji sajber prostor je: „Globalno područje unutar informacionog okruženja koje se sastoji od međuzavisnih mreža infrastruktura informacionih tehnologija i podataka u njima, uključujući Internet, telekomunikacione mreže, računarske sisteme, i ugrađene procesore i kontrolere“.[187] Ova definicija je postala zajednička za celo Ministarstvo odbrane SAD, objavljivanjem u dopunjenom Rečniku termina od 15. februara 2013. godine.[188]

Iako je između objavljivanja prve i poslednje definicije proteklo manje od trinaest godina, njihovo značenje se značajno izmenilo. Na to utiču tehnološki i društveni faktori. Kako pri analizi definicije iz 2001. godine navodi Kvejl[189], savremeni sajber prostor se odavno ne može više smatrati konceptualnim, niti je njegovo svrstavanje u „digitalizovanu“ ili „kompjuterizovanu“ oblast dovoljno široko da predstavi stvarnu prirodu sajber prostora

---

[184] Chairman of the Joint Chiefs of Staff (CJCS), *Memorandum 0363-08, The Definition of Cyberspace*, (10 July 2008).

Ova definicija je navedena u Memorandumu zamenika državnog sekretara za odbranu, Gordona Englanda, koja ima klasifikovan stepen tajnosti „samo za službenu upotrebu“, pa je stoga preuzeta posredno iz drugih izvora:

Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem." *Cyberpower and National Security* (2009): 26-28 i Noah Shachtman, „26 Years After Gibson, Pentagon Defines ‘Cyberspace’,“ *Wired*, May 23, 2008, http://www.wired.com/2008/05/pentagon-define/ (preuzeto 12. decembra 2015).

[185] *Department of Defense Dictionary of Military and Associated Terms: Joint Publication 1-02*, Washington, DC: Joint Chiefs of Staff, 2001 (as amended through 26 August 2008), 141, http://www.bits.de/NRANEU/others/jp-doctrine/jp1_02%288-08%29.pdf (preuzeto 22. decembra 2015).

[186] *Cyberspace Operations: Joint Publication 3-12*.

[187] *Cyberspace Operations: Joint Publication 3-12,* GL-4.

[188] *Department of Defense Dictionary of Military and Associated Terms: Joint Publication 1-02,* Washington, DC: Joint Chiefs of Staff, 2010 (as amended through 15 February 2013), 71, http://www.bits.de/NRANEU/others/jp-doctrine/jp1_02%282-13%29%5B1%5D.pdf (preuzeto 22. decembra 2015).

[189] Daniel Kuehl (1949-2014), profesor i direktor programa Informacione operacije na Nacionalnom Univerzitetu odbrane u Vašingtonu, SAD.

u smislu velikih tehnoloških i društvenih promena u koje je uključen. [190] Proteklo vreme je pokazalo, slična ocena se može dati u različitim periodima. Za to je zaslužna velika brzina razvoja informaciono-komunikacionih tehnologija, tehnoloških inovacija i njihovog prihvatanja od strane pojedinaca i društva. Zbog te brzine i društvenih promena koje tehnološke inovacije uzrokuju, i priroda sajber prostora se brzo menja. Tehnologija nije jedini uzrok za njenu evoluciju. Kao posledica terorističkog napada 11. septembra 2001. godine, u SAD su se desile krupne društvene promene u periodu od 2001. do 2008. godine. Celokupna američka nacionalna politika se okrenula ka pooštravanju mera za očuvanje nacionalne bezbednosti. Formirano je Ministarstvo unutrašnje bezbednosti[191] 2002. godine, sa ogromnim budžetom[192], velikim brojem potčinjenih agencija, direktorata i službi[193], i sa preko 240.000 zaposlenih[194]. Ovom ministarstvu su dodeljene značajne nadležnosti koje su dovele do novih standarda u pogledu poštovanja privatnosti vlastitih građana, i do gotovo potpunog nepoštovanja prava na privatnost pojedinaca koji nisu u nadležnosti sopstvenog suvereniteta. Posledica ovakvog društvenog okruženja je da je definicija sajber prostora iz tog perioda vrlo bezbednosno orjentisana.

3.3. Definicija sajber prostora

S obzirom da međunarodno pravo kreiraju države, u pogledu međunarodnopravnog definisanja sajber ratovanja i sajber prostora, od najvećeg značaja su stavovi država, a zatim i relevantnih međunarodnih stručnih organizacija. Međutim, ne postoji jedinstvena definicija sajber prostora kao tehničkog, društvenog, vojnog ili prirodnog fenomena. U akademskoj i stručnoj javnosti postoji mnoštvo različitih definicija koje se razlikuju po kontekstu, sadržaju i nameni.[195] Većina država koje kreiraju vlastite strategije razvoja informacionog društva ili strategije nacionalne bezbednosti i odbrane su usvojile

[190] Kuehl, "From Cyberspace to Cyberpower“, 26-28.

[191] *Department of Homeland Security* (DHS).

[192] Budžet Ministarstva unutrašnje bezbednosti se kretao od 37,7 milijardi američkih dolara u 2003. godini do 66,4 milijardi dolara u 2011. godini. Izvor: Department of Homeland Security, *DHS Budget*, preuzeto sa http://www.dhs.gov/dhs-budget

[193] Department od Homeland Security, *Operational and Support Components*, preuzeto sa http://www.dhs.gov/components-directorates-and-offices

[194] Department of Homeland Security, About DHS, preuzeto sa http://www.dhs.gov/about-dhs

[195] Rain Ottis and Peeter Lorents, "Cyberspace: Definition and Implications." *Proceedings Of The International Conference On Information Warfare & Security* (January 2010): 267-270.

sopstvene definicije sajber prostora. U određenom broju slučajeva, razlike u njihovim stavovima su značajne.

Definicije se razlikuju zavisno od prihvaćenog kriterijuma. Takođe, zbog brzog razvoja računarskih nauka, inženjerstva i informaciono-komunikacionih tehnologija, značenje pojma sajber prostor se menja u vremenu čak i u okviru istog konteksta, odnosno u okviru istih institucija.[196] Zbog brze i dinamične izmene prirode sajber prostora, u cilju analize njegovog uticaja na sukobe u sajber prostoru i njihovo regulisanje, bitnije od izbora same definicije je utvrđivanje njegovih ključnih univerzalnih svojstava i elemenata.

3.3.1. Odabir relevantnih izvora

U svetskoj akademskoj i stručnoj zajednici formirano je nekoliko projekata i baza podataka/agregatora definicija ključnih pojmova od značaja za informacionu bezbednosti i upotrebu informaciono-komunikacionih tehnologija. Među njima su najkompletnije baza podataka *Međunarodne unije za telekomunikacije* (ITU)[197], NATO *Centra izuzetnosti za kooperativnu sajber odbranu* (CCDCOE)[198] i američke nevladine tink-tank organizacije *Otvoreni tehnološki institut* (OTI)[199].

Definicije pojmova od značaja je moguće naći i pregledom nacionalnih strategijskih dokumenata u oblasti nacionalne bezbednosti, sajber bezbednosti i odbrane. Preglede ovih strategija ažuriraju *Agencija Evropske Unije za mrežnu i informacioni bezbednost* (ENISA)[200] i CCDOCE[201].

Pored navedenih izvora, od značaja za analizu su i definicije odgovarajućih pojmova koje su navedene u standardima koji se odnose na sajber i informacionu bezbednost čiji su autori vodeće međunarodne organizacija za standardizaciju; u izveštajima i studijama

[196] Daniel T Kuehl, "From Cyberspace to Cyberpower," 6-28. Napomena: kao primer je izabran specifičan pogled Ministarstva odbrane SAD, s obzirom da je iz naučnog projekta ove institucije i nastao savremeni sajber prostor, kroz projekat ARPANET.

[197] ITU, *ITU Terms and Definitions*.

[198] CCDCOE, *Cyber Definitions*.

[199] Open Technology Institute (OTI), *Cyber Security Definitions*, https://data.opentechinstitute.org/dataset/cyber-security-definitions (preuzeto 23. decembra 2015).

[200] ENISA, "National Cyber Security Strategies".

[201] NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), *Cyber Security Strategy Documents*, https://ccdcoe.org/strategies-policies.html, (preuzeto 12. januara 2015).

stručnih organizacija koje se bave istraživanjem navedenih oblasti, kao i definicije iz referentnih rečnika[202].

U cilju ontološke i funkcionalne analize prirode sajber prostora, korisno je izvršiti komparativnu analizu navedenih definicija sajber prostora iz pomenutih izvora. Međutim, zbog broja postojećih definicija, nije praktično, a zbog različite relevantnosti izvora, nije ni neophodno analizirati sve postojeće definicije. Njihovi sadržaji se u velikom broju slučajeva preklapaju po značenju, zbog međusobnog stručnog, društvenog, političkog ili vojno-bezbednosnog uticaja. Takođe, ni same definicije pojmova nemaju trajan karakter, već se menjaju tokom vremena u skladu sa razvojem okruženja i tehnologije. Različite države objavljuju sopstvene strategije u različitim vremenskim periodima, što rezultira time da trenutne definicije potiču iz različitih vremenskih perioda, sa vremenskom razlikom između njihovog nastanka koja je često veća i od pet godina. U uslovima brzog razvoja informaciono-komunikacionih tehnologija i njihove praktične primene u oblasti nacionalne bezbednosti i odbrane, ovaj period se može smatrati dugačkim, s obzirom da se prosečna srednjoročna evolucija ciklusa upravljanja rizikom u oblasti nacionalne bezbednosti i odbrane najčešće odvija u periodu oko pet godina, a dugoročna u periodu od deset godina.

Trajanje strategijskog ciklusa u oblasti bezbednosti i odbrane zavisi od više faktora, koji se mogu grupisati na spoljne i unutrašnje. U spoljne spadaju razni elementi strategijskog okruženja, poput verovatnoće pojave novih pretnji i rizika u odnosu na postojeću strategiju, koji nisu obuhvaćeni aktuelnom strategijom bezbednosti i/ili odbrane, očekivanog stanja resursa i spoljnih faktora od značaja. U unutrašnje faktore prvenstveno se ubrajaju elementi društvene i političke organizacije, izborni i srednjoročni budžetski ciklus, pojava unutrašnjih pretnji i rizika, očekivana dostupnost kritičnih resursa i drugi. U manjim organizacionim sistemima, kao što su poslovne organizacije, dužina ciklusa strategijskog akcionog plana može biti kraća i kreće se od 3-5 godina, što zavisi i od dinamike razvoja strukture i ciljeva organizacije. Imajući u vidu izneto, može se smatrati da je za potrebe utvrđivanja karakteristika sajber prostora dovoljno izvršiti uporednu analizu stavova (definicija) šireg skupa relevantnih faktora. Nesumnjivo, u tom pogledu,

[202] Pre svega iz engleskog jezika, s obzirom na to da je to podrazumevani jezik u oblasti informacione bezbednosti, najrasprostranjeniji jezik u komunikaciji na međunarodnom nivou i jezik države porekla većine tehnologija i pojmova u oblasti informaciono-komunikacionih tehnologija.

najveći uticaj u svetu ostvaruju one države koje ostvaruju najveći uticaj na razvoj računarskih nauka i informaciono-komunikacionih tehnologija, na razvoj sajber prostora, na njegovu primenu u oblasti bezbednosti i odbrane, koje imaju najveću ekonomsku, političku, privrednu i vojnu moć i sposobnosti istraživanja i razvoja u oblasti sajber bezbednosti. U odsustvu egzaktne kvantitativne metrike u oceni relevantnosti državnih pristupa i uticaja na sajber bezbednost i odbranu, od praktične koristi za poređenje mogu biti ekspertske analize kvalitativne prirode, odnosno rezultati dobijeni na osnovu rangiranja subjektivnih stavova anketiranih stručnjaka. U tom pogledu, kao polazna osnova su uzete sledeće studije i izveštaji iz područja razvoja informaciono-komunikacionih tehnologija, inovacija, visokotehnoloških kompanija, konkurentnosti, vojne moći, sajber odbrane i sajber bezbednost:

- ITU ICT Development Index[203],
- Global Inovation Index (GII)[204],
- The Bloomberg Innovation Index (High Tech Companies Category)[205],
- The Global Competitivenes Index 2015-2016 Rankings[206],
- Global Fire Power (GFI) (2016)[207],
- McAfee/Security & Defence Agenda (SDA), Cyber Defense 2012 Report: Country Defense Rankings[208],
- ABI Research & ITU Global Cybersecurity Index & Cyberwellness Profiles 2015[209] (Tabela 1).

[203] International Telecommunication Union, *ICT Development Index, 2015*, http://www.itu.int/net4/ITU-D/idi/2015/ (preuzeto 2. januara 2016).

[204] Soumitra Dutta, Bruno Lanvin and Sacha Wunsch-Vincent, eds., *The Global Innovation Index 2015: Effective Innovation Policies for Development* (Cornell University, INSEAD, WIPO, 2015), https://www.globalinnovationindex.org/userfiles/file/reportpdf/GII-2015-v5.pdf (preuzeto 2. januara 2016).

[205] Bloomberg, *The Bloomberg Innovation Index: High-Tech Companies*, http://www.bloomberg.com/graphics/2015-innovative-countries/ (preuzeto 2. januara 2016).

[206] Klaus Schwab, *The Global Competitiveness Report 2015-2016*, World Economic Forum, http://www3.weforum.org/docs/gcr/2015-2016/Global_Competitiveness_Report_2015-2016.pdf (preuzeto 2. januara 2016).

[207] Global Firepower (GFP), http://www.globalfirepower.com/ (preuzeto 2. januara 2016).

[208] McAfee (Intel Company), "57% Believe a Cyber Arms Race is Currently Taking Place, Reveals McAfee-Sponsored Cyber Defense Report", http://www.businesswire.com/news/mcafee/20120130005063/en/57-Cyber-Arms-Race-Place-Reveals-McAfee-Sponsored (1. februara 2016).

[209] ABI Research/ITU, *Global Cybersecurity Index & Cyberwellness Profiles Report*, (2015), https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf (1. februara 2016).

Tabela 1. Pregled aktuelnih spiskova vodećih država sveta na sedam karakterističnih međunarodnih listi od značaja za razvoj sajber prostora.

	ITU ICT Development Index	Global Fire Power (GFI) (2016)	The Global Competitivenes Index 2015-2016 Rankings	Global Inovation Index (GII)	The Bloomberg Innovation Index (Hight Tech Companies Category)	McAfee asked the Security & Defence Agenda (SDA) Cyber Defense 2012 Report: Country Defense Rankings	ABI Research & ITU Global Cybersecurity Index & Cyberwellness Profiles 2015
1	Južna Koreja	SAD	Švajcarska	Švajcarska	SAD	Finska	SAD
2	Danska	Rusija	Singapur	Švedska	Kina	Izrel	Kanada
3	Island	Kina	SAD	Holandija	Japan	Švedska	Australija
4	Velika Britanija	Indija	Nemačka	SAD	Južna Koreja	Danska	Malezija
5	Švedska	Velika Britanija	Holandija	Finska	Kanada	Estonija	Oman
6	Luksemburg	Francuska	Japan	Singapur	Velika Britanija	Francuska	Novi Zeland
7	Švajcarska	Južna Koreja	Hong Kong	Irska	Hong Kong (Kina)	Nemačka	Norveška
8	Holandija	Nemačka	Finska	Luksemburg	Francuska	Holandija	Brazil

9	Hong Kong (Kina)	Japan	Švedska	Danska	Nemačka	Španija	Estonija
10	Norveška	Turska	Velika Britanija	Hong Kong (Kina)	Australija	Velika Britanija	Nemačka
11	Japan	Izrael	Norveška	Nemačka	Izrael	SAD	Indija
12	Finska	Indonezija	Danska	Island	Švedska	Australija	Japan
13	Australija	Australija	Kanada	Južna Koreja	Poljska	Austrija	Južna Koreja
14	Nemačka	Kanada	Katar	Novi Zeland	Malezija	Kanada	Velika Britanija
15	SAD	Tajvan (Kina)	Tajvan (Kina)	Kanada	Rusija	Japan	Austrija
16	Novi Zeland	Italija	Novi Zeland	Australija	Singapur	Kina	Mađarska
17	Francuska	Pakistan	Ujedinjeni Arapski Emirati	Austrija	Švajcarska	Italija	Izrael
18	Monako	Egipat	Malezija	Japan	Tajland	Poljska	Holandija
19	Singapur	Poljska	Belgija	Norveška	Italija	Rusija	Singapur
20	Estonija	Tajland	Luksemburg	Francuska	Norveška	Brazil	Letonija

Tabela 2. Pregled učestalosti pojavljivanja država na aktuelnim listama faktora razvoja primene informacionih tehnologija na nacionalnom nivou

Redni broj	**Država**	**Broj pojavljivanja na listi vodećih država**	**Definisan je termin „sajber prostor“**	**Ne postoji definicija termina „sajber prostor“**	**Nisu objavljeni ili usvojeni nacionalni strategijski dokumenti**
1	SAD	7	x		
2	Nemačka	7	x		
3	Japan	7	x		
4	V. Britanija	6	x		
5	Kanada	6	x		
6	Južna Koreja	6		x	
7	Australija	5	x		
8	Holandija	5	x		
9	Danska	5		x	
10	Švedska	5			x
11	Norveška	5		x	
12	Singapur	5		x	
13	Finska	4	x		
16	Izrael	4	x		
14	Francuska	4	x		
15	Novi Zeland	4	x		
17	Švajcarska	4	x		
18	Luksemburg	4		x	
20	Rusija	3	x		
22	Kina	3			x
19	Italija	3	x		
21	Estonija	3		x	
23	Malezija	3		x	
26	Austrija	3	x		
24	Indija	2	x		
25	Poljska	2	x		

Navedene studije i liste su najcitiranije i stručno najpoznatije u relevantnom području, odnosno imaju utvrđenu metodologiju istraživanja. U analizi za potrebe ove disertacije je usvojen kvantitativni faktor relevantnosti uticaja u međunarodnim okvirima u pogledu kvalitativnog definisanja pojmova i kategorija u oblasti primene informaciono-komunikacionih tehnologija po kriterijumu da je pojedina država rangirana u prvih 20 država u predmetnim kategorijama više od jednog puta. Upoređivanjem rezultata navedenih istraživanja dobijen je spisak od ukupno 25 država (Tabela 2).

Pregledom baza podataka iz prethodno navedenih izvora[210], kao i pojedinačnih strategijskih dokumenata država sa spiska, utvrđen je podatak da sedam evidentiranih država nije definisalo pojam „sajber prostor“ u svojim aktuelnim nacionalnim strategijskim dokumentima, dok dve države nisu javno objavile svoje odgovarajuće strategijske dokumente, ili su oni još u vek u fazi izrade.

Definicijama navedenim u nacionalnim strategijama preostalih 16 država su pridodate reprezentativne definicije iz rečnika i baza podataka definicija iz Oksfordskog rečnika pojmova[211], Međunarodne organizacije za standardizaciju (ISO)[212], Međunarodne telekomunikacione unije[213], *Talinskog priručnika o međunarodnom pravu primenjivom na sajber ratovanje*[214] i međunarodne nevladine stručne organizacije *EastWest Institute*

[210] ITU, *ITU Terms and Definitions*; CCDCOE, *Cyber Definitions*; OTI, *Cyber Security Definitions.*

[211] Oxford English Dictionary (OED) sadrži preko 600.000 pojmova na engleskom jeziku i predstavlja referentni rečnik ovog jezika u svetu, kao i veliki broj specijalizovanih rečničkih izdanja u različitim oblastima ljudskog znanja. Preuzeto sa http://www.oed.com/. Engleski jezik je odabran kao nezvanični jezik oblasti računarskih nauka, informaciono-komunikacionih tehnologija i informacione bezbednosti pošto su one u najvećoj meri nastale u državama engleskog govornog područja, SAD i Velikoj Britaniji. I sam sajber prostor je nastao radovima inženjera u pomenutim državama, a njegov jezički termin u SAD i Kanadi.

[212] *International Organization for Standardization* (ISO) je vodeća nezavisna međunarodna nevladina stručna organizacija za standardizaciju sa sedištem u Ženevi, čiji su članovi 163 nacionalne organizacije za standarde. Osnovni cilj ove organizacije je kreiranje zajedničkih tehničkih specifikacija za proizvode, servise i sisteme sa ciljem da se obezbedi njihov kvalitet, bezbednost i efikasnost. Do sada je objavila više od 20.500 standarda u različitim oblastima. Preuzeto sa http://www.iso.org.

International Electrotechnical Commision (IEC) je najveća svetska nevladina i neprofitna organizacija za izradu i objavljivanje međunarodnih standarda za sve vrste električnih, elektronskih i povezanih tehnologija, sa sedištem u Ženevi. U njenom članstvu je 60 nacionalnih organizacija. Preuzeto sa http://www.iec.ch.

Vodeća familija standarda (skup više standarda grupisanih u specifično područje sa jedinstvenom tematikom) u oblasti informacione i sajber bezbednosti u svetu je serija standarda ISO/IEC 27000, koja se bavi sistemima menadžmenta informacionom bezbednošću i tehnikama bezbednosti u oblasti informacionih tehnologija. Spisak svih javno objavljenih ISO i ISO/IEC standarda koje se bave informacionim tehnologijama i informacionom bezbednošću je značajno širi. Preuzeto sa http://standards.iso.org/ittf/PubliclyAvailableStandards/. Spisak svih međunarodnih standarda u ovoj oblasti je još veći. European Network and Information Security Agency (ENISA), *Shortlisting Network and Information Security Standards and Good Practices, Version 1.0*, (2012), preuzeto sa https://resilience.enisa.europa.eu/article-13/shortlist-of-networks-and-information-security-standards (preuzeto 4. januara 2016).

[213] *International Telecommunication Union*. ITU je specijalizovana agencija Ujedinjenih Nacija (UN) sa sedištem u Ženevi koja se na sveobuhvatan način bavi pitanjima međunarodne regulacije upotrebe informaciono-komunikacionih tehnologija. Preuzeto sa http://www.itu.int/en/about/Pages/default.aspx

[214] *Tallin Manual on the International Law Applicable to Cyber Warfare*, poznat u stručnoj javnosti i kao *Tallinn Manual* (Talinski priručnik) je akademska studija o smernicama kako se Međunarodno pravo oružanih sukoba može praktično primeniti na sukobe u sajber prostoru i sajber ratovanje. Ovaj priručnik (knjiga) je rezultat rada grupe najeminentnijih autora iz oblasti Međunarodnog prava

(EWI)[215], kao referentnih savremenih izvora u oblasti primenjene informacione bezbednosti u sajber prostoru.

3.3.2. Pregled i analiza definicija

Pojam sajber prostora je od strane 21 izabrane referentne institucije u svetu definisan na isto toliko različitih načina, pristupom koji se kreće od potpuno opšteg, do vrlo specifičnog.

1. *Oksfordski rečnik pojmova na engleskom jeziku* definiše „sajber prostor" kao: „prostor virtuelne realnosti; konceptualno okruženje u kome se elektronska komunikacija dešava (naročito putem Interneta)"[216].
2. ISO standard ISO/IEC 27032 definiše sajber prostor kao: „kompleksno okruženje koje je nastalo interakcijom ljudi, softvera i servisa na Internetu uz pomoć tehnoloških uređaja i povezanih mreža, koje ne postoji ni u jednom fizičkom obliku"[217], dok sajber bezbednost definiše kao: „očuvanje poverljivosti, integriteta i dostupnosti informacija u sajber prostoru"[218].

oružanih sukoba iz više država članica NATO saveza, okupljenih u projektu Centra izuzetnosti za saradnju u oblasti sajber odbrane (*Cooperative Cyber Defence Centre of Excellence – CCDCOE*) iz Talina, Estonija. Projekt je započet 2009. godine, a 2016. godine se očekuje njegovo drugo izdanje na kome rade stručnjaci iz većine država NATO saveza. Ovaj projekat ima istraživačku i obrazovnu prirodu, i kao takav ne predstavlja obavezujući izvor prava za NATO članice, ali mu je uticaj među njima izuzetno veliki, zbog čega predstavlja vodeći stručno-akademski izvor pravne regulacije sukoba u sajber prostoru u svetu. U daljem tekstu Talinski priručnik.

Preuzeto sa https://ccdcoe.org/tallinn-manual.html;

Schmitt, *Tallinn Manual*.

[215] EastWest Institute (EWI) je međunarodna nezavisna neprofitna nevladina institucija koja se bavi aktivnostima neformalne diplomatije u cilju rešavanja međunarodnih sukoba dijalogom između svetskih sila, posebno u oblastima političkih, vojnih i ekonomskih pitanja, http://www.eastwest.ngo/ EastWest Institute je 2011. godine izdalo prvo, a 2014. godine drugo izdanje ontološko-taksonomijskog rečnika definicija pojmova iz oblasti sajber sukoba i ratovanja, koji je rezultat saradnje EastWest instituta i Instituta za informacionu bezbednost Moskovskog Univerziteta. Ovaj specijalizovani rečnik predstavlja prvi sistematičan i pojmovno potpun metodološki rečnik posvećen sajber ratovanju te vrste u svetu.

[216] *Oxford English Dictionary*, s.v. „weapon," http://www.oed.com.nduezproxy.idm.oclc.org/view/Entry/240849?redirectedFrom=cyberspace#eid, (preuyeto 11. januara 2016).

[217] International Organization for Standardization and International Electrotechnical Commission, *ISO/IEC 27032:2012, Information technology — Security techniques — Guidelines for cybersecurity* (Geneva, Switzerland: ISO/IEC, 2012).

[218] Ibid.

3. ITU umesto termina „sajber prostor“ koristi termin „sajber okruženje“ (eng. *cyber environment*), u koje uključuje: „korisnike, mreže, uređaje, celokupan softver, procese, informacije koje se čuvaju ili komuniciraju, aplikacije, servise i sisteme koji mogu biti direktno ili indirektno povezani sa mrežama“. [219]
4. Autori *Talinskog priručnika* definišu sajber prostor kao: „okruženje formirano od fizičkih i nefizičkih komponenti, koje karakteriše upotreba računara i elektromagnetnog spektra za čuvanje, modifikaciju i razmenu podataka koristeći računarske mreže“.[220]
5. Međunarodna tink-tank organizacija *EastWest Institute* definiše sajber prostor kao: „elektronsku sredinu u kojoj se informacije stvaraju, upućuju, primaju, čuvaju, obrađuju i uništavaju“[221].
6. Ministarstvo odbrane SAD definiše sajber prostor kao: „Globalno područje unutar informacionog okruženja koje se sastoji od međuzavisnih mreža infrastruktura informacionih tehnologija i podataka u njima, uključujući Internet, telekomunikacione mreže, računarske sisteme, i ugrađene procesore i kontrolere“.[222]
7. Projekat *Veća Federacije Skupštine Ruske Federacije* definiše da je sajber prostor (rus. *киберпространство*): „Sfera aktivnosti u okviru informacionog prostora, stvorena skupom komunikacionih kanala Interneta i drugih telekomunikacionih mreža, tehnoloških infrastruktura koje obezbeđuju njihovo funkcionisanje, i svaki oblik ljudske aktivnosti na njima (individualne, organizacione, državne).[223]
8. Po *Strategiji sajber bezbednosti* Velike Britanije, sajber prostor je: „interaktivno područje koje se sastoji od digitalnih mreža koje se koriste za čuvanje, modifikovanje i komunikaciju informacija. To područje uključuje internet, ali i

[219] ITU, *ITU Terms and Definitions*.

[220] Schmitt, *Tallinn Manual,* 258.

[221] James B. Godwin III, Andrey Kulpin, Karl Frederick Rauscher and Valery Yaschenko, eds., *Russia-U.S. Bilateral on Cybersecurity: Critical Terminology Foundations 2* (New York, NY: The EastWest Institute, 2014), 22.

[222] *Cyberspace Operations: Joint Publication 3-12,* V.

[223] Совет Федерации, Федералыного Собрания Российской Федерации, *Концепция стратегии кибербезопасности Российской Федерации - Проект*, (10 января 2014), 2, http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf (preuzeto 5. januara 2016).

druge informacione sisteme koji podržavaju naše poslovanje, infrastrukture i servise“[224].

9. *Federalno ministarstvo unutrašnjih poslova Nemačke* definiše sajber prostor kao: „…virtuelni prostor svih sistema informacionih tehnologija povezanih na nivou podataka u globalnim okvirima. Osnova sajber prostora je Internet kao univerzalna i javno dostupna mreža za povezivanje i transport koja može biti dopunjena bilo kojim brojem dodatnih mreža podataka. Sistemi informacionih tehnologija u izolovanom virtuelnom prostoru nisu deo sajber prostora.“[225]
10. Vlada Izraela definiše sajber prostor kao: „Fizičko i nefizičko područje koje stvaraju ili sačinjavaju delovi ili celine sledećih komponenti: mehanizovanih i kompjuterizovanih sistema, računarskih i komunikacionih mreža, programa, računarskih informacija, računarskih sadržaja saobraćajnih i kontrolnih podataka i onih koji koriste takve podatke“.[226]
11. *Nacionalna strategija odbrane i bezbednosti informacionih sistema Francuske* daje sledeću definiciju sajber prostora: „Komunikacioni prostor koji stvara svetska međukonekcija automatizovane opreme za obradu digitalnih podataka“.[227]
12. *Nacionalna politika sajber bezbednosti Indije* definiše sajber prostor kao: „…kompleksno okruženje koje stvaraju interakcije između ljudi, softvera, uređaja, omogućene svetskom distribucijom informaciono-komunikacionih uređaja i mreža“[228]

---

[224] United Kingdom, *The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World*, (United Kingdom, UK Cabinet Office, 2011) 11, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf (preuzeto 5. januara 2016).

[225] FR Germany, Federal Ministry of the Interior, *Cyber Security Strategy for Germany* (February 2011), 9, https://www.bsi.bund.de (preuzeto 6. januara 2016).

[226] Israel, Government of Israel, *Resolution No. 3611: Advancing National Cyberspace Capabilities* (2011), 1, http://www.pmo.gov.il/English/PrimeMinistersOffice/DivisionsAndAuthorities/cyber/Documents/Advancing%20National%20Cyberspace%20Capabilities.pdf (preuzeto 6. januara 2016).

[227] France, Agence Nationale de la Securite des Systemes d'Information, *Information Systems Defence and Security: France's Strategy* (2011), http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world (preuzeto 6.januara 2016). Napomena: Nova francuska strategija iz 2015. godine ne sadrži definiciju sajber prostora.

[228] India, National Cyber Security Policy (2013), 1, http://deity.gov.in/content/national-cyber-security-policy-2013-1 (preuzeto 6. januara 2016).

13. *Strategija sajber bezbednosti Finske* definiše da pojam „sajber područje“ predstavlja: „…područje obrade elektronskih informacija (podataka) koje obuhvata jednu ili nekoliko infrastruktura informacionih tehnologija“[229]
14. *Nacionalni strategijski okvir za bezbednost u sajber prostoru Italije* definiše sajber prostor kao: “…veštački stvoreno područje suštinski sačinjeno od informaciono-komunikacionih čvorišta i mreža, koje skladište i obrađuju stalno narastajuće bogatstvo podataka od strateškog značaja za države, kompanije, i podjednako građane, kao i za sve političke, društvene i ekonomske donosioce odluka“.[230]
15. *Nacionalna strategija bezbednosti Japana* definiše sajber prostor kao „...globalno područje sačinjeno od informacionih sistema, telekomunikacionih i drugih mreža, koje omogućava osnovu za društvene, ekonomske, vojne i druge aktivnosti“.[231]
16. *Strategija sajber bezbednosti Kanade* definiše sajber prostor kao: „…elektronski svet koji sačinjavaju međupovezane mreže informacionih tehnologija i informacija u tim mrežama. To je zajedničko dobro u kome je više od 1,7 milijardi ljudi međusobno povezano u cilju razmene ideja, servisa i prijateljstva“.[232]
17. Po *Strategiji sajber odbrane Holandije*, „sajber prostor obuhvata sve entitete koji su ili potencijalno mogu biti digitalno povezani. Njegovo područje obuhvata stalne, privremene ili lokalne veze, a u svim tim slučajevima je na neki način povezano sa podacima (izvorni kod, informacije, itd.) koji postoje u njemu“.[233]
18. *Strategija sajber bezbednosti Novog Zelanda* definiše sajber prostor kao „globalnu mrežu nezavisnih infrastruktura informacionih tehnologija,

[229] Finland, Ministry of Defence, Secretariat of the Security and Defence Committee, *Finland's Cyber Security Strategy* (2013), 12, http://www.enisa.europa.eu/media/news-items/new-cyber-security-strategies-of-austria-finland-worldwide (preuzeto 9. januara 2016).

[230] Presidency of the Council of Ministers, Government of Italy, *National Strategic Framework for Cyberspace Security* (2013), 9, https://www.ccdcoe.org/strategies-policies.html (preuzeto 9. januara 2016).

[231] Japan, Government of Japan, *National Security Strategy* (2013), 9, http://www.cas.go.jp/jp/siryou/ (preuzeto 9. januara 2016).

[232] Canada, Government of Canada, *Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada* (2010), 2, http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/index-eng.aspx (preuzeto 12. januara 2016).

[233] Netherlands, Ministry of Defence, *The Defence Cyber Strategy* (2012) 4, http://www.ccdcoe.org/strategies/Defence_Cyber_Strategy_NDL.pdf (preuzeto 12. januara 2016).

telekomunikacionih mreža i sistema za računarsku obradu u kome se odvijaju onlajn komunikacije“.[234]

19. Po *Strategiji sajber bezbednosti Austrije*, sajber prostor je “virtuelni prostor sačinjen od svih sistema informacionih tehnologija međusobno povezanih u globalnim okvirima na nivou podataka. Osnova sajber prostora je Internet kao univerzalna i javno dostupna komunikaciona i transportna mreža, koja može biti dopunjena i proširena drugim mrežama podataka…pored toga, sajber prostor predstavlja i globalnu mrežu različitih nezavisnih informaciono-komunikacionih infrastruktura telekomunikacionih mreža i računarskih sistema”.[235] Pored toga, austrijska strategija ističe da primena sajber prostora omogućava sve vrste kulturnih, društvenih, poslovnih i političkih aktivnosti pojedincima, a državama funkcionisanje kritičnih nacionalnih infrastruktura.[236]
20. *Politika zaštite sajber prostora Poljske* navodi da je sajber prostor: „prostor u kome se obrađuju i razmenjuju informacije stvorene od strane IKT sistema, zajedno sa vezama između njih i odnosima između korisnika“[237]
21. *Nacionalna strategija za zaštitu Švajcarske od sajber rizika* navodi da država, privatni sektor i društvo omogućavaju sajber prostor koji sačinjavaju Internet, mobilne mreže i aplikacije, elektronsko poslovanje i uprava, kao i računarski kontrolni sistemi.[238]

Nabrojane definicije potiču iz različitih država i dokumenata, kreiranih u različitim nacionalnim i međunarodnim kontekstima. Većina definicija potiče iz dokumenata koji su bezbednosno orjentisani. Bez obzira na specifičnosti i različitost, sve one imaju više

[234] Germany (2011), 12, http://www.dpmc.govt.nz/sites/all/files/publications/nz-cyber-security-strategy-june-2011_0.pdf (preuzeto 12. januara 2016).

[235] Austria, Bundeskanzleramt Osterreich, Austrian Cyber Security Strategy, (2013), 21, http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world (preuzeto 12. januara 2016).

[236] Austria, *Austrian Cyber Security Strategy*.

[237] Poland, Ministry of Administration and Digitisation, Internal Security Agency, *Cyberspace Protection Policy of the Republic of Poland* (2013), 5, https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/copy_of_PO_NCSS.pdf (preuzeto 12. januara 2016).

[238] Switzerland, Federal Department of Defence, Civil Protection and Sport DDPS, *National strategy for the protection of Switzerland against cyber risks* (2012), 5, https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/National_strategy_for_the_protection_of_Switzerland_against_cyber_risksEN.pdf (preuzeto 12. januara 2016).

zajedničkih karakteristika (Tabela 3). Analizom zajedničkih karakteristika i razlika može se doći do objektivnog stava o prirodi sajber prostora.

Zajednička temeljna svojstva svih definicija sajber prostora su:

- sajber prostor je rezultat primene računarskih nauka i upotrebe informaciono-komunikacionih tehnologija;
- računarski informacioni sistemi imaju sposobnost međusobne interakcije, odnosno stalnog ili povremenog umrežavanja i
- sve informaciono-komunikacione tehnologije funkcionišu kroz operacije sa podacima i informacijama.

Ostala svojstva koja se tiču postojanja, upotrebe i karakteristika sajber prostora su ili izvedena iz prethodno navedenih, ili zavise od njih. U te izvedene elemente se mogu svrstati, veličina, položaj/pozicija u prostorno-geografskom smislu,[239] trajanje,[240] gustina, vrednost i druge.

U pogledu osnove sajber prostora, opšti stav je da on predstavlja okruženje, prostor ili najčešće, sredinu, u kojoj postoje podaci elektromagnetne prirode i koji je nastao veštačkim putem.

U svim definicijama sajber prostor ima nematerijalnu prirodu (najčešće da je „virtuelni prostor“), odnosno da je deo šireg informacionog okruženja ili prostora.

[239] Sajber prostor nije prostor u smislu Dekartovog geometrijskog shvatanja prostora, već okruženje specifičnih stanja, aktivnosti i servisa vezanih za manipulaciju sa podacima i informacijama.

[240] Vreme postoji i u sajber prostoru, ali je ta vremenska dimenzija značajno izmenjena, kvantitativno i kvalitativno. Informacije putuju sajber prostorom bukvalno brzinom svetlosti, što je po ljudskom opažanju izjednačeno sa trenutnim, ali poimanje vremena ipak postoji i ono je vezano za algoritamski redosled vremenskih sekvenciji izvršavanja programiranih radnji, kapacitet protoka informacija, kao i za fizičko ograničenje rada hardvera.

Tabela 3. Uporedni pregled karakteristika sajber prostora u nacionalnim definicijama

Ko?	Šta?	Aktivnost	Elementi	Omogućava ga
Oksfordski rečnik	virtuelna realnost	elektronska komunikacija	/	elektronska komunikacija, Internet
ISO/IEC	kompleksno, nefizičko okruženje, Internet	interakcija ljudi, softvera i servisa	ljudi, softver, servisi, uređaji, mreže	tehnološki uređaji, povezane mreže
ITU	okruženje	direktna ili indirektna umreženost	korisnici, mreže, softver, servisi, sistemi, procesi, informacije	Interakcija
Tallinn Manual CCDCOE NATO	okruženje formirano od fizičkih i nefizičkih komponenti	čuvanje, modifikacija i razmena podatka	računari, elektromagnetni spektar, podaci, mreže	računari, elektromagnetni spektar, mreže
EWI	elektronska sredina	stvaranje, prijem, slanje, čuvanje, obrada i uništavanje informacija	informacije	informacije i informacioni sistemi
SAD	deo informacionog okruženja, globalno, Internet	sveukupne aktivnosti	mreže IT sistema, podaci, Internet, mreže, računarski sistemi, procesori, kontroleri	međuzavisne mreže, infrastrukture informacionih tehnologija i podaci
Rusija	sfera aktivnosti, deo informacionog prostora	sveukupne aktivnosti	tehnološke infrastrukture, mreže, ljudi, organizacije, države	skup komunikacionih kanala i mreža, tehnološke infrastrukture
V. Britanija	interaktivno područje	čuvanje, modifikovanje i komunikacija informacija, poslovanje, servisi, izgradnja infrastrukture	digitalne mreže, Internet i informacioni sistemi	Internet i informacioni sistemi
Nemačka	virtuelni prostor, nefizičko	povezanost na nivou podataka	svi IT sistemi	Internet, mreže podataka
Izrael	fizičko i nefizičko područje	sveukupne aktivnosti,	ljudi, sistemi, informacije, podaci	ljudi, sistemi, informacije, podaci
Francuska	komunikacioni prostor	/	automatizovana IT oprema, digitalni podaci	oprema za obradu digitalnih podataka
Indija	kompleksno okruženje	interakcija ljudi, softvera i uređaja	ljudi, softver, uređaji	svetska interkonekcija uređaja i mreža

Finska	područje obrade podataka	obrada elektronskih podataka	infrastrukture informacionih tehnologija	informacione tehnologije
Italija	veštačko područje	čuvanje i obrada podataka	države, kompanije, građani	čvorišta i mreže
Japan	globalno okruženje	društvene, ekonomske, vojne i druge aktivnosti	informacioni sistemi, mreže	/
Kanada	elektronski svet, zajedničko dobro	razmena ideja, servisa i prijateljstva	mreže i informacije	međupovezane mreže informacionih tehnologija
Holandija	skup entiteta	digitalno povezivanje	svi entiteti i podaci	povezivanje (stalno, povremeno, lokalno)
Novi Zeland	globalna mreža	onlajn komunikacije	infrastrukture, mreže i sistemi	informacione tehnologije
Austrija	virtuelni prostor	povezivanje na nivou podataka, društvene, kulturne, poslovne, političke aktivnosti, funkcionisanje kritičnih infrastruktura	sistemi, Internet, IKT infrastrukture, mreže	informacione tehnologije
Poljska	prostor	obrada i razmena informacija	IKT sistemi, informacije, veze i korisnici	IKT sistemi i veze
Švajcarska	/	/	Internet, mobilne mreže, aplikacije, e-uprava, e-poslovanje, računarski kontrolni sistemi	država, privatni sektor i društvo
Pretežne zajedničke karakteristike	– veštačka tvorevina – elektronsko okruženje, sredina	– neposredna: stvaranje, čuvanje, obrada, komunikacija elektronskih podataka – posredna: sve ljudske aktivnosti	– informacije, – računarski informacioni sistemi (softver, hardver), – procesi – ljudi	– fizička osnova – umrežavanje sistema, komunikacija informacija informacija, servisa i ljudi

Konačno, pretežni stav je da je sajber prostor elektronsko okruženje, pri čemu se, osim elektronskog, ne spominju drugi vidovi čuvanja i prenošenja informacija u elektromagnetnom području (optičkim putem, magnetnim zapisom ili kvantnom tehnologijom).

U sajber prostoru se čuvaju podaci/informacije i sa njima se manipuliše, pri čemu se, osim skladištenja informacija, najčešće ne definišu oblici manipulacije (šalju, primaju, obrađuju, uništavaju, kreiraju).

Aktivnosti sa podacima (informacijama) u sajber prostoru omogućavaju interakciju između ljudi, softvera i hardvera, kao i sve kulturne, društvene, privredne, finansijske, političke ili vojne aktivnosti.

Elementi sajber prostora su:

- podaci/informacije;
- informacioni sistemi, posebno mreže;
- infrastruktura informaciono-komunikacionih tehnologija;
- servisi i procesi, i
- ljudi kao autori, korisnici i učesnici.

Postojanje sajber prostora i aktivnosti u njemu omogućavaju računarska informaciona tehnologija (računarski uređaji, senzori, kontroleri, kablovi, mreže, infrastruktura i drugi) i ljudi.

Ključni faktori koji omogućavaju postojanje sajber prostora su njegova fizička osnova (infrastruktura) i međusobno povezivanje svih njegovih elemenata, odnosno umrežavanje.

Izabrane definicije potenciraju ulogu učesnika (ljudi i tehnoloških sistema uz primenu servisa) u kreiranju, održavanju i razvoju bezbednosti u sajber prostoru.

Navedeni dokumenti načelno definišu sajber bezbednost kao informacionu bezbednost u sajber prostoru, čime posredno razlikuju opštu informacionu bezbednost (bezbednost informacija i informacionih sistema) od informacione bezbednosti u sajber prostoru.

Takođe, posredno se može doneti zaključak da je sajber prostor deo šireg informacionog prostora, koga karakteriše upotreba računarskih uređaja, softvera i servisa.

U tom pogledu se ističe definicija navedena u Nacionalnoj strategiji bezbednosti Nemačke iz 2011. godine, po kojoj sajber prostor postoji samo kao deo globalne informacione mreže – Interneta,[241] a ne kao deo sveobuhvatnog informacionog okruženja. Po njemu, informacioni sistemi umreženi u lokalne mreže odvojene od Interneta nisu deo sajber prostora: „IT sistemi u izolovanom virtuelnom prostoru nisu deo sajber prostora“[242]. Međutim, stvarnost i praksa razvoja i primene informacionih tehnologija pokazuju suprotno. Za to postoji više argumenata tehnološke i organizaciono-bezbednosne prirode.

Tehnološki razvoj je doveo do pojave, jeftine i masovne upotrebe novih tehnologija za bežično umrežavanje, koje nisu primarno namenjene za stvaranje fiksnih, već povremenih mreža, niti im je osnovna svrha samo po sebi umrežavanje sa Internetom, već umrežavanje u cilju ostvarivanja specifične funkcije ili potrebe. Najraširenije među njima su različiti samouspostavljajući i samokonfigurišući protokoli za *ad hok* umrežavanja lica [243], vozila[244] ili mobilnih sistema različite namene[245], tehnologije za identifikaciju i autentifikaciju na malom rastojanju poput *Radio Frequency Identification* (RFID), *Near Field Communication* (NFC) ili *Quick Response Code* (QR Code), ili širi koncepti zasnovani na više različitih tehnologija poput Interneta stvari (*Internet of Things* – IoT) i okružujućeg računarstva (*Ubiquitous Computing*). Niska cena tehničkih sistema zasnovanih na navedenim tehnologijama, jednostavnost primene, otvorenost razvoja tehnologija i odsustvo potrebe za fiksnim mrežama dovodi do toga da se sposobnost umrežavanja podrazumevano omogućava kod svih sistema i stvari upotrebom navedenih i drugih tehnologija.

[241] FR Germany, *Cyber Security Strategy.*

[242] FR Germany, *Cyber Security Strategy*, 9, and Germany, Federal Office for Information Security (BSI), *Glossary/Terminology*, http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world (preuzeto 13. januara 2016).

[243] Personal Ad Hoc Network - PANET

[244] Vehicular Ad Hoc Network - VENET

[245] Mobile Ad Hoc Networks - MANET

Postoji i drugi pravac razvoja globalnog umrežavanja svega. Vodeće svetske kompanije u oblasti informacionih tehnologija, a pre svih vodeći pružaoci onlajn usluga, *Google*[246, 247, 248] i *Facebook*[249, 250] kao i mnogobrojne lokalne i gradske uprave,[251] pre svega u SAD, razvijaju fiksne bežične informacione mreže, i besplatno nude njihovu upotrebu svim potencijalnim korisnicima koji se nađu u dometu tih mreža. Njihov cilj je da klijentima širom sveta direktno dostave svoje servise i usluge, preko kojih ostvaruju ogromne profite, zaobilazeći pružaoce internet usluga, odnosno nacionalne provajdere, koji naplaćuju, usmeravaju i kontrolišu protok internet saobraćaja. U oba slučaja, razvojem ad hok umrežavanja ili proširivanjem fiksnih mreža, sposobnost umrežavanja postaje sve dostupnija i jeftinija i inherentno ugrađena u stvari i objekte. Osoba, objekat ili stvar ne

[246] U okviru „Project Loon" kompanija *Google* planira da ostvari „globalni Internet" puštanjem velikog broja (relativno jeftinih) balona u stratosferu (na 18 km visine, na granici vazdušnog prostora i svemira, na visini na kojoj nije definisana državna jurisdikcija) i da na njih zakači uređaje za emitovanje bežičnog internet signala (mobilna LTE4 mreža zasnovana na IP protokolu) koji će uspostavljati vezu međusobno, kao i sa baznim stanicama na Zemlji i tako obezbedi jeftiniji Internet pristup milijardama ljudi koji sada nemaju Internet ili imaju Internet lošijeg kvaliteta, a da pritom ona bude davalac Internet usluga. U prvoj fazi se planira pokrivanje države Šri Lanke, Indonezije i gotovo celog južno azijskog regiona, a zatim i celog sveta stvaranjem prstena hiljada balona koje u krug nose vazdušne struje oko planete Zemlje. Ova bežična veza između balona u pokretu i zemaljskih stanica je specifična *MESH aerial wireless network*. Ovim projektom *Google* nastoji da postane globalni davalac Internet usluga, i da tako učini nerelevantnim sve tradicionalne davaoce usluga koji su razvili infrastrukturu na kopnu. Ukoliko se projekat ostvari, Google će postati vrlo značajan faktor u ekonomskom, medijsko-informacionom i čak u političkom pogledu.

Google, Project Loon, http://www.google.com/loon/.

[247] Conal Urquhart, "Project Loon: Google Plans Balloon Network to Extend Internet Reach," *The Guardian*, 15 June 2013, http://www.theguardian.com/technology/2013/jun/15/project-loon-google-balloon-internet (preuzeto 22. oktobra 2015).

[248] Agence-France Presse, "Project Loon: Google Baloon that Beams Down Internet Reaches Sri Lanka," *The Guardian*, 16 February 2016, http://www.theguardian.com/technology/2016/feb/16/project-loon-google-balloon-that-beams-down-internet-reaches-sri-lanka (preuzeto 17. februara 2016).

[249] Slično projektu *Google Loon*, kompanija *Facebook* razvija projekat Internet.org u kome ogromne i lagane bespilotne letelice *Aquila* (dronovi), pogonjene na solarnu energiju, sposobne da u dugom periodu od tri meseca do pola godine neprekidno lete na visinama od 18.000-27.000 km, uspostavljaju besplatan Internet velikog kapaciteta milijardama ljudi na područjima preko kojih lete u radijusu od 50 km.

Facebook, Internet.org, https://info.internet.org/en/.

[250] Jessi Hempel, "Inside Facebook's Ambitious Plan to Connect the Whole World," *Wired*, January 19, 2016, http://www.wired.com/2016/01/facebook-zuckerberg-internet-org/ (preuzeto 17. februara 2016).

[251] Michael Springer, "57 Cities Now Have Free Wi-Fi, but They're Not Thinking Big Enough," *Mic*, October, 9, 2013, http://mic.com/articles/66891/57-cities-now-have-free-wi-fi-but-they-re-not-thinking-big-enough#.n8ljLl2cL; http://qz.com/414061/helsinkis-free-city-wide-wi-fi-network-is-faster-than-your-home-internet/ (preuzeto 17. februara 2016).

moraju više biti povezani računarima na Internet da bi bili umreženi, već su neprekidno umreženi na neku od mreža ili imaju mogućnost da to budu.

Trend digitalizacije i umrežavanja svega i brojni bezbednosni rizici koje on donosi, doveo je do toga da se danas koristi ogroman broj fizički izolovanih lokalnih, ali i globalnih mreža koje su podrazumevano fizički odvojene od Interneta. Na primer, samo u nadležnosti Ministarstva odbrane SAD, funkcioniše 15.000 zasebnih računarskih informacionih mreža,[252] koje sadrže klasifikovane vojne podatke i servise i koje nisu predviđene da ikada budu povezane na Internet, a prostiru se, poput njega, globalno. To se odnosi i na razne sisteme kritične infrastrukture, kompanijske mreže zatvorenog tipa i druge. Dosadašnja praksa sajber kriminala i sukoba u sajber prostoru je pokazala da se navedeni sistemi biraju kao primarni ciljevi napada. Najpoznatija operacija u sajber prostoru do sada, u kojoj je u dužem periodu upotrebljen skup malicioznih računarskih programa poznat pod zajedničkim nazivom Staksnet (*Stuxnet*), ostvarena je napadom na informacioni sistem i uređaje nuklearnog postrojenja u Natancu, u Iranu, koji su bili u potpunosti odvojeni od Interneta.[253, 254, 255] Ključni trenutak te specijalne operacije, koja je očigledno preduzeta od strane specijalnih obaveštajnih jedinica jedne ili više država,[256,257] bilo je otkrivanje informacija neophodnih za infiltraciju u postrojenje i pripremu softvera za dejstvo na sistem, a to je obavljeno u fizičkom okruženju, van sajber prostora. Dakle, sajber prostor ne postoji samo u okviru globalne mreže, kako to tvrdi

[252] Martin E. Dempsey, "Defending the Nation at Network Speed," (Brookings Institution, 27 June 2013), 5, http://www.brookings.edu/~/media/events/2013/6/27%20cybersecurity%20dempsey/martin%20e%20dempsey%20prepared%20remarks.pdf (preuzeto 12. decembra 2015).

[253] Kim Zetter, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon," *Wired*, November 3, 2014, http://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/ (preuzeto 12. Decembra 2015).

[254] David Kushner, "How Kaspersky Lab Tracked Down the Malware that Stymied Iran's Nuclear-fuel Enrichment Program," *IEEE Spectrum*, February 26, 2013, http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet/ (preuzeto 12. decembra 2015).

[255] Joseph Menn, "Exclusive: U.S. Tried Stuxnet-style Campaign against North Kora but Failed – Sources," *Reuters*, May 29, 2015, http://www.reuters.com/article/us-usa-northkorea-stuxnet-idUSKBN0OE2DM20150529 (preuzeto 14. decembra 2015).

[256] Ellen Nakashima and Joby Warrick, "Stuxnet was Work of U.S. and Israeli Experts, Officials Say," *The Washington Post*, June 2, 2012, https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html (preuzeto 14. decembra 2015).

[257] Nate Anderson, "Confirmed: US and Israel Created Stuxnet, Lost Control of it," *Ars Technica*, June 1, 2012, http://arstechnica.com/tech-policy/2012/06/confirmed-us-israel-created-stuxnet-lost-control-of-it/ (preuzeto 14. decembra 2015).

navedena nemačka strategija[258]. Tehnologija je dovela do stanja u kome svi sistemi i sve izolovane mreže lako mogu biti deo opšteg globalnog sajber prostora, odnosno postoji mogućnost da se između izolovanih sistema i Interneta ili međusobno uvek ostvari mrežna veza ili protok podataka, čak i ukoliko to nije inherentno planirano ili se odvija bez znanja korisnika sistema. U suprotnom, sajber ratovanje bi postalo „Internet ratovanje“, što ne odgovara dosadašnjoj praksi, kao ni sadašnjoj, niti očekivanoj realnosti.

3.3.3. Definisanje sajber prostora

Imajući u vidu karakteristike sajber prostora koje sadrži većina analiziranih definicija država u prethodnom izlaganju, kao i karakteristike koje proističu iz društvenih, tehnoloških i stručnih pristupa primene sajber prostora, može se izvesti sledeća definicija sajber prostora je:

Sajber prostor je ljudska tvorevina stvorena primenom informaciono-komunikacionih tehnologija u elektromagnetnom okruženju u kome se podaci stvaraju, čuvaju, šalju, primaju, obrađuju i uništavaju, čiji su elementi podaci, sistemi, procesi i ljudi koji su umreženi ili mogu biti umreženi.

Karakteristike sajber prostora su:

- sajber prostor je veštačka tvorevina ljudi, zasnovana na primeni tehnologije;
- deo je informacionog prostora;
- postoji na osnovu ili kao deo elektromagnetnog okruženja;
- u njemu se stvaraju, čuvaju, šalju, primaju, obrađuju i uništavaju podaci, odnosno informacije;
- postoji i funkcioniše na osnovu primene računarskih informacionih tehnologija;
- njegovi elementi su podaci/informacije (u digitalnom obliku), informacioni sistemi i infrastruktura, procesi i ljudi kao kreatori, učesnici aktivnosti i procesa;
- karakteriše ga sposobnost ili mogućnost umreženosti i protoka podataka između delova sistema ili između odvojenih sistema;

[258] FR Germany, *Cyber Security Strategy,* 9.

- povezanost između njegovih delova se načelno ostvaruje na nivou podataka, a može biti ostvareno i na fizičkom nivou (fizičke infrastrukture i veze), nivou procesa (uspostavljene veze), nivou ljudi (kao kreatora sajber prostora, faktora koji omogućava njegovo postojanje, korisnika i obrađivača);
- osnova, procesi, efekti i korisnici sajber prostora mogu postojati na fizičkom, logičkom i kognitivnom nivou.

3.4. Slojevi sajber prostora

Osnova sajber prostora se ne nalazi u takozvanom „virtuelnom" prostoru. Sajber prostor postoji u različitim realnim okruženjima. On postoji tamo gde se mogu stvarati, čuvati, saznavati, slati i primati, obrađivati i uništavati informacije primenom računarskih informacionih sistema unutar elektromagnetnog područja. Njegovo okruženje i struktura nisu uniformni. Postojanje sajber prostora se ne zasniva na prirodi okruženja, sadržaju ili organizaciji informacionih sistema i njihovih mreža, već na sposobnosti da se vrše nabrojane manipulacije sa informacijama u elektromagnetnom području i uspostavljanju organizovane veze između sistema na nivou podataka. Takođe, sajber „prostor" uopšte nije prostor u fizičkom smislu, već specifična sredina u kojoj se vrše navedene aktivnosti. U sajber prostoru fizičke veličine, poput prostora i vremena nemaju isti uticaj kao onaj koji ostvaruju u fizičkom svetu. Na primer, elektronska poruka poslata putem *Gmail* servisa[259] ne putuje fizički najkraćim putem između pošiljaoca i primaoca, već ekonomski najisplativijem putem za kompaniju davaoca usluge.

Nortkat iz SANS Tehnološkog instituta[260], opisuje ukupnu „površinu napada" u sajber prostoru kao skup svih ranjivosti koje napadači mogu pronaći, doći do njih i iskoristiti ih za neovlašćeni upad u sistem. Tu površinu napada, sačinjavaju tri konceptualno odvojene površine napada: mrežna, softverska i ljudska.

Po jednom ranijem modelu Vojske SAD, površina napada u sajber prostoru se sastoji od pet slojeva (geografskog, sloja fizičke mreže, sloja logičke mreže, sloja uređaja,

[259] Servis kompanije *Google*, najpoznatiji i najveći svetski onlajn sistem za slanje elektronskih poruka, https://www.google.com/intl/en_us/mail/help/about.html.

[260] *SANS Technology Institute*, privatna organizacija iz SAD koja se bavi informacionom bezbednošću.

„persona“ sloja i sloja ličnosti, organizovanih u tri nivoa: fizičkom, logičkom i društvenom (Tabela 4).

Po doktrinarnom dokumentu Združenog generalštaba Ministarstva odbrane SAD, *Operacije u sajber prostoru*, sajber prostor je jedino nefizičko globalno područje u kome se realizuju civilne i vojne aktivnosti, i koje se „prostire“ kroz tri međusobno zavisne oblasti, sačinjene od različitih struktura:

- fizičke mreže (sredine kroz koju prolaze podaci),
- logičke mreže (koju sačinjavaju pravila, procesi i protokoli, apstrahovani u odnosu na fizičko područje) i
- „sajber-persona“ područja (koje čine ljudi čije aktivnosti zavise od logičkog informacionog područja).[261]

Tabela 4. Slojevi sajber prostora.[262]		
Fizički nivo	Logički nivo	Društveni nivo
Geografska komponenta mreže	Logička komponenta mreže	Komponenta ličnosti
Fizička komponenta mreže		Komponenta sajber ličnosti

Dakle, u savremenom globalnom okruženju politički i bezbednosni efekat dejstava u sajber prostoru se manifestuje na tri nivoa: fizičkom, logičkom i kognitivnom.[263] Sva tri pomenuta područja su međusobno zavisna, povezana i uslovljena. Način na koji sajber napadi ostvaruju posredne posledice na objekte u fizičkom prostoru je rezultat te interakcije računarsko-informacionih sistema, odnosno sajber prostora sa entitetima u pomenutim područjima. Jedan od ključnih uzroka njihove povezanosti je i sveprisutna i rastuća primena računarskih informacionih tehnologija u gotovo svemu. U kratkom vremenskom periodu od deceniju i po, upotreba mobilne telefonije i interneta u svetu je

[261] *Cyberspace Operations: Joint Publication 3-12.*

[262] United States, Department of the Army, Military Operations, *TRADOC Pamphlet 525-7-8, Cyberspace Operations Concept Capability Plan 2016-2028,* February 22, 2010, http://www.fas.org/irp/doddir/army/pam525-7-8.pdf (preuzeto 11. avgusta 2015).

[263] Ibid.

vrtoglavo porasla. [264, 265, 266, 267, 268, 269] U elektronskom informacionom području, ljudi kreiraju takozvane „virtuelne identitete“, pri čemu jedan čovek može imati više takvih identiteta, koji mu služe u svrhu informisanja, zabave ili za profesionalne potrebe. Bez obzira da li se radi o stvarnim ili izmišljenim identitetima, oni ostvaruju nekakav informacioni uticaj u sajber prostoru.

Relevantni subjekti smatraju da će se broj automatizovanih umreženih uređaja koji samostalno obavljaju nekakvu funkciju, u skoroj budućnosti drastično porasti. Po procenama kompanije *Gartner*, broj uređaja umreženih u koncept „Internet stvari“[270] će do 2020. godine dostići 25 milijardi,[271] dok kompanija *Cisco* procenjuje da će taj broj iznositi čak 50 milijardi uređaja[272]. To znači da će po stanovniku Zemlje broj umreženih računarskih uređaja iznositi u proseku 3,5-6,5.

Informacione tehnologije nisu samo kablovske i bežične računarske mreže, koje čine globalnu osnovu sajber prostora, već i sve vrste računarskih sistema, ugrađenih procesora, kontrolera i senzora, koje čine njegovu, po mestu perifernu, a po značaju ključnu nadogradnju. Ta nadogradnja postaje sve šira i važnija zahvaljujući razvoju sposobnosti ugrađenih i perifernih računarsko-informacionih sistema da međusobno stupaju u stalne ili ad hok mreže, bez upotrebe fiksne osnove sajber prostora. Skoro svi savremeni tehnički

---

[264] International Telecommunication Union, *ICT Facts and Figures 2015*, https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx (preuzeto 10. januara 2016).

[265] International Telecommunication Union, *Global ICT Developments*, 2001-2015, https://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2015/stat_page_all_charts_2015.xls (preuzeto 10. januara 2016).

[266] Ibid.

[267] *Metadata for Percentage of Individuals Using Internet 2000-2014* (Excel datoteka), https://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2015/Individuals_Internet_2000-2014.xls (preuzeto 10. januara 2016).

[268] *Mobile-cellular Telephone Subscriptions 2000-2014* (Excel datoteka), https://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2015/Mobile_cellular_2000-2014.xls (preuzeto 10. januara 2016).

[269] ICT Data and Statistics Division, Telecommunication Bureau, International Telecommunication Union, *ICT Fact & Figures*, https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf (preuzeto 10. januara 2016).

[270] Engl. *Internet of Things* (IoT).

[271] Gartner, „Gartner Says 4.9 Billion Connected “Things” Will Be in Use in 2015,” press release, Bacelona, Spain, November 11, 2014, http://www.gartner.com/newsroom/id/2905717 (preuzeto 10. januara 2016).

[272] Dave Evans, Cisco, *The Internet of Things: How the Next Evolution of the Internet Is Changing Everything*, White Paper (April 2011), http://www.iotsworldcongress.com/documents/4643185/0/IoT_IBSG_0411FINAL+Cisco.pdf (preuzeto 10. januara 2016).

sistemi, uključujući medicinske uređaje, sredstva za identifikaciju, finansijske transakcije, vozila, industrijske sisteme imaju ugrađene senzorske, kontrolerske ili računarske informacione tehnologije. Obim u kome ljudi i životinje, tehnički sistemi, industrijska infrastruktura, objekti i okruženje zavise od navedenih sistema, uvezanih u sajber prostor je sve veći. U nekim slučajevima, poput razvoja autonomnih vozila na kopnu, u vazduhu ili vodi, informacione tehnologije stvaraju revolucionarno ili disruptivno dejstvo. To važi i u području razvoja i upotrebe vojnih borbenih i neborbenih sistema.

Sa rastom značaja informacionih sistema za sisteme, ljude i svet, raste i ozbiljnost posledica napada na te sisteme. Informacioni sistemi imaju inherentne i implicirane nedostatke. Napadači koriste te nedostatke za napad na informacionu bezbednost sistema, izazivajući direktne i izvedene posledice. U skladu sa tim raste i moć dejstava sajber napada. Što je veća funkcionalna povezanost svih entiteta koji sačinjavaju fizički, logički i društveni sloj sajber prostora, veći su i domet i efekti napada u sajber prostoru. Veze između sistema i ljudi u sajber prostoru su automatizovane, odvijaju se u realnom vremenu i ljudi su često nesvesni tehničke strane te interakcije. Međutim, ta veza omogućava da se direktna dejstva sajber napada u logičkom području sajber prostora prenose na fizičko područje, uključujući i živi svet.

Na fizičkom nivou sajber prostor je efikasno podeljen na delove u nadležnosti državnih suvereniteta. Po projektu *EastWest* Instituta pod nazivom *Osnove kritične terminologije 2*, „sajber infrastruktura“ (infrastruktura sajber prostora) predstavlja „skup ljudi, procesa i sistema koji čine sajber prostor“[273]. Sistemi (fizička infrastruktura) i lica podležu jurisdikciji nacionalnih sudova i savremena praksa pokazuje da informacione tehnologije to ne mogu da promene ni u čemu. Po Raušeru, infrastrukturu sajber prostora čine sledeći ključni elementi:

1. Okruženje (objekti, prirodno okruženje i fizički prostor u kome fizička infrastruktura postoji);
2. Energija (električno napajanje koje omogućava funkcionisanje hardvera i procesa);

[273] Godwin, Kulpin, Rauscher and Yaschenko, eds., *Russia-U.S. Bilateral*, 18.

3. Hardver (procesori, čipovi, provodnici, kablovi, uređaji itd.);
4. Softver (izvorni kod, baze podataka, algoritmi, aplikacije, protokoli itd.);
5. Mreže (mrežne veze, čvorišta, topologije);
6. Elektronski sadržaj (podaci i informacije, generisani podaci o procesima i saobraćaju, greške i namerni prekidi u funkcionalnosti stanja i toka informacija);
7. Ljudi (autori softvera i hardvera, tehničari koji implementiraju sisteme, operatori, osoblje koje održava sisteme i mreže, korisnici) i
8. Propisi i pravila (sporazumi, standardi, politika, regulative itd.).[274]

U skladu sa trendom razvoja računarskih nauka i informacionih tehnologija, navedenim elementima bi trebalo dodati i dva dodatna:

- Sisteme (tehničke, društvene, organizacione, sajber prostor je sistem sačinjen od sistema) i
- Inteligentnu nameru (ciljeve, interese i volju ljudi, kao i izabrani pravac delovanja automatizovanih sistema i inteligentnih sistema veštačke inteligencije).

Sajber prostor je kompleksan po formi, strukturi i logički zasnovanim procesima. Po formi, sajber prostor nije ograničen vidljivim granicama poput geografskih prostora, kopna, mora, vazduha ili svemira, već je amorfan i nestalan, uz tendenciju širenja, kako se povećava zastupljenost i domet informacionih tehnologija.[275] U sajber prostoru dimenzije prostora i vremena nemaju isto značenje kao u fizičkom prostoru. Međutim, sajber prostor nije virtuelni[276], apstraktni fenomen zasnovan na informacijama i idejama koji nema materijalnu komponentu, niti je nezavistan od fizičkog okruženja.

Osnova sajber prostora jesu logički odnosi koji omogućavaju procese i manipulaciju podacima. Ti procesi i aktivnosti se odvijaju u logičkom području, ali unutar infrastrukture koja se prostire u fizičkom području. Oni imaju uzroke i ostvaruju efekte na fizičko i informaciono okruženje. U pogledu strukture i uzročno-posledičnih odnosa,

[274] Karl F. Rauscher, "Protecting Communications Infrastructure," *Bell Labs Technical Journal* 9, no. 2 (2004): 1-4.

[275] Alexander Hellemans, „Two Steps Closer to a Quantum Internet," *IEEE Spectrum*, December 30, 2015, http://spectrum.ieee.org/telecom/security/two-steps-closer-to-a-quantum-internet (preuzeto 10. januara 2016).

[276] Virtuelan – (fr. virtuel, lat. virtus – sposobnost, valjanost, snaga (ali se ne koristi tom sposobnošću), prividan, suprotno od realan), Milan Vujaklija, *Leksikon stranih reči i izraza*, Treće izdanje (Beograd, Prosveta, 1980), 152.

sajber prostor se ne može efektivno posmatrati kao fenomen u jednoj realnosti (ravni posmatranja) u jednom trenutku vremena, već istovremeno u više njih, pri čemu su podaci (informacije) ključni zajednički faktor na kome počiva veza sva tri sloja.

Kao primer za razumevanje ovakvog modela sajber prostora, može se analizirati način funkcionisanja nekog uobičajenog servisa, poput sistema elektronskih poruka. Kada neka osoba pošalje elektronsku poruku, ta poruka, odnosno informacija, putuje u obliku elektronskih signala i mnoštva paketa podataka kroz fizičku infrastrukturu sajber prostora, koja se često prostire na velikim fizičkim udaljenostima. Infrastrukturu čine računari, kablovi, radio talasi, ruteri lokalnih, nacionalnih i usputnih davalaca internet usluga, međukontinentalni optički kablovi za prenos informacija, serveri pružaoca usluge elektronskog servisa, računari u kojima informacija biva obrađena, baze podataka i sistemi za fizički smeštaj podataka u kojima se informacija zapisuje i čuva, procesori koji obrađuju informacije.

Vreme koje je potrebno da se izvrši ta operacija malo zavisi od fizičke udaljenosti, a više od načina rada aplikacija i procesora. I putanja kojom signali fizički prolaze ne zavisi samo od geografskog položaja učesnika komunikacije, već od cene operacije, pa poruke putuju najjeftinijim putem po davaoca usluge, a ne fizički najbližim putem. Ta putanja nije unapred utvrđena, već se kreira automatski u toku samog puta, na osnovu matematičkih algoritama, odnosno logičkih pravila i instrukcija za kretanje podataka, funkcionisanje servisa, protokola i sistema prenosa podataka. To su, na primer, *Domain Namer System* (DNS), *Border Gateway Protocola* (BGP) ili *Transmission Control Protocol/Internet Protocol* (TCP/IP). Navedeni i drugi protokoli stvaraju jedinstveni i kompleksan sistem u kome su jednoznačno određene adrese svih učesnika[277], kao i svaki pojedinačni paketi podataka, čime se postiže da svaki deo informacije ima jedinstveno mesto u okviru nje, bez obzira na put kojim se kreće. Oni omogućavaju fizičkim uređajima da automatski komuniciraju razmenjujući informacije i određuju puteve kretanja paketa podataka. Ta logička pravila određuju i način na koji se poruke dele na pojedinačne pakete podataka, način njihovog slanja, prosleđivanja i primanja i druge

[277] Pošiljalaca, primalaca i usputnih stanica.

aktivnosti. Ta pravila su standardizovana, što znači da u bilo kom delu jedinstvene mreže, isti uzrok uvek izaziva istu posledicu.

Konačno, svaka poruka ili multimedijalni sadržaj ima svoje kognitivno značenje, odnosno neku saznajnu, ekonomsku, umetničku, ili pravnu vrednost, odnosno kvalitet. Elektronsku poruku je neko sačinio. Taj „neko“ ima svoj onlajn identitet, predstavljen nalogom elektronske pošte. Bez obzira da li je identitet u sajber prostoru stvaran ili lažan i da li predstavlja organizaciju ili pojedinca, iza njega se nalazi neki sistem, stvarno fizičko lice ili društvena organizacija.

3.4.1. Veza između fizičkog, logičkog i kognitivnog nivoa sajber prostora

Podaci omogućavaju logičku, fizičku i kognitivnu vezu između sva tri sloja sajber prostora. Sajber prostor sačinjavaju različiti sistemi (uređaji i softver), procesi i učesnici. Neki od njih koriste iste standarde, a neki ne. Bez obzira na to, osnove svih informacionih tehnologija moraju biti zajedničke da bi postojala mogućnost međusobne interakcije na nivou podataka. Te osnove se nalaze u samom načinu matematičko-logičke interpretacije i obrade podataka. Isti podatak može postojati u različitim oblicima zapisa, ali u svima njima mora imati istu vrednost. Takođe, mora postojati mogućnost da svaki podatak bude neograničen broj puta konvertovan u neki drugi oblik zapisa[278]. Čuvanje, obrada (procesiranje), slanje i primanje podataka se obavlja uz pomoć tehničkih sistema[279] koji su deo fizičkog sveta i logičkog okruženja i imaju sposobnost da vrše obradu informacija[280].

Podaci imaju numeričku vrednost, predstavljaju informacije i mogu biti zapisani u obliku signala. Da bi ostvarili interakciju sa fizičkim svetom, podaci se prevode u signale i obrnuto. U opštem smislu, signal predstavlja funkciju koja nosi informaciju o ponašanju ili atributima nekog fenomena. U teoriji informacija signal predstavlja kodifikovanu poruku. Tradicionalno, signal predstavlja „fizičku manifestaciju informacije koja se

[278] U savremenoj praksi u elektromagnetnom obliku: elektronskom, magnetnom, svetlosnom ili kvantnom.

[279] Hardvera (uređaja i infrastrukture), odnosno softvera (baza podataka, programa, odnosno bilo koja logička pravila za izvršavanje programiranih naredbi).

[280] U savremenom okruženju, u digitalnom obliku.

menja kroz prostor i/ili vreme“ [281], ali isto tako i apstraktnu informaciju koja postoji u informacionom ili biološkom području (na primer molekul DNK sagrađen od gena)[282]. Pri tome je obrada signala „tehnologija koja omogućava obuhvatanje fundamentalne teorije, aplikacija, algoritama i primene obrade ili prenosa informacija koje postoje u mnogim različitim fizičkim, simboličkim ili apstraktnim oblicima generalno označenim kao signali i koja koristi matematičke, statističke, računarske, heurističke i/ili lingvističke reprezentacije, formalizme i tehnike za predstavljanje, modelovanje, analizu, sintezu, otkrivanje, oporavljanje, očitavanje, dobavljanje, izdvajanje, učenje, bezbednost ili forenziku“[283].

Prema načinu distribucije vrednosti signalne funkcije u odnosu na vreme, signali mogu biti analogni, digitalni ili kvantni[284]. Analogni signali su kontinualno promenljive vrednosti po intenzitetu (amplitudi) i frekvenciji u vremenu. Dok se čovečije opažanje sveta zasniva na analognim signalima (vid, zvuk, miris, ukus, dodir), savremene računarske informacione tehnologije, zasnovane na tranzistorima u procesorima, se zasnivaju na obradi digitalnih podataka i signala. Za stvaranje digitalnih signala je pogodna primena različitih vrednosti pojava u elektromagnetizmu, poput promene napona električnog impulsa ili njegovo prekidanje, prisustva ili odsustva namagnetisanosti malog područja magnetnog medija, vrednosti radio signala, intenziteta ili postojanja svetlosnog signala i sličnih. U kvantnom računarstvu, koje se zadržava u području elektromagnetizma, od značaja za stvaranje signala je određivanje superpozicije (omogućava veći broj istovremenih stanja), odnosno stanja kubita.

Zbog navedene činjenice da se podaci mogu pretvarati u različite vrste signala, nije ispravno nazivati sajber prostor „digitalnim područjem“, pošto su digitalne tehnologije preovlađujuće u savremenim tehničkim sistemima, ali ne i jedini mogući oblik predstavljanja i obrade podataka. Postoje razvijeni sajber napadi koji koriste različite

[281] Jose M.F. Moura, „What Is Signal Processing?“, *IEEE Signal Processing Magazine*, 26, no. 6 (2009), 6, http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5230869 (preuzeto 18. avgusta 2015).

[282] Ibid.

[283] Ibid.

[284] Yonina Chana Eldar, „Quantum Signal Processing,“ (PhD diss., Massachusetts Institute of Technology, Cambridge, 2002), https://dspace.mit.edu/bitstream/handle/1721.1/16805/50544999-MIT.pdf?sequence=2 (preuzeto 20. avgusta 2015).

vrste manipulacije podacima koje koriste, na primer, zvučne talase i toplotno zračenje, za interakciju sa računarima, dakle analogne informacije. Vrsta zapisa podataka u signale zavisi od tehnologije i to nije suština sajber prostora, odnosno sajber sukoba. Njegova suština je manipulacija podacima i njihov transfer između fizičkog, logičkog i kognitivnog nivoa sajber prostora u cilju narušavanja informacione bezbednosti sistema.

Funkcionisanjem i povezivanjem računarskih informacionih sistema nastaje sajber prostor. U sajber prostoru se podaci čuvaju, nastaju, šalju i primaju, obrađuju i uništavaju. Tehnički sistemi uvek obavljaju svoju funkciju manipulišući podacima. Na logičkom nivou to radi softver, a na hardverskom procesori. Mikroprocesori ili centralne procesorske jedinice (eng. *Central Processing Unit* – CPU)[285] kopiraju digitalne podatke i međusobno ih upoređuju. Procesore sačinjavaju tranzistori[286], koji su napravljeni od poluprovodničkih materijala i vrše pojačavanje električnog signala ili njegovo prekidanje. U zavisnosti od njihove funkcije, vrednost osnovne informacije, *bita*,[287] može biti *1* ili *0*, pa se u računarskoj tehnologiji primenjuju digitalna elektronika i binarni brojčani sistem. Po rečniku Meriam-Vebster, bit predstavlja „fizičku predstavu osnovne informacije pomoću električnog impulsa[288], namagnetisane tačke[289], ili perforirane rupice[290] čije

[285] Mikroprocesori su računarski procesori smešteni na jedno ili više integralnih kola, sposobni da izvršavaju funkcije centralnih procesorskih jedinica (CPU) zahvaljujući svojstvu da mogu da procesiraju (obrađuju) digitalne podatke koji u njih ulaze, na osnovu logičkih instrukcija koje su ugrađene u njihovu memoriju, dajući obrađene vrednosti kao rezultat na izlazu. Zbog funkcionalne strukture tranzistora, od kojih su procesori sačinjeni, da funkcionišu sa dva jednostavna stanja u kojima električni signal prolazi ili je prekinut, procesori koriste binarni brojni sistem u kome postoje samo dve brojne vrednosti 0 i 1 (da/ne ili tačno/pogrešno). Svaka od ovih vrednosti predstavlja pojedinačni *bit*, odnosno osnovnu jedinicu informacije u računarstvu.

[286] Tranzistor je uređaj izgrađen od poluprovodničkog materijala koji pojačava električni signal ili strujni tok ili služi kao njegov prekidač. U prakasa ima najmanje tri konektora za povezivanje sa spoljnim strujnim kolom. Može se koristiti samostalno, ali je njegova ključna sposobnost modularnost, koja omogućava da se veći broj tranzistora integriše u jedno strujno kolo. Izumeo ga je Džulijus Lilenfeld (Julius Lilenfeld) 1926. godine, a praktično je napravljen od strane fizičara u Belovoj laboratoriji 1947. godine.

Stan W. Amos and Mike R. James, *Principles of Transistor Circuits* (Woburn, MA: Newnes Butterworth-Heinemann, 2000).

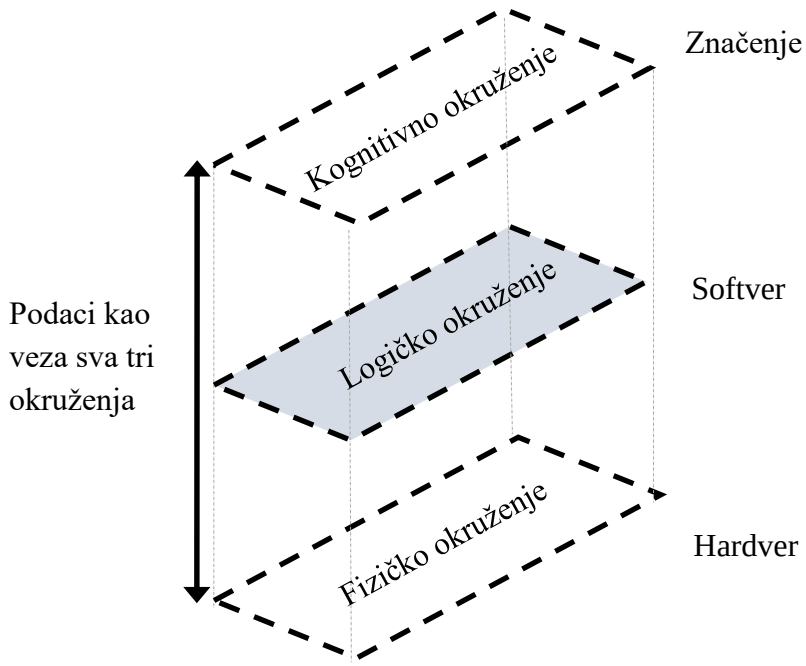
[287] Bit je osnovna vrednost informacije u računarstvu. Po rečniku *Merriam-Webster* bit predstavlja „jedinicu računarske informacije koja je ekvivalentna rezutatu izbora između dva alternativna stanja (*da* ili *ne, uključeno* ili *isključeno*)“. 4 bit (noun), *Merriam-Webster*, s.v. „bit“ http://www.merriam-webster.com/dictionary/bit (preuzeto 23. januara 2016).

[288] Impuls u području obrade signala. Područje obrade signala se bavi ekstrakcijom informacija iz električnog signala.

[289] Na namagnetisanom materijalu

[290] Na perforiranoj papirnoj kartici ili traci (prvobitni način zapisa podataka u računarstvu, koji su koristile elektromehaničke ili električne mašine za obradu podataka.

prisustvo ili odsustvo indicira podatak“[291] Tranzistori se mogu koristiti samostalno, ali im je ključna osobina modularnost, zbog koje se mnogo pojedinačnih tranzistora može sastaviti u jedinstveni sklop, na primer integrisano kolo[292]. Proširenjem strukture i funkcionalnosti integrisanog kola dobija se mikroprocesor.



Slika 5. Konceptualni prikaz slojeva (okruženja) sajber prostora

Podaci su ključni entitet u računarskim informacionim tehnologijama koji povezuju funkcionisanje softvera, zaduženog za logičku manipulaciju podacima i ostvarivanje međusobne interakcije (logički nivo), hardvera, koji fizički obrađuje podatke i usmerava tok signala (fizički nivo), i ljudi, koji koriste softver i hardver na višem nivou reprezentacije. Mikroprocesori vrše svoju funkciju sa podacima (u elektronskom obliku) primenjujući matematičke (aritmetičke ili logičke) operacije, definisane softverskim instrukcijama koje su integrisane u njihov dizajn. Međutim, zahvaljujući ograničenom

[291] *Merriam-Webster*, s.v. „bit“.

[292] Integrisano električno kolo ili kraće integralno kolo je složeni elektronski uređaj koji je sastavljen od više pojedinačnih uređaja, uglavnom tranzistora, namenjeno za ugradnju u druge složene elektronske sisteme. U opštem slučaju, integralno kolo se sastoji od monolitnog elektronskog sklopa sa mnoštvom ugrađenih tranzistora (čipa), koji je postavljen na jedinstvenu podlogu, kućišta i odgovarajućih priključaka koji mu omogućavaju priključenje u složenije elektronske sisteme.

broju elementarnih radnji tranzistora, procesori su u stanju da ostvaruju samo jednostavne matematičko-logičke operacije upoređivanja, kopiranja, dodavanja, oduzimanja ili prebacivanja brojeva, odnosno podataka iz jednog skupa u drugi. To im daje sposobnost da prevode kvantitet u kvalitet. Jednostavnost funkcije procesora se prevodi u složenost multicipliranjem njihovog broja. Broj tranzistora u integrisanom kolu je proporcionalan procesorskoj snazi. Što je više tranzistora u integralnom kolu, a kola u mikroprocesoru, to je veća sposobnost procesora da izračunava zadate operacije i izvodi instrukcije zadate softverom u jedinici vremena. Procesori se sastoje od više jezgara, a računari mogu da sadrže više procesora. Tehnologija izrade i serijske proizvodnje procesora neprekidno se unapređuje, tako da savremeni procesori sadrže i do 15 miliona tranzistorskih kola po 1 mm^2, odnosno ukupno i više milijardi po procesoru, a taj se broj zahvaljujući novim dometima nauke i tehnologije povećava.

Tehnologija koja omogućava savremenim procesorima veliku procesorsku snagu da vrše složena izračunavanja u vrlo kratkom vremenu je tehnologija njihove proizvodnje i konstantnog povećanja broja tranzistora na ograničenom prostoru. Taj rast sposobnosti tehnološke proizvodnje je u proteklih pedeset godina bio eksponencijalan i predvideo ga je inženjer Gordon Mur, jedan od suosnivača kompanije Intel. [293] On je 1965. godine predvideo da će se broj tranzistora u integrisanom kolu (zasnovanom na poluprovodničkoj tehnologiji baziranoj na primeni silicijuma) po minimalnoj ceni proizvodnje udvostručavati svake godine, i da će taj trend trajati najmanje jednu deceniju.[294] To je naknadno revidirao i predvideo da će se taj rast u budućnosti odvijati duplo sporije.[295, 296] U svakom slučaju, fizička ograničenja za beskonačan napredak tehnologije preko granice prirodnih zakona postoje i stručnjaci previđaju skori kraj navedene tendencije u pogledu

[293] Intel Corporation iz Santa Klare u Kaliforniji, SAD je najveća svetska kompanija za proizvodnju poluprovodničkih čipova (mikroporocesora), http://www.intel.com/

[294] Moore, "Cramming More Components."

[295] Computer History Musem, *Moore's Law,* http://www.computerhistory.org/revolution/digital-logic/12/267 (preuzeto 5. oktobra 2015).

[296] Intel Corporation, "Over 6 Decades."

primene silicijumskih materijala.[297, 298] Međutim, nauka razvija nove materijale i načine obrade podataka, poput, na primer kvantnog računarstva.

Podaci predstavljaju i vezu između softvera i hardvera. Softverski sistemi predstavljaju skup algoritama/instrukcija napisanih u nekom programskom jeziku sa ciljem da usmere procesore da izvode zadate aktivnosti sa podacima. Bez obzira da li je reč o sistemskom ili aplikativnom softveru, ova svrha uvek postoji, direktno ili indirektno. Podaci su zajednička veza između različitih vrsta softvera, odnosno između softvera napisanih različitim programskim jezicima. Svi programski jezici su zasnovani na istoj matematičkoj logici, uz različit način i nivo predstavljanja naredbi. U programiranju je uobičajena procedura da se složeni programi (softverski sistemi) pišu primenom više različitih programskih jezika. Izvršavanje komandi tih programskih blokova se mora usaglasiti kako bi oni mogli da dele zajedničke resurse (servisa, procesora, podataka). Da bi se međusobno usaglasilo izvršavanje komandi tih programskih blokova primenjuju se različite programske tehnike poput takozvanog „premošćavanja“ (eng. *bridging*) ili „ugrađivanja“ (eng. *embedding*), primene koncepta „crnih kutija“ (eng. *black box*) ili zajedničkih deljivih „biblioteka“ (eng. *shared libraries*). Iako navedene tehnike programiranja koriste različite metode interakcije u odnosu na procese i servise, u krajnjem slučaju one se uvek odnose na rad sa podacima primenom iste matematičke logike.

Bez obzira na način obrade signala, u osnovi sajber prostora uvek postoje podaci i matematičko-logičke instrukcije. Oni ujedno predstavljaju i vezu koju sajber prostor pravi između informacionog i fizičkog okruženja. Veza podataka sa kognitivnim okruženjem je sadržana u značenju vrednosti koju podaci reprezentuju.

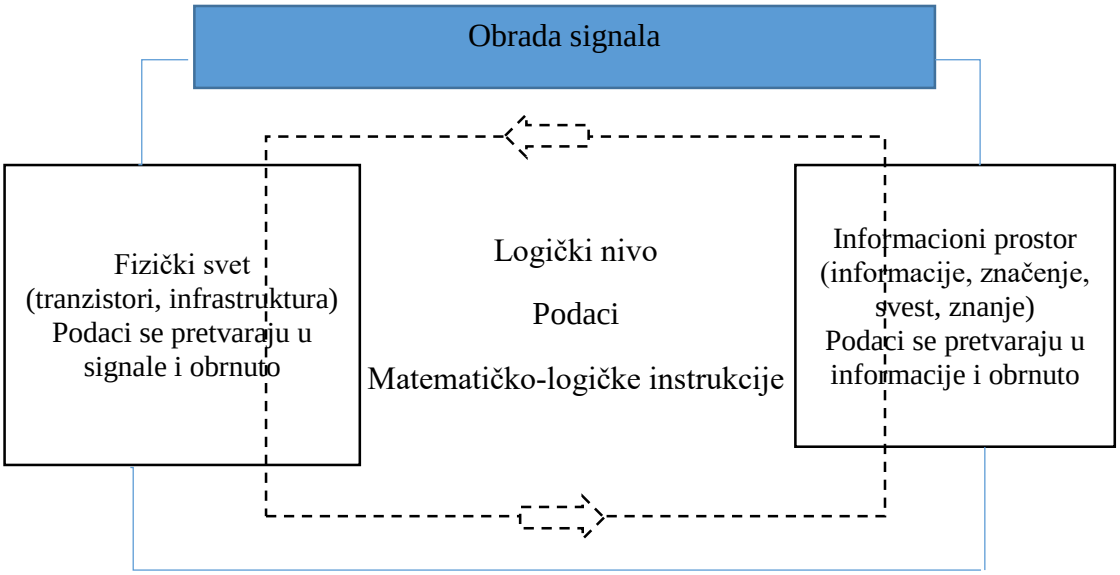
U kontekstu računarskih nauka, podaci i programi predstavljaju dve opšte kategorije softvera. Softver ili logičko područje sajber prostora je ključna veza koja povezuje fizički svet sa informacionim područjem značenja i predstavlja osnovu prirode sajber prostora. Međutim, softver se ne može posmatrati samostalno, već kao deo šireg sistema u kome

[297] Joel Hruska, ExtremeTech, „Intel’s Former Chief Architect: Moore’s Law Will Be Dead Within a Decade,“ August 30, 2013, http://www.extremetech.com/computing/165331-intels-former-chief-architect-moores-law-will-be-dead-within-a-decade (preuzeto 23. januara 2016).

[298] Anirudh Regidi, „Moore’s Law: The Legendary Computing Rule is Dying, Thanks to Smartphones,“ *Firstpost*, February 16, 2016, http://tech.firstpost.com/news-analysis/moores-law-the-legendary-computing-rule-is-dying-thanks-to-smartphones-299363.html (preuzeto 23. januara 2016).

postoji fizička infrastruktura i kognitivna sfera značenja, pri čemu su ti slojevi povezani stanjima i procesima.

Iako je sajber prostor veštačka tvorevina ljudi, njegova funkcija ne zavisi nužno od ljudi. Potpuno je svejedno da li je neki proces ili podatak generisao čovek ili tehnički sistem. Potpuno je svejedno da li ontološko značenje pojma ili značenje neke informacije razume čovek ili sistem veštačke inteligencije. Dakle, sajber prostor ne zavisi primarno od učesnika, već od stanja i procesa.



Slika 6. Redukovan model sajber prostora zasnovan na podacima i logičkim instrukcijama

Takođe, važno je imati u vidu da tehnologija ne predstavlja samo tehničke veštačke sisteme, već i biološke veštačke sisteme. Informacija se može uskladištiti i obrađivati i u živim sistemima. U njima se informacije takođe predstavljaju signalima i obrađuju u živim tkivima koji su evoluirali u tu svrhu. Sistem DNK je jedan od najefikasnijih prirodnih načina za masovno, trajno i pouzdano skladištenje i upotrebu veoma važnih informacija. Greška u tom sistemu donosi bolest i defekte živom biću, ali ne nužno. Nekada te greške mogu ostati bez uticaja na razvoj i funkcionisanje živog bića (bioloških sistema), dovesti do drugačijih karakteristika, pa čak i do poboljšanja njihovih

sposobnosti. I u tom slučaju postoji trijada nivoa tog jedinstvenog okruženja zasnovanog na informacijama: fizički nivo (tkiva), logički nivo (pravila ustrojstva DNK, neurona i ćelija) i kognitivno-informacioni nivo (značenje gena, nervnih signala, misli, ćelijskih hemijsko-bioloških procesa za živo biće). Kada o veštačkim živim biološkim sistemima govorimo sa aspekta nauke, a ne etike, takođe je reč o tehnologiji, kao i u slučaju elektronike ili mašinstva. Konačno, veštački živi sistemi stvoreni na osnovu tehnološkog inženjeringa su već pravno patentirani kao „proizvodi“, pri čemu od nacionalnog zakonodavstva zavisi da li je granica tome na biljnim, životinjskim ili ljudskim organizmima, živim bićima ili tkivima ili hibridnim živim bićima, čija je genetska struktura dobijena kombinovanjem različitih vrsta živih organizama. Takvi sistemi će se neizostavno razvijati u budućnosti, pri čemu je jedina dilema u tome kako će biti prihvaćeni etički i moralni obziri, odnosno kada će tehnologija dostići komercijalno prihvatljive načine veštačke „proizvodnje“ tehnološki modifikovanih živih sistema.

Dakle, bez obzira da li se radi o tehničkim ili biološkim sistemima, sajber prostor uvek označava tehnološki stvoreno okruženje, u kome se postojanje podataka i manipulacija njima ostvaruje na fizičkom, logičkom i informaciono-kognitivnom (saznajnom) nivou i u kome postoji mogućnost umrežavanja na nivou podataka. Pitanje je, kako se u tom okruženju ostvaruje ratovanje, i šta je izvor i cilj napadačkog dejstva?

4. SAJBER SUKOBI

Nakon završetka Hladnog rata, nastupio je novi vojno-bezbednosni kontekst, koga karakteriše difuzno i raznovrsno okruženje, zadržavanje nuklearne pretnje i nova, prilagođena struktura vojne organizacije. Nuklearna vojna tehnologija je toliko razvijena da je svaka strana u Hladnom ratu sigurno mogla da uništi protivnika, bez obzira na rezultat rata. U ratu koji podrazumeva upotrebu nuklearne tehnologije ne bi bilo pobednika. Zbog toga se američki koncept proširuje na vid vojnog dejstva koji, pored raspolaganja nuklearnim kapacitetima, obuhvata i pametnu kombinaciju vojnih dejstava i delovanja na društveni i psihološki status protivnika kao sistema, čiji centar odlučivanja je potrebno učiniti ranjivim i nesposobnim da donosi dobre odluke (čime se umanjuje njegova sposobnost pokretanja i vođenja oružane borbe). Istovremeno, u svetu se pojavljuje veći broj manjih pretnji po bezbednost i nacionalne ciljeve sila. Američki admiral Cebrovski ističe da standard nove vojne strukture postaje veći broj manjih, sinhronizovanih vojnih jedinica, kojima tehnologija omogućava umrežavanje i veću efikasnost i operativnost: "Mi smo u dobu malih, brzih i mnogobrojnih"[299]. Ovakva situacija iziskuje promenu postojeće vojne strategije i doktrine, koja zahteva sposobnost umrežavanja tih brojnih i raznovrsnih elemenata. Navedena ideja predstavlja osnov modela mrežnocentričnog ratovanja.[300] Taj model je komplementaran sa prethodnim konceptima vojne organizacije u SAD, poput Šelingove "Strategije sukoba"[301] i posebno, Vordenovog koncepta uticaja na centar gravitacije protivnika.[302]

---

[299] Arthur Cebrowski, quoted in Samantha L. Quigley, „Transformation Chief Outlines Strategy for New Battlefield", *American Forces Press Service*, 5 August 2004, http://www.au.af.mil/au/awc/awcgate/transformation/oft_cebrowski_new_battlefield_strategy.pdf (preuzeto 9. septembra 2015).

[300] Arthur K. Cebrowski, and John J. Garstka. "Network-centric warfare: Its origin and future," *US Naval Institute Proceedings*, 124, no. 1 (1998): 28-35.

[301] Thomas C. Schelling, *The Strategy of Conflict*, (Cambridge, MA: Harvard University Press, 1960). Matematičar i ekonomista Tomas Šeling je razvio matematički koncept teorije igara u kojem je predstavio model društvenih odnosa suprotstavljenih strana u kome u istom trenutku postoji i interes i za sukob i za saradnju.

[302] John A. Warden III, „The Enemy as a System," *Airpower Journal*, (Spring 1995), http://www.airpower.maxwell.af.mil/airchronicles/apj/apj95/spr95_files/warden.htm (preuzeto 5. septembra 2015).

Pukovnik Džon Vorden je razvio teoriju nelinearnog sukoba pod nazivom „Pet prstenova", po kojoj se protivnik posmatra kao sistem pet koncentričnih komponenti: rukovodstva, resursa, komunikacije, stanovništva i vojske. U cilju efikasnog dejstva, potrebno je razviti vlastitu sposobnost za dejstvo po bilo kom krugu bez direktnog masovnog sukobljavanja sa neprijateljevim vojnim snagama.

U periodu koji je usledio, mnoge nacije su, kako je vreme kasnije pokazalo, pogrešno razumele i prihvatile ovu ideju, nastalu u SAD. Njihova odluka je bila političke, a ne vojne prirode. Svetska ekonomska kriza početkom 21. veka i unipolarno okruženje koje je rezultiralo širenjem NATO saveza na Istok, doveli su do trenda naglog smanjivanja oružanih snaga i vojne moći među evropskim državama. Političari rukovode vojskom u ratu i miru. To znači da su u situaciji da donose političke odluke koje se tiču primene specifične vojne teorije i prakse i da svojim usmeravanjem utiču na taj sistem znanja i veština. Oni su to učinili podstaknuti situacijom u okruženju, za koju su bili karakteristični ekonomski problemi i izmenjena vojno-politička situacija u svetu, a ne onim principima koje su određivali interesi SAD da prilagode sopstvenu strukturu u cilju razvoja sposobnosti manifestacije vojne moći u svetu. Dinamično povezivanje brojnih manjih delova u jedinstvenu celinu zahteva postojanje jedinstvene mreže koja preuzima funkcije, sposobnosti i zadatke prethodnih velikih i neumreženih celina. Bez te mreže, umanjivanje ukupne brojnosti, smanjivanje veličine i decentralizacija strukture imaju negativne, a ne pozitivne efekte na ukupnu vojnu moć i redukuju ukupnu moć jedinstvene organizacije. Česte promene strukture oružanih snaga u procesu traženja rešenja za angažovanje minimalnih vojnih kapaciteta u periodu nakon detanta do današnjih dana dodatno su oslabile sposobnost za odbranu tih država. Brojčano manje i operativno slabije snage u odsustvu mrežnocentričnog okruženja postale su ukupno vojno slabije od prethodnih, tradicionalnih struktura vojnih snaga. To je često obrazlagano novim bezbednosno-odbrambenim ciljevima tih država, iako se suštinski, za većinu država oni nisu značajno promenili. Na primer, iako je terorizam u svetu postao zastupljeniji, nisu sve države u svetu podjednako ugrožene od njega. Jedina država sposobna da ostvari globalno mrežnocentrično okruženje bila je SAD, zahvaljujući svom neproporcionalno visokom vojnom budžetu u odnosu na sve druge države sveta. Ideju mrežnocentričnosti su prihvatili i vojni sistemi najbližih saveznika SAD, poput Australije, Britanije, Kanade, zbog učešća u jedinstvenim vojnim sistemima saveza "Pet očiju", kao i pojedine države NATO, čije je strategijsko opredeljenje u oblasti odbrane blisko povezano sa aktivnostima SAD.

Ideja primene informaciono-komunikacionih tehnologija kao ključnog faktora koji omogućava mrežnocentričnost vojnih operacija u državama koje nisu učestvovale u programima ovakvog tipa nije imala ni potrebe ni osnove. Međutim, to ne znači da druge

vojne sile nisu razvijale vlastite vojne organizacione sisteme u pravcu intenzivne primene informaciono-komunikacionih tehnologija u skladu sa drugačijim modelima. Mrežnocentričnost vojne organizacije u SAD je ključni faktor zbog koga je bio neophodan razvoj strukture sajber prostora i sposobnosti zasnovanih na njemu. Za Vojsku SAD postojanje i funkcionisanje sajber prostora je bio jedini način da se stvori optimalni organizacioni sistem globalno distribuirane vojne strukture.

Vremenom je mrežnocentrično vojno okruženje Vojske SAD raslo i sa ubrzanom digitalizacijom sistema je preraslo u koncept "sistema sistema". Ovaj koncept predstavlja direktnu primenu teorije ili nauke sistema[303] na organizaciju vojnih snaga i model vođenja sukoba. Budući da je bio blisko povezan sa upotrebom informacionih sistema, iz ovog koncepta je ubrzo izrasla potreba za razvoj sposobnosti ispoljavanja nacionalne moći zasnovanih na sajber prostoru.

4.1. Kompleksni vojni „sistemi sistema"

Po teoriji sistema, okruženje u kome se ostvaruje delovanje nacionalnog sistema odbrane je jedan veliki "sistem sistema". Tačnije, svaki oblik sistemske organizacije smatra se "sistemom sistema", bilo da je u pitanju sopstvena struktura ili okruženje. Primena informaciono-komunikacionih tehnologija se smatra važnim faktorom globalizacije na svetskom nivou. Upotreba informacionih komunikacionih sredstava poput televizije, mobilne telefonije i Interneta je omogućila razmenu informacija i ideja između ljudi u svim delovima sveta, ravnomerniju dostupnost znanju i približila različite kulture.[304] U procesu globalizacije posebno se ističe pojava i primena sajber prostora. Međutim, uprkos globalizaciji, a nekada baš zbog nje, sukobi nastavljaju da izbijaju, ali im se menja forma. U skladu s tim, menja se i način organizacije i funkcionisanja sistema odbrane, posebno u pogledu zavisnosti od primene informaciono-komunikacionih tehnologija.

U skladu sa nacionalnim ciljevima, delovi oružanih snaga SAD su raspoređeni i vojno deluju globalno, više od bilo koje druge nacionalne armije. Od 1980. do 2015.godine,

[303] Systems science

[304] Edward Mortimer, „Globalisation ant the Role of United Nations in the 21st Century" (speech at the meeting organized by the Hellenic Foundation for European & Foreign Policy (ELIAMEP) and the United Nations Information Centre, Athens, Greece, January 19, 2001), http://www.eliamep.gr/old/eliamep/files/op0104.PDF (preuzeto 6. septembra 2015).

SAD su aktivno učestvovala u čak 11 ratova, ne računajući tajne i specijalne operacije koje su izvodile Vojska SAD i Centralna obaveštajna agencija (eng. *Central Intelligence Agency* – CIA). Po podacima britanske nevladine organizacije *Biro za istraživačko novinarstvo*, prikupljenim iz lokalnih i svetskih medija, samo u četiri azijske i afričke države (u Pakistanu, Avganistanu, Jemenu i Somaliji) agencija CIA i Vojska SAD su u periodu od započinjanja takozvanog "Rata protiv terora" nakon terorističkih napada na SAD 2001. godine, pa do kraja 2015.godine, izvele ukupno između 1.374 i 1.383 oružana napada bespilotnim letelicama (dronovima), u kojima je poginulo između 6.592 i 10.023 i ranjeno između 1.683 i 2.541 lica.[305] Za daljinsko upravljanje tim dronovima korišćeni su resursi u najmanje 64 specijalizovane avio baze na teritoriji SAD i u 60 takvih baza raspoređenih širom sveta[306]. Pojedinačno najveći broj tih napada, bez obzira gde su se dogodili, izveden je daljinskim upravljanjem iz centara vazduhoplovne baze Krik u Nevadi.[307, 308, 309] Navedene aktivnosti i sposobnosti zahtevaju postojanje pouzdane, bezbedne i efikasne mreže informacionih veza između centara i pokretnih borbenih sistema (često bez ljudske posade) u bilo kom delu sveta. Uspostavljena mreža sistema koja omogućava kreiranje i protok informacija je od suštinske važnosti za manifestaciju vojne moći SAD u svetu, i sama predstavlja sistem koji se koristi u oružanim operacijama i stoga može biti cilj oružanih napada. U tehnološkom pogledu, taj koncept "sistem sistema" je pre svega omogućen razvojem i primenom informaciono-komunikacionih tehnologija. Proces vođenja rata zavisi od mnoštva faktora, kao što su vojna organizacija, raspolaganje sredstvima za ispoljavanje oružane sile, materijalni i ekonomski resursi, stepen organizacije i morala i drugih, a sistem sistema povezuje sve te elemente u

[305] „Get the Data: Drone Wars," *The Bureau of Investigative Journalism*, https://www.thebureauinvestigates.com/category/projects/drones/drones-graphs/ (preuzeto 3. septembra 2015).

[306] Nick Turse, „America's Secret Empire of Drone Bases", *The World Can't Wait*, http://www.worldcantwait.net/index.php/features/covert-drone-war/7447-americas-secret-empire-of-drone-bases (preuzeto 3. septembra 2015)

[307] David Zucchino, „Drone pilots have a front-row seat on war, from half a world away", *Los Angeles Times*, February 21, 2010, http://articles.latimes.com/2010/feb/21/world/la-fg-drone-crews21-2010feb21 (preuzeto 3. septembra 2015).

[308] Craig Whitlock, "Remote U.S. base at core of secret operations," *The Washington Post*, October 25, 2012, https://www.washingtonpost.com/world/national-security/remote-us-base-at-core-of-secret-operations/2012/10/25/a26a9392-197a-11e2-bd10-5ff056538b7c_story.html (preuzeto 4. septembra 2015).

[309] Brian Evarstine, "Inside the Air Force's drone operations", *Air Force Times*, June 22, 2015, http://www.airforcetimes.com/story/military/2015/06/22/air-force-drone-operations-creech/28881503/ (preuzeto 4. septembra 2015).

jedinstvenu, funkcionalnu i efikasnu celinu. To je razlog zbog koga je sajber prostor proglašen petim područjem vojnih operacija.[310, 311]

Pojam "kompleksnosti" se u opštem smislu koristi za označavanje nečega što se sastoji od mnoštva delova koji imaju međusobne odnose koji se najčešće odvijaju na različite načine.[312] Sistem se odnosi na skup elemenata (delova celine) koji su međusobno zavisni, jer stupaju u međusobne interakcije i tako grade jedinstvenu kompleksnu i zamršenu celinu sistema.[313] Po italijanskim profesorima Bertulji i Vaiju "sistemi su objekti sa promenjivim stepenom kompleksnosti"[314]. Iako su navedene definicije "sistema" i "kompleksnosti" generalne, jasno se uočava da ova dva pojma označavaju istu stvar, s tim što je kompleksnost obavezno stanje koje omogućava sistemu da bude to što jeste.

Svaki sistem je kompleksan. Kompleksnost je opšta karakteristika sistema, jer se sistem sastoji od elemenata koji ne mogu samostalno postojati, i bez interakcije tih elemenata između sebe i sa spoljnim okruženjem.[315] Kompleksnost sistema se razlikuje po broju, vrsti međusobnih veza elementarnih delova sistema.[316] Sistem sistema američke vojske je najsloženiji vojni sistem na svetu. Cebrovski smatra da se sa kompleksnim sistemima može operativno postupati isključivo primenom informaciono-komunikacionih tehnologija [317], kao i odgovarajućom organizacionom strukturom vojske, zasnovanom na principima nelinearnost, kompleksnosti i haosa.

Sistem se može smatrati i skupom pravila koji određuju ponašanje strukture. Oni predstavljaju logičku osnovu te strukture. U tom pogledu se sistemima mogu smatrati i

---

[310] „War in the Fifth Domain," *The Economist*, July 1, 2010, http://www.economist.com/node/16478792 (preuzeto 12. oktobra 2015).

[311] Robert J. Bunker and Charles „Sid" Heal, eds. *Fifth Dimensional Operations: Space-Time-Cyber Dimensionality in Conflict and War—A Terrorism Research Center Book* (Bloomington, IN: iUniverse LLC, 2014).

[312] Johnson, "Two's Company."

[313] *Merriam-Webster*, s.v. "system," http://www.merriam-webster.com/dictionary/system (preuzeto 24. februara 2016).

[314] Cristoforo Sergio Bertuglia and Franco Vaio, *Nonlinearity, Chaos & Complexity, The Dynamics of Natural and Social Systems*, (New York, NY: Oxford University Press, 2005) 3.

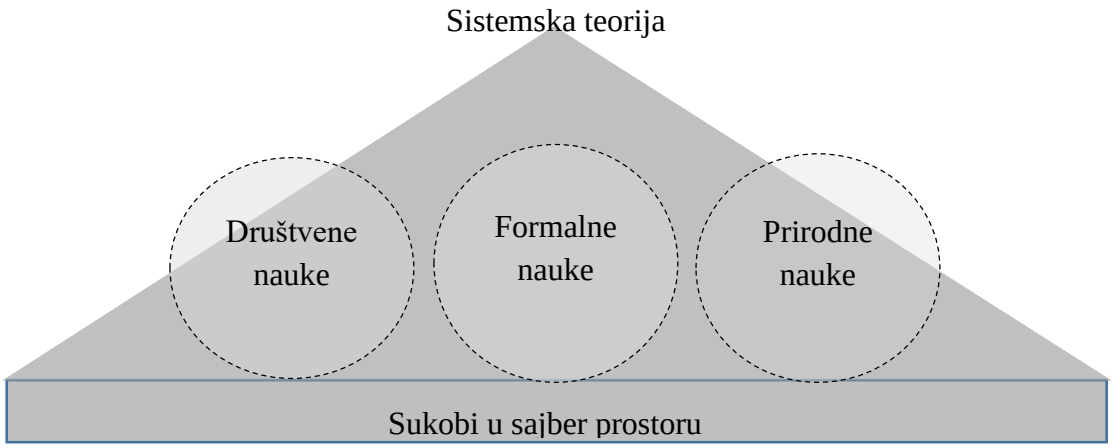
[315] Jeremy J. Ramsden, „An Introduction to Complexity" in *Complexity and Secuirty*, eds. Jeremy J. Ramsden and Paata .J. Kervalishvili, 58 (Amsterdam, Netherlands: IOS Press, 2008), Proceedings of the NATO Advanced Research Workshop on Complexity and Security, Tbilisi, Georgia, 2007.

[316] Ibid, 59.

[317] James R. Blaker, *Transforming Military Force, The Legacy of Arthur Cebrowski and Network Centric Warfare*, (Westport, CT: Preager Security International, 2007).

informacione tehnologije koje izgrađuju sajber prostor, kao i Međunarodno pravo oružanih sukoba, koje reguliše sukobe u sajber prostoru. Propisi i norme *ius ad bellum* i *ius in bello* Međunarodnog prava oružanih sukoba su skupovi pravila koji uređuju odnose između strana u sukobu međusobno i sa neutralnim stranama. U tom pogledu, može se zaključiti da informacioni (tehnički) sistemi, organizacioni sistemi koje ti tehnički sistemi omogućavaju (struktura sistema odbrane i bezbednosti), kao i sam društveno-pravni sistem međunarodnog prava počivaju na specifičnim logičkim pravilima.

Navedeni model se može posmatrati i na novi način. Na primer, u smislu aksioma koji je u okviru transdisciplinarnog pristupa jedinstvene teorije o nivoima realnosti postavio rumunski teorijski fizičar Nikolesku: "Struktura ukupnosti nivoa realnosti nastaje u našem znanju o prirodi, društvu i nama samima kao kompleksna struktura: svaki nivo je ono što jeste zbog toga što svi nivoi postoje istovremeno."[318]



Slika 7. Simbolični prikaz konceptualnog odnosa formalnih i prirodnih nauka u okviru teorije sistema

U osnovi informacionih i teorijskih računarskih nauka primenjuju se formalne nauke, discipline i tehnike, poput matematike, logike, teorijskih računarskih nauka, teorije

[318] Basarab Nicolescu, „Methodology of Transdisciplinarity – Levels of Reality, Logic of the Included Middle and Complexity," *Transdisciplinary Journal of Engineering and Science*, 1, no. 1 (December 2010):19-38, http://www.basarab-nicolescu.fr/Docs_Notice/TJESNo_1_12_2010.pdf (preuzeto 15. februara 2016).

informacija, teorije igara, pa čak i delova lingvistike (na primer, kroz načine izgradnje sintakse računarskih ili programskih jezika, koji služe za stvaranje softvera).

U opštem smislu, "sistem je skup elemenata ili komponenti, organizovanih u cilju izvršavanja zajedničke svrhe".[319] Primena teorije sistema u području odbrane i bezbednosti nema isključivo konceptualni značaj, već i praktičan, pre svega u metodološkom pogledu. Takav pristup pruža mogućnost standardizovanog razmatranja i identifikacije elemenata različitog porekla i sadržaja u svojstvu delova opšte strukture sistema, kao i procesa koji postoje između tih elemenata.

Najviši opšti "sistem sistema" ukupne primene informacionih tehnologija je sajber prostor. Sistemi informacionih tehnologija nisu statični. Njihova ključna sposobnost, umrežavanje, je ugrađena u njih na nivou svojstva elementa i ostvaruje se na raznim nivoima, uključujući i nivo podataka. Savremeni sistemi informacionih tehnologija nisu vremenom evoluirali iz "nemrežnih" u "mrežne" sisteme; oni su to oduvek bili, zahvaljujući sposobnosti informacija u digitalnom zapisu da budu beskonačno puta umnožene i međusobno upoređene i obrađivane po značenju. Umrežavanje računarskih informacionih sistema čovek je prvo manuelno izvršavao, primenom specifičnih medija za zapis informacija u stanju čuvanja ili obrade (na principima mehaničkog, elektromehaničkog ili magnetnog zapisa). Umrežavanje je zatim automatizovano primenom elektronske i tranzistorske tehnologije, da bi se došlo do savremenog automatskog povezivanja sistema kroz hardver[320], softver i procese.

Bez obzira na sadržaj, poreklo i funkciju sistema, od primarne važnosti su elementi, način njihove organizacije (struktura) i odnosi (procesi). U tom pogledu, sve je sistem: vlastita mrežna struktura,[321] neprijatelj,[322] i kompleksno okruženje u kome se manifestuju

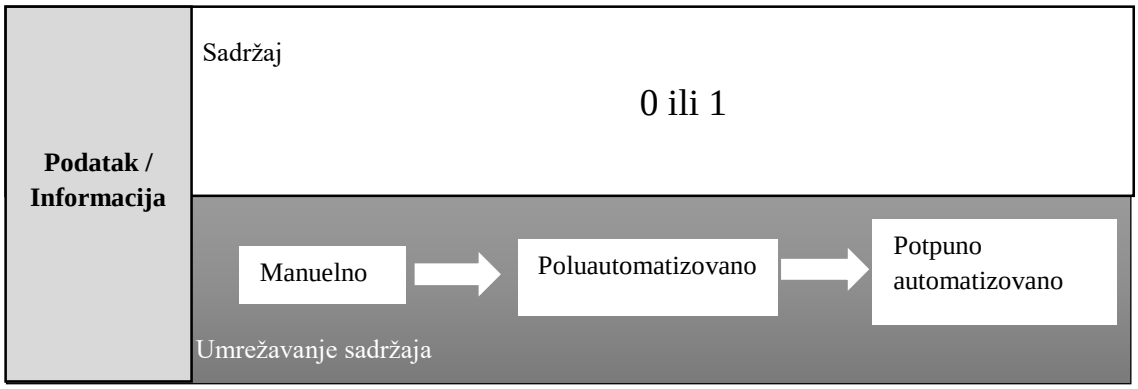
[319] *WhatIs.com, Coputer Glossary*, Computer Terms, s.v. "system," http://whatis.techtarget.com/search/query?q=system (preuzeto 22. novembra 2015).

[320] Ne samo savremeni računarski informacioni uređaji, poput računara i perifernih uređaja, softverskih aplikacija i operativnih sistema, već (skoro) svi savremeni tehnički sistemi imaju sposobnost automatskog umrežavanja, koje je podrazumevano uključeno: kućni uređaji, poput televizora, frižidera; prevozna sredstva, poput automobila, aviona, brodova; industrijske mašine i oprema, sistemi infrastrukture i drugi. U takvom okruženju koncepti veštačkog sveta oko nas postaju podrazumevano mrežni, poput Interneta stvari (*Internet of Things – IoT*).

[321] Cebrowski and Garstka, "Network-centric Warfare."

[322] John A. Warden III, „The Enemy as a System", *Airpower Journal* (Spring 1995), http://www.airpower.maxwell.af.mil/airchronicles/apj/apj95/spr95_files/warden.htm (preuzeto 16. avgusta 2015).

defanzivno-ofanzivna dejstva. Tehnološka manifestacija takvog okruženja je sajber prostor. Uvođenje teorije sistema u oblast istraživanja sukoba u cilju unapređenja efikasnosti nacionalne odbrane predstavlja suštinski uticaj informacionih tehnologija na vojne organizacije.



Slika 8. Razvoj sposobnosti umrežavanja na nivou digitalnih podataka

Na primer, u analizi modela "pet prstenova" Vorden poredi koncept sistema sukoba sa ljudskim telom (biološki sistem), državom (makro-organizacioni društveni sistem), kriminalnom organizacijom (mikro društveno-organizacioni sistem) i električnom mrežom (tehnički sistem), nalazeći suštinske sličnosti u načinu organizacije, funkcionisanja i strukturne povezanosti njihovih elemenata.[323]

Kasniju ideju Cebrovskog o mrežnocentričnom ratovanju prethodno je u tehnološkom i operativnom smislu formalno uobličio američki admiral Ovens sa konceptom "sistem sistema"[324]. Po Ovensu[325], vojna organizacija u dejstvu (vođenju sukoba) predstavlja "sistem sistema", odnosno usklađeno združeno funkcionisanje svih postojećih, organizaciono specifičnih vojnih komponenti, za čiju efikasnost kao jedinstvene celine je potrebna posebna i prilagođena doktrina planiranja, organizovanja i izvođenja vojnih operacija.[326] Pri tome su ključni resurs koji omogućava harmonično funkcionisanje sistema informacije o okruženju, sopstvenim i protivničkim procesima i aktivnostima,

[323] John Warden, „The Enemy as a System".

[324] William A. Owens, „Emerging US system-of-systems," *Strategic Forum*, 63 (February 1996).

[325] Ibid.

[326] Ibid.

koje kontinuirano i u realnom vremenu stižu do učesnika aktivnosti i objedinjene i shvaćene predstavljaju znanje o kompleksnom borbenom prostoru.

Uvođenje koncepta "borbenog prostora" je neophodno zbog povećanja broja vrsta naoružanja, načina njihovog dejstva, dometa i destruktivnosti, kao i mobilnosti oružanih snaga. Sukobe više nije dovoljno posmatrati na linearan način u seriji uzročno-posledičnih događaja u tradicionalnom pogledu kao aktivnosti u prostorno-vremenskoj ravni na mestu sukoba, na kome se izvode borbene operacije strana u sukobu. To je predstava tradicionalnog bojnog polja, ograničenog na manjoj površini, odnosno bojišta (eng. *batllefield*), kao većeg i amorfnijeg područja sukoba. Piloti savremenih aviona se u toku borbe u vazduhu se i ne vide bez instrumenata, a dejstvuju po protivniku iz velike daljine i pri velikoj brzini. Oni lete i komuniciraju uz pomoć satelita, čvorišta veze na brodovima, zemaljskih stanica i drugih aviona, specijalno namenjenim za tu svrhu. Trupe na kopnu imaju direktnu i neprekidnu komunikacionu vezu sa komandnim centrom koji može biti i na drugom kontinentu. Dejstva na protivnika se ostvaruju sinhronizovano sa kopna, iz vazduha, svemira, i sa mora, u dodiru sa protivnikom ili sa udaljenosti. Te brze i automatizovane aktivnosti snaga u svim fizičkim područjima i sajber prostoru zahtevaju sigurne i pouzdane tokove informacija velikog kapaciteta u oba smera. Vojna dejstva se stoga odigravaju u uzročno-posledično-prostorno-vremenski isprepletanom multiverzumu (multidimenzionalom okruženju), uvek u okviru širokog borbenog prostora (eng. *batllespace*) sa velikim brojem uključenih, aktivnih ili neutralnih aktera. Osnovni faktor koji omogućava tu izrazitu povezanost ljudi, sistema i procesa na borbenom prostoru jesu informacije i sistemi za prikupljanje, obradu, i razmenu informacija i servisi, koji moraju biti stalno dostupni, pouzdani i sigurni. Značaj informacija za ovakav sistem koji neprekidno funkcioniše je očigledno veći nego što je ikada bio. Bez pravovremenih, potpunih, sigurnih i brojnih informacija različiti vojni elementi ne mogu biti uspešno povezani i ne može se ostvariti sinergijski efekat delovanja celine kao "sistema sistema".

Ovakav pristup utiče i na razumevanje odnosa taktičkih, operativnih i strategijskih vojnih aktivnosti u drugačijem svetlu. Umreženi sistemi i aktivnosti kojima se vode vojne operacije postoje u svim područjima fizičkog okruženja, ali postoje istovremeno i u logičkom i informacionom okruženju. Teorijski modeli ovakvog načina vođenja sukoba

u savremenoj međunarodnoj praksi se različito nazivaju, poput specijalnog ratovanja (*Special Warfare*)[327], nelinearnog ratovanja (*Non-linear Warfare*)[328], mrežnocentričnog ratovanja (*Network-Centric Warfare*)[329], asimetričnog ratovanja (*Assymetric Warfare*), ratovanja četvrte generacije (*Fourth Generation Warfare* – 4GW)[330], neograničenog ratovanja (*Unrestricted Warfare*)[331], hibridnog ratovanja (*Hybrid Warfare*)[332] i drugih. Svi navedeni koncepti ratovanja se razlikuju po teorijskom modelu i nastali su sukcesivno u različitim vremenskim epohama. Međutim, svi oni imaju zajedničku karakteristiku, a to je da ne određuju formu budućih sukoba, već da su njihovi modeli kreirani opisivanjem postojećih sukoba. Pobeda u sukobu sa drugom državom je krajnji cilj svake države. Pošto je sam opstanak države ulog u sukobu, države nemaju razloga da se ograničavaju na specifične oblike vođenja sukoba. U nekim slučajevima, poput građanskih ratova, sve se odvija haotično bez reda i pravila. To pokazuje da se kompleksnost sukoba povećava u skladu sa vremenom, sa razvojem novih tehnologija za vođenje sukoba, povećavanjem broja aktera sukoba i strategije delovanja na protivnika.

4.2. Združeno informaciono okruženje kao sistem

Najbolji primer koncepta „sistem sistema“ je sama armija SAD. Rasprostranjena globalno, njena celovitost i operativna moć počivaju na isprepletanoj mreži kopnenih, podvodnih, satelitskih, bežičnih, fiksnih i mobilnih komunikacija širom sveta. Ministarstvo odbrane SAD je razvilo Globalnu informacionu mrežu (engl. *Global Information Grid* - GIG)[333], kao i Informacionu arhitekturu organizacije (eng. *The*

[327] John R. Schindler, “The Coming Age of Special War,” *The XX Committee* (blog), September 20, 2013, http://20committee.com/2013/09/20/the-coming-age-of-special-war/ (preuzeto 15. septembra 2015).

[328] Валерий Герасимов, „Ценность Науки в Педвидении,“ *Военно-Промишлений Куриер*, 8 (476), 27. Februar 2013, http://www.vpk-news.ru/articles/14632 (preuzeto 23. februara 2016).

[329] Cebrowski and Garstka, "Network-centric Warfare.“

[330] William S. Lind, Keith Nightengale, John F. Schmitt, Joseph W. Sutton, Garry I. Wilson, "The Changing Face of War: Into the Fourth Generation," *Marine Corps Gazzette*, 73, no. 10 (1989): 22-26, https://www.mca-marines.org/files/The%20Changing%20Face%20of%20War%20-%20Into%20the%20Fourth%20Generation.pdf (preuzeto 18. oktobra 2015).

[331] Qiao Liang and Wang Xiangsui, *Unrestricted Warfare* (Beijing: PLA Literature and Arts Publishing House, 1999).

[332] Герасимов, „Ценность науки в предвидении.“

[333] *Global Information Grid* - GIG obuhvata sve vojne komunikacije Ministarstva odbrane SAD, računarske sisteme i informacione mreže, podatke, softver i servise, koji su u vlasništvu MO SAD ili su iznajmljene od civilnih kompanija. GIG je najveća vojna informaciona mreža na svetu.

Department of Defense Information Enterprise Architecture). Ovi sistemi su toliko veliki, da se o njihovom funkcionisanju i informacionoj bezbednosti brinu čitave vojne agencije sa desetinama hiljada pripadnika.

Za primenu sistemske teorije u okviru Ministarstva odbrane SAD ima više razloga. Većina informaciono-komunikacionih tehnologija nastala je baš za potrebe odbrane, uglavnom u projektima ministarstava odbrane SAD i Velike Britanije.[334, 335] Sama informaciona struktura Ministarstva odbrane SAD predstavlja jedan veliki, globalni sistem koji predstavlja jedinstvenu i sinhronizovanu celinu. Okosnica tog sistema je takozvano *Združeno informaciono okruženje* (eng. *Joint Information Environment*)[336] , koje se razvilo iz prethodnog koncepta *Globalne informacione mreže* (eng. *Global Information Grid* – GIG).

Ovo okruženje predstavlja jedinstveni, bezbedni, pouzdani, dinamični sistem koji omogućava optimizaciju funkcija, sposobnosti, resursa i strukture svih delova i celine istovremeno; minimizaciju sistemskih resursa; trenutnu i bezbednu dostupnost licima i organizacijama kojima je namenjen, bilo gde i bilo kada; razmenu informacija između svih delova celine i okruženja, i zasnovano je na zaštiti podataka kao ključne vrednosti sistema.[337] Njegovo funkcionisanje ima za cilj da svim korisnicima obezbedi pristup zajedničkoj informacionoj mreži i resursima iz bilo koje tačke u svetu; razmenu informacija i servisa između brojnih službi, agencija i predstavnika privatne industrije koja radi za Ministarstvo odbrane i da minimizuje resurse i unifikuje arhitekturu objedinjenim sistemom.

Globalni informacioni sistem Ministarstva odbrane SAD se sastoji od najmanje 200.000 mrežnih uređaja, 17.000 lokalnih mreža, 55 satelitskih mrežnih kapija (eng. *gateway*) i

---

[334] Alex Roland and Philip Shiman, *Strategic Computing: DARPA and the Quest for Machine Intelligence, 1983-1993* (Cambridge, MA: The MIT Press, 2002).

[335] Nicholas Metropolis, Jack Howlett and Gian-Carlo Rota, eds., *A History of Computing in the Twentieth Century: A Collection of Essays* (New York, NY: Academic Press, Inc, 1980).

[336] Združeno informaciono okruženje (JIE) je jedinstvena, pouzdana i bezbedna organizaciona celina koja predstavlja zajedničko globalno informaciono okruženje Ministarstva odbrane SAD, za čije stručno funkcionisanje je zadužena Agencija za odbrambene informacione sisteme (eng. *Defense Information Systems Agency*).

[337] Defense Information Systems Agency (DISA), „Enabling The Joint Information Environment (JIE): Shaping the Enterprise for the Conflicts of Tomorrow," May 5, 2014, http://www.disa.mil/~/media/Files/DISA/About/JIE101_000.pdf (preuzeto 2. februara 2016).

4.5 miliona jedinstvenih identiteta na mreži.[338] U sistemu Ministarstva odbrane SAD postoji veći broj specijalizovanih informacionih mreža, različite klasifikacije tajnosti,[339] koje obezbeđuju veliki broj korisnika iz raznih vojnih, obaveštajnih i drugih vladinih agencija. Ministarstvo odbrane SAD se u kreiranju i organizovanju ovog sistema nije vodilo političkim, već stručnim odlukama.[340] Pored operacionalizacije i optimizacije sistemskog pristupa jedinstvenoj vojnoj strukturi organizacije na globalnom nivou, zasnivanoj na primeni informaciono-komunikacionih tehnologija, uspostavljanje *Združenog informacionog okruženja* predstavlja i omogućavanje tehnološkog pristupa vlastitoj odbrani. Glavni oficir zadužen za informacione tehnologije u okviru Generalštaba Vojske SAD je na konferenciji u Vašingtonu 2015. izjavio: „Upravo sada mi imamo suviše različitih mreža. Mi imamo suviše ranjivosti koje naši neprijatelji mogu iskoristiti“[341]. Zbog toga je uspostavljanje i razvoj Združenog informacionog okruženja operativni imperativ Ministarstva odbrane SAD.

Navedeno okruženje predstavlja vezu između svih informacionih resursa sistema i funkcija koje se odvijaju u virtuelnom borbenom području i fizičke infrastrukture, odnosno kapaciteta za vođenje bitke u fizičkom području. U njegovom slučaju, dakle, nije reč o "vođenju dejstava u sajber prostoru“, već o primeni informacionih tehnologija u sajber prostoru i kroz njega sa ciljem da se podrže i izvode sve vrste vojnih operacija. U tom smislu treba posmatrati i koncept sajber ratovanja. U njemu, svako vojno dejstvo u sajber prostoru ima implikacije u fizičkom i/ili kognitivnom okruženju. Sajber prostor

[338] Defense Infromation Systems Agency (DISA), Evolving Operations, January 12, 2015, http://disa.mil/News/Stories/2014/Evolving-Ops (preuzeto 3. septembra 2015).

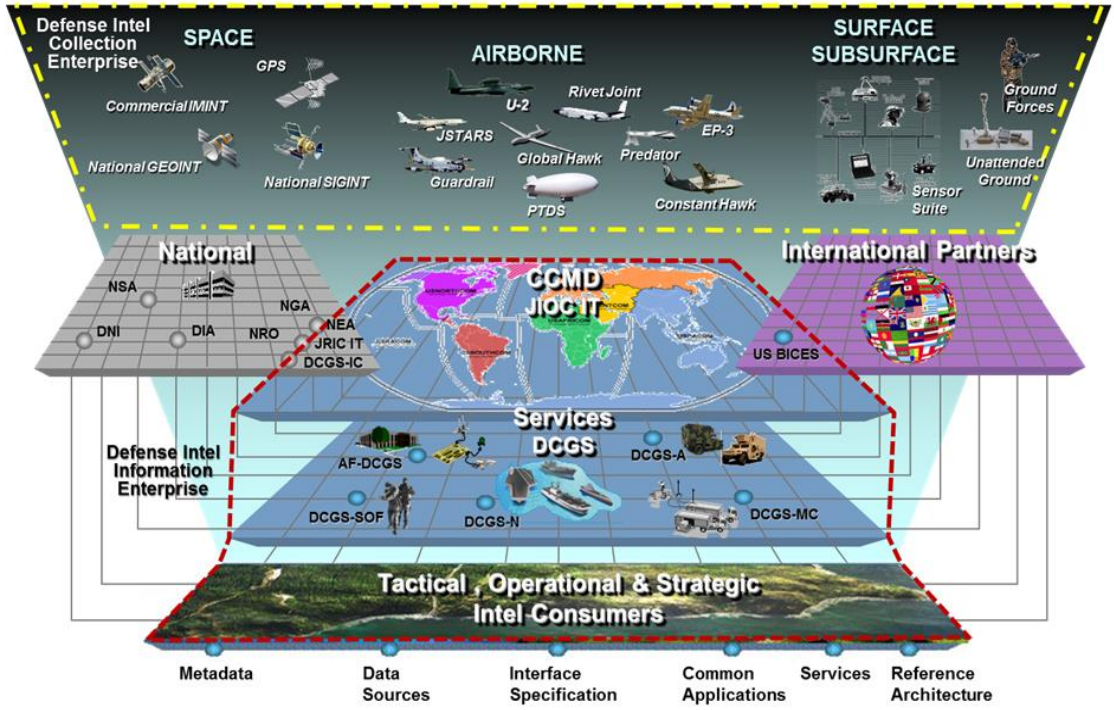
[339] „US Military and Intelligence Computer Networks,“ *Electrospaces.net*, March 11, 2015, http://electrospaces.blogspot.rs/2015/03/us-military-and-intelligence-computer.html (preuzeto 22. decembra 2015).

[340] Zanimljivo je da se na odnosno naslovnoj strani konceptualnog dokumenta koji opisuje Združeno informaciono okruženje, izdatog od strane načelnika Združenog generalštaba Vojske SAD, generala Martina Dempseja, nalaze dve izreke - drevnog kineskog generala Sun Cua: „Boriti se i pokoriti protivnika u svim bitkama nije vrhovna veština, vrhovna veština se sastoji u slamanju neprijateljevog otpora bez borbe“ i pokojnog direktora kompanije *Apple*, menadžera Stiva Džobsa: „Neki ljudi misle da dizajn znači kako nešto izgleda. Međutim, naravno, ako kopate dublje, radi se u stvari o tome kako nešto radi“.

US DoD Joint Chiefs of Staff, *Joint Information Environment*, White Paper, 22 January 2013, http://www.jcs.mil/Portals/36/Documents/Publications/environmentalwhitepaper.pdf

[341] Robert S. Ferrell, US DoD Joint Staff, J-6, Panel Discussion, July 9, 2015, in Lisa Ferdinando, „Joint Information Environment is 'Operational Imperative',“ *US Army*, July 9, 2015, http://www.army.mil/article/152064/Joint_information_environment_is__operational_imperative_/ (preuzeto 22. jaunuara 2016).

nije nešto odvojeno od fizičkog okruženja, već faktor na kome je zasnovana upotreba lica, sistema i snaga u fizičkom okruženju. On povezuje fizičko dejstvo svih elemenata sistema na taktičkom, operativnom i strategijskom nivou. Sajber ratovanje je ostvarivanje vojnih dejstava na protivnikovu sposobnost da izvodi vojne operacije bilo gde, u fizičkom ili sajber okruženju.



Slika 9. Vojnoobaveštajna informaciona organizacija (eng. *Defense Intelligence Information Enterprise* – DI2E), kao deo Združenog informacionog okruženja, Nazanin Azizian, „Defense Intelligence Information Enterprise (DI2E).[342]

U okviru *Združenog informacionog okruženja* se ostvaruju mnogobrojne funkcije, od obaveštajnog obezbeđenja (Slika 9), preko logističke podrške, do borbenih operacija. To znači da ono u bukvalnom smislu predstavlja sistem sistema, organizovanih na više nivoa, koji su dinamični i stalno se menjaju i razvijaju. Pri tome, ovo informaciono okruženje nije samo organizaciono-funkcionalni koncept, već je sačinjeno i od podataka, softvera i

[342] Nazanin Azizian, „Defense Intelligence Information Enterprise (DI2E),“ Office of the Under Secretary of Defense for Intelligence, October 29, 2014, PowerPoint Presentation, 5, http://www.dtic.mil/ndia/2014system/16835WedTrack6Azizian.pdf (preuzeto 22. januara 2016).

hardvera i ljudi koji unutar njega imaju specifične funkcije (rukovođenje, planiranje, kontrola, izvršavanje, razvoj, održavanje, upotreba i druge).[343]

4.3. Pravo i kompleksni "sistem sistema"

Sukobi između kompleksnih "sistema sistema" dovode do složenih situacija u međunarodnim odnosima, koje se u pogledu prava bitno razlikuju od situacija koje nastaju tokom tradicionalnih oružanih sukoba. Postavlja se pitanje, da li tradicionalno međunarodno pravo može da reguliše te kompleksne situacije, i ako može, kako?

Ključni faktor homogenizacije i dinamičke organizacije „sistema sistema" su informaciono-komunikacione tehnologije. Njihova primena ima strategijski značaj, pošto u funkcionalnom pogledu, omogućavaju borbeno obezbeđenje i podršku vojnim operacijama u fizičkom okruženju, ali istovremeno i razvoj sposobnosti za operativno delovanje u sajber prostoru. Informaciono-komunikacione tehnologije omogućavaju uspostavljanje i same strukture sistema odbrane i bezbednosti, omogućavajući tri ključne funkcije: logističku podršku svim sistemima, sve vrste komunikacija i nadzor svih lica, servisa i entiteta u sajber prostoru. Taj proces je nužan, jer predstavlja suštinsku promenu pristupa procesu praćenja i prilagođavanja pretnjama. Umesto procesa detekcije, identifikacije i praćenja ciljeva novi proces je praćenje svih i uočavanje obrazaca u skupu podataka o svima (Slika 10).

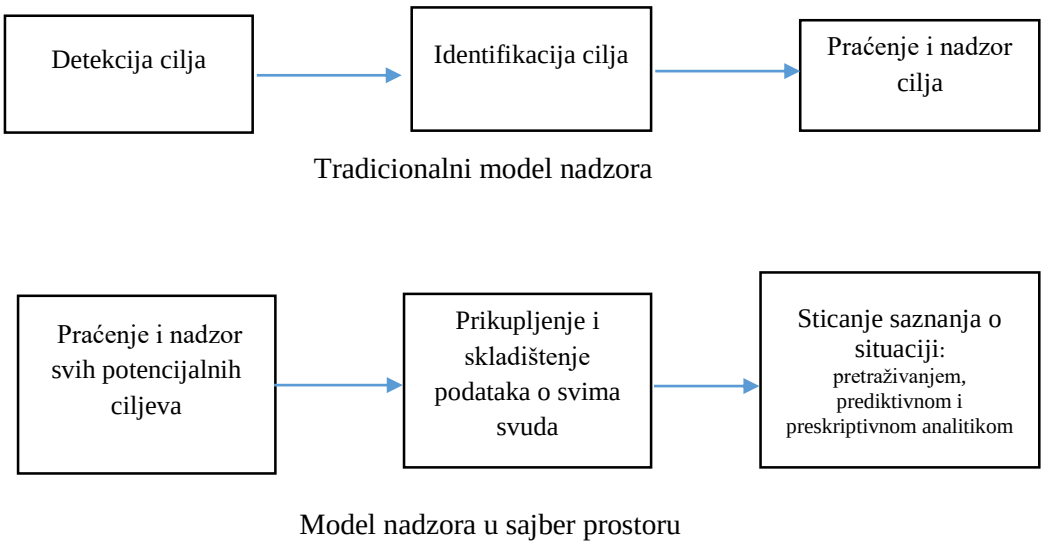
Ovakav pristup se simbolično označava strategijom „Prikupiti sve" [344] informacije o svakome i zatim ih pretraživati primenom logičkih metoda. Umesto težišnog specijalizovanog obaveštajnog rada na velikom broju specifičnih zadataka, ključna obaveštajna aktivnost u dobu informacija je postalo masovno prikupljanje podataka i informacija, njihovo masovno skladištenje i obrada pretraživanjem po zadatim logičkim

[343] Cheryl Pellerin, „DoD Advances Elements of Joint Information Environment," *U.S. Department of Defense Website*, March 24, 2015, http://www.defense.gov/News-Article-View/Article/604340 (preuzeto 22. januara 2016).

[344] Po Vašington Postu, viši rukovodilac u okviru obaveštajne zajednice SAD je o planu direktora agencije NSA i ujedno komandantu Sajber komande, generala Aleksandera izjavio sledeće: „Umesto da traži pojedinačnu iglu u plastu sena, njegov pristup je bio 'prikupimo ceo plast'…prikupi sve, označi, sačuvaj…i šta god želiš sa tim da uradiš, možeš da to potražiš"

Ellen Nakashima, and Joby Warrick, „For NSA Chief, Terrorist Threat Drives Passion to 'Collect it All'", July 14, 2013, *The Washington Post*, https://www.washingtonpost.com/world/national-security/for-nsa-chief-terrorist-threat-drives-passion-to-collect-it-all/2013/07/14/3d26ef80-ea49-11e2-a301-ea5a8116d211_story.html (preuzeto 30. novembra 2015).

algoritmima, kao i primena prediktivne i preskriptivne analitike. Navedene metode omogućavaju sticanje uvida u znanja koji nisu direktno vidljiva u ogromnoj masi nestrukturiranih podataka.



Slika 10. Dva modela sticanja saznanja o bezbednosnoj operativnoj situaciji zasnovana na upravljanju podacima

Navedeni pristup pruža nove mogućnosti, ali i zahteva nove sposobnosti. Tradicionalan pristup bezbednosti podrazumeva da se otkrije cilj-objekat nadzora (lice, sistem, proces), zatim da se identifikuju njegovi atributi, i konačno da se taj objekat prati i prikupljaju se podaci o njemu. Ovakav postupak je zahtevan u pogledu resursa, pošto za jedan objekat praćenja potrebno angažovati jednog ili više subjekata koji preduzimaju praćenje. Uvid koji se ostvaruje o objektu praćenja se odnosi samo na njega i saznanja o više pojedinačnih objekata praćenja se moraju uporediti radi sagledavanja ukupne slike. Takav proces, primenjen na globalno okruženje, doveo je do situacije u kojoj je glomazni obaveštajni sistem SAD imao pojedinačne podatke o napadačima na SAD u terorističkom napadu 11. septembra 2011, ali nije imao vizuelizovanu predstavu na osnovu tih informacija da će se napadi desiti, odnosno nije bio u stanju da te podatke operativno

poveže kako bi se stekao jedinstveni uvid i blagovremeno se reagovalo u cilju sprečavanja napada.[345, 346]

Novi sistem nadzora u cilju borbe protiv terorizma, razvijen nakon tog perioda predstavlja potpunu izmenu koncepta obaveštajnog rada. On podrazumeva izgradnju sistema sposobnog da istovremeno prati sva lica i entitete u globalnim razmerama. Rezultat njegovog funkcionisanja je prikupljanje i pohranjivanje ogromne količine podataka i metapodataka[347]. To zahteva posedovanje centara za čuvanje podataka ogromnih kapaciteta. Na primer, američka agencija NSA je 2014. godine izgradila ogroman centar za skladištenje digitalnih podatka u Blafdejlu u američkoj državi Juta, površine 140.000 m^2, vredan 1,5 milijardi dolara.[348] Konačno, vrši se obrada i analiza tih podataka u moru podataka (eng. *Big Data*). Ovakav postupak je tehnički zahtevniji, ali pruža neuporedivo veće sposobnosti praćenja i sticanja uvida od tradicionalnog. Takođe, omogućava prediktivnu i preskriptivnu analitiku, odnosno sposobnost predviđanja verovatnog sleda događaja ili sleda akcija praćenih entiteta. Konačno, stvara mnoge nove dileme u pogledu primene tradicionalnog prava, a posebno ljudskih prava, podjednako na nacionalnom, kao i na međunarodnom nivou. Zbog ovog modela dolazi do mešanja nadležnosti obaveštajno-bezbednosnih agencija, kao i do zadiranja sistema zaduženih za odbranu spolja u područje unutrašnjeg prava i bezbednosti koje je regulisano nacionalnim ustavima. Sve to na tehničkom nivou omogućava postojanje i široka primena informacionih tehnologija i sajber prostora.

Međutim, zbog očiglednih ograničenja, mali je broj država koje tehnološki mogu razviti ovakav sistem na širokom nivou. U pogledu prava, postavlja se pitanje, kako linearno

---

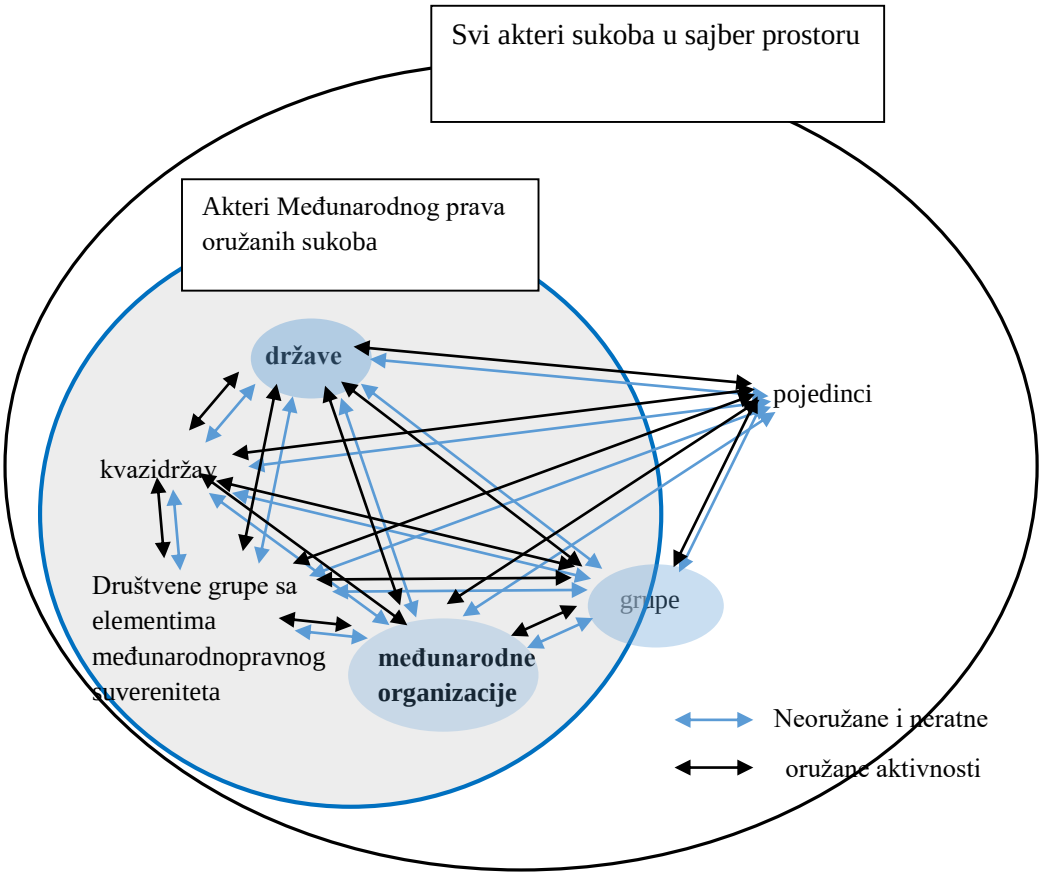
[345] National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission report, Final Report of the National Commission on Terrorist Attacks Upon the United States, Executive Summary*, http://www.9-11commission.gov/report/911Report_Exec.htm (preuzeto 22. decembar 2015).

[346] Amy B. Zegart, "September 11 and the Adaptation Failure of US Intelligence Agencies," *International Security* 29, no. 4 (2005): 78-111.

[347] Metapodaci su (tehnički) podaci o podacima, koji ne sadrže informacije o sadržaju ili delovima sadržaja primarne informacije, već podatke o mestu i vremenu kada je neki skup podataka napravljen, sredstvu sa kojim je to urađeno, ko je tu informaciju kome poslao i tako dalje. Postojanje metapodataka omogućava primena digitalnih tehnologija. Svaki skup podataka je smešten u neku digitalnu datoteku, koja pored podataka o sadržaju ima i metapodatke o informacijama o toj datoteci i poreklu podataka.

[348] Joao Lima, „Top 10 biggest data centres from around the world," Computer Business Review, April 2, 2015, http://www.cbronline.com/news/data-centre/infrastructure/top-10-biggest-data-centres-from-around-the-world-4545356 (preuzeto 30. novembra 2015).

orjentisani sistem tradicionalnog međunarodnog prava može da reguliše sukobe koji se vode neprekidno, primenom kompleksnih vojnih "sistema sistema"?



Slika 11. Kompleksni odnosi međunarodnih učesnika u sajber prostoru

Efekti aktivnosti sukoba manifestuju se u svim područjima, bez obzira da li je stanje mira ili rata, a ne isključivo u vojnom području aktivnosti, tokom oružanih sukoba. I u ratu i u miru izvodi se nasilje nad drugom stranom, ali to nasilje se ne manifestuje samo nad objektima i telima ljudi (u fizičkom okruženju), već i nad njihovim dušama, odnosno svešću (u informaciono-kognitivnom okruženju).[349] Konačno, razvoj logičkog okruženja i sposobnosti tehničkih sistema da funkcionišu kreativno i smisleno poput čoveka kroz sisteme veštačke inteligencije i robotike, omogućavaju da se nasilje sprovodi i u logičkom okruženju.

[349] Đuro Šušnjić, *Ribari ljudskih duša* (Beograd: Čigoja, 2008).

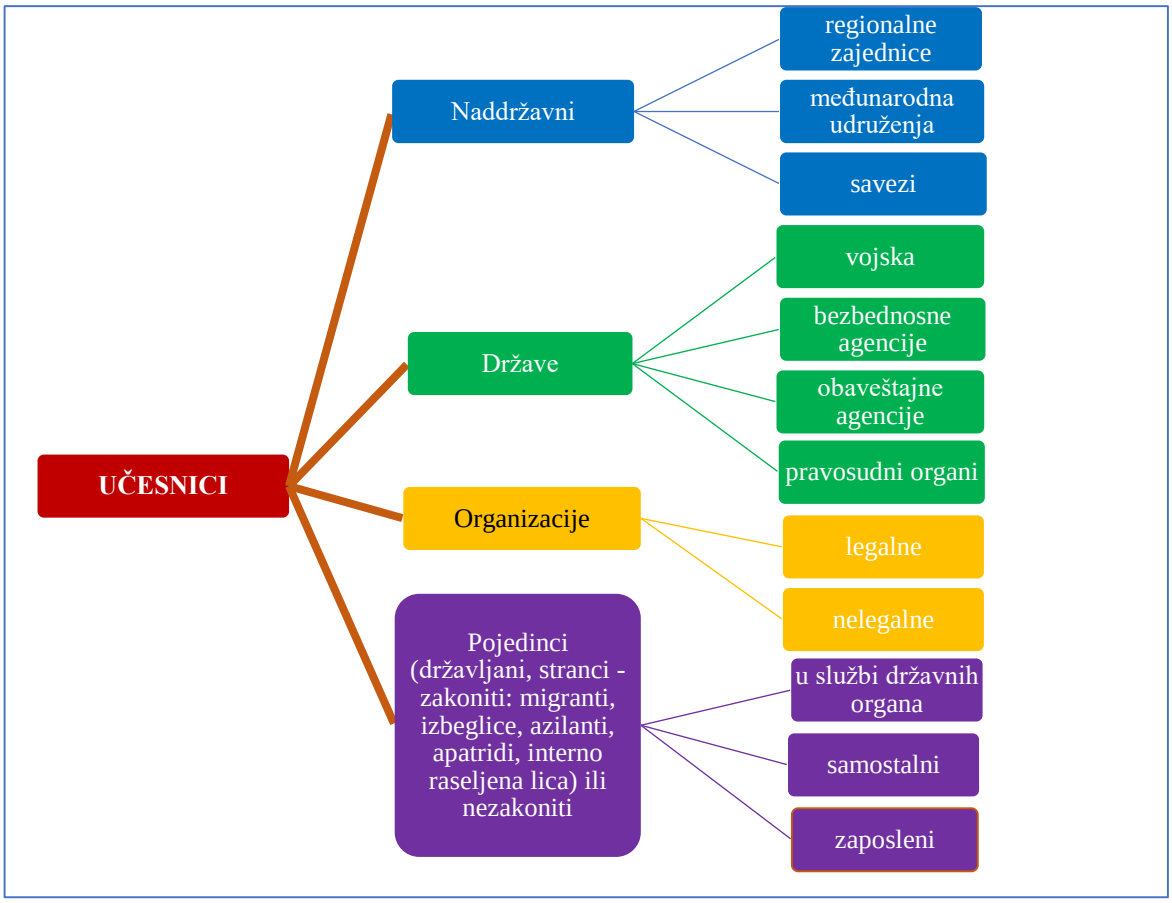
Međutim, sa razvojem dinamike vođenja sukoba, smanjuje se moć međunarodnog javnog prava da efikasno reguliše sukobe. U slučaju sajber prostora postoji više problema u smislu nadležnosti Međunarodnog prava oružanih sukoba nego što postoji uređenih mogućnosti za njihovu regulaciju. Međunarodno pravo oružanih sukoba ima nadležnost da uređuje pravne odnose i reguliše posledice aktivnosti aktera u globalnom sajber prostoru, ali u slučaju ovakvog načina ratovanja nema praktičnu mogućnost da to ostvari u svim situacijama, čime se ugrožava njegova osnovna svrha.

Odsustvo zajedničkih, univerzalnih propisa na međunarodnom nivou, konkurencija nacionalnih propisa, interesa i elemenata nacionalne moći, u kombinaciji sa odsustvom mogućnosti detekcije učinjenih dela i aktivnosti, atribucije odgovornih entiteta, dokazivanja njihove odgovornosti i konačno, odsustvo mogućnosti da se u praksi ostvari vladavina prava u međunarodnim odnosima dovodi do situacije koja je vrlo složena i teži regulatornom haosu. Tu situaciju dodatno komplikuje okolnost da je sajber prostor značajno širi od Interneta na kome postoji kakva-takva mogućnost identifikacije lica i entiteta. U globalnom sajber prostoru države nisu jedini akteri. Pri tome, svi mogući akteri izvršavaju određena dela koja ostavljaju određene posledice na entitete u sajber prostoru ili na sisteme i procese koji su u njihovoj nadležnosti ili su im od interesa.

5. UČESNICI SUKOBA U SAJBER PROSTORU

Tehnološka priroda sajber ratovanja se zasniva na raspolaganju i upravljanju znanjem iz oblasti informacione bezbednosti i na praktičnoj sposobnosti za izvođenje specijalnih operacija u specifičnom okruženju sajber prostora. Imajući to u vidu, može se zaključiti da se stvarna sposobnost vođenja sajber sukoba preduzimanjem sajber napada može ostvariti na svim društvenim organizacionim nivoima:

- nacionalnom/državnom,
- organizacionom, i
- individualnom.



Slika 12. Ključni učesnici sukoba u sajber prostoru u svojstvu strana u sukobu, neučesnika sukoba i neutralnih strana

Nacionalni nivo je nivo nacionalnih država, uključujući pojedinačne funkcionalne i strukturne delove država, kao i više nivoe organizacije zasnovane na državama. **Nadnacionalni nivo** obuhvata svaki oblik udruživanja država u njihovim međunarodnim odnosima. **Organizacioni** nivo obuhvata svaki oblik institucionalnog i strukturalno hijerarhijskog uređenog neinstitucionalnog organizovanja. **Individualni nivo** čine pojedinci, koji mogu biti samostalni akteri ili akteri koji postupaju u skladu sa planom i u sklopu organizacije raznih društvenih organizacija.

5.1. Naddržavne organizacije kao učesnici sukoba u sajber prostoru

Za određivanje odnosa među državama u sajber prostoru važno je razumeti i viši i niži nivo organizovanja od državnog. Na nadnacionalnom planu, države se udružuju u **regionalne zajednice**, prihvatajući zajedničke kulturne, ekonomske, bezbednosne i uopšteno, civilizacijske norme[350] sa ciljem unapređenja sopstvene i zajedničke efikasnosti stvaranjem sinergijskog efekta u kome funkcionisanje zajednice omogućava dodatne vrednosti u odnosu na prosti zbir ostvarenih vrednosti pojedinačnih elemenata. Međutim, taj proces udruživanja je posledica ispoljavanja nacionalne moći ključnih aktera, pre svega na ekonomskom, političkom i odbrambeno-bezbednosnom planu. To implicira da proces integracije ne predstavlja društvenu zakonitost. Često veći uticaj na to da li će se države prikloniti nekoj grupi država u poštovanju nekog međunarodnog pravnog akta, ma koliko ta grupa velika bila, ima stanje i obim nacionalne moći, nego pravne odredbe koje su prihvaćene od strane zajednice[351].

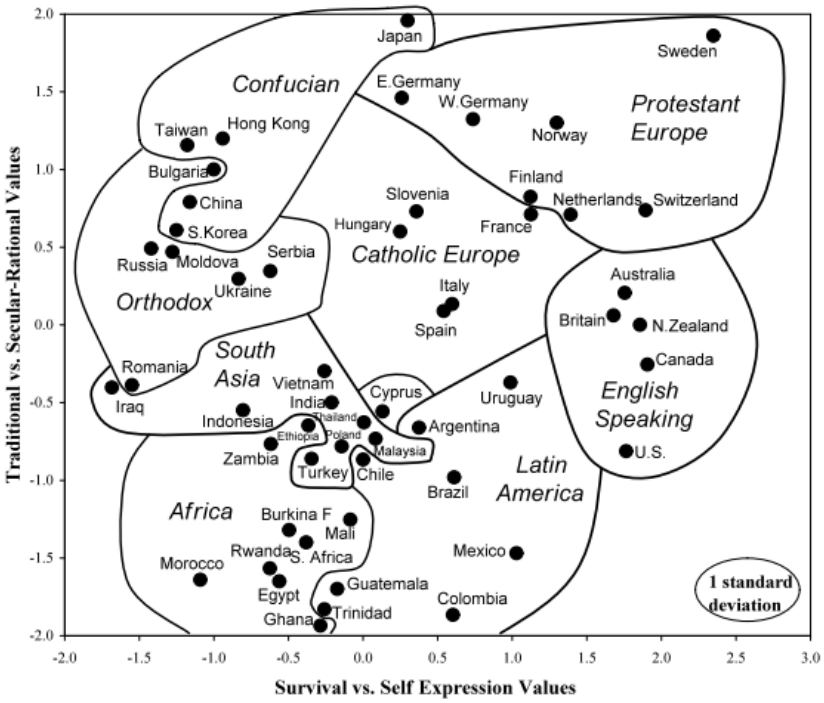
Pod višim nivoima organizacije država smatraju se sve vrste organizovanog **međunarodnog udruživanja** koje je zasnovano na volji država. Države formalnim udruživanjem ostvaruju različite interese na osnovu deljenja zajedničkih resursa, sposobnosti i vrednosti na biološkim (rasnim, i delimično plemenskim i nacionalnim), društveno-političkim (nacionalna kultura[352], jezik, ideologija, politički sistem, oblik

[350] Na primer, u UN.

[351] Na primer, SAD su aktivno učestvovale u izradi *Konvencije Ujedinjenih Nacija o pravu mora* (The United Nations Convention on the Law of the Sea - UNCLOS), ali je nisu ratifikovale iz ekonomskih razloga.

[352] Teorija kulturnih dimenzija Gerta Hofstedea ističe šest karakterističnih faktora koji određuju kulturu nekog društva: individualizam-kolektivizam; izbegavanje neizvesnosti; distanca moći (jačina društvene hijerarhije), muškost-ženstvenost (orjentacija na izvršenje zadataka nasuprot orjentaciji ka ličnosti); dugoročna orjentacija i zadovoljenje (trenutno) – uzdržavanje (u cilju ostvarenja višeg cilja).

organizacije društva i državne vlasti), ekonomskim, bezbednosnim (način ispoljavanja nacionalne moći) i drugim relevantnim osnovama. Stanovništvo pojedinačnih država može imati identično nacionalno i religijsko poreklo, isti ili sličan jezik, deliti identične ili slične kulturne vrednosti i interesovanja. Na osnovu toga, udružujući pojedinačne sposobnosti, nacije dele zajedničku politiku u međunarodnim odnosima i sprovode je kroz zajedničke akcije i funkcije. U tom procesu bliskost i stepen povezivanja država zavisi od kulturološke, društveno-političke, ekonomske, vojno-bezbednosne i drugih vrsta povezanosti (Slika 13).



Slika 13. Položaj 53 nacionalne zajednice na globalnoj kulturnoj mapi u periodu 2005-2007. Ronald Inglehart and Christian Welzel, "Changing Mass Priorities: The Link Between Modernization and Democracy [353]

Navedeni koncept opisuje efekte karakteristične društvene kulture na vrednosti koje prihvataju članovi tog društva i kako te vrednosti utiču na ponašanje članova društva i društva u celini. Hofstedeov koncept se može primeniti na svaki vid komunikacije između različitih kultura, pa tako i na širi aspekt sukoba u sajber prostoru.

Geert Hofstede, Gert Jan Hofstede, and Michael Minkov, *Cultures and Organizations: Software of the Mind*. Vol. 2 (London: McGraw-Hill, 1991);

Geert Hofstede, *Culture's Consequences: International Differences in Work-related Values,* Vol. 5 (Thousand Oaks CA: Sage Publications, 2001).

[353] Ronald Inglehart and Christian Welzel, "Changing Mass Priorities: The Link Between Modernization and Democracy," *Perspectives on Politics* Vol. 8, No. 02 (2010): 551-567.

Od elemenata zajedništva, a pod dejstvom nacionalnih interesa i metoda ispoljavanja moći u međunarodnim odnosima, zavisi i angažovanje država u sukobima i ratovima, uključujući i u sajber prostoru, a time i u oblasti sajber odbrane i bezbednosti. U oblasti bezbednosti i odbrane, nacionalna kultura nije imaginarni faktor, već realni koji utiče na angažovanje nacija u ratu. Primer za ovu tvrdnju se može naći u poređenju operativnih kapaciteta za sajber bezbednost i odbranu Evropske Unije (EU) i takozvane Zajednice „Pet očiju“ [354] ili UKUSA[355].

U okviru EU, sve članice dele zajedničke evropske vrednosti koje predstavljaju fundamentalne elemente kulture. One određuju značenje i značaj određenih kategorija za ljude koji pripadaju određenom društvenom sistemu.[356] Te vrednosti u zajednici većeg broja država sa raznorodnim nacionalnim kulturama, tradicijom i jezicima, kakav je EU,[357] predstavljaju važan faktor kohezije, pa su predmet intenzivnog proučavanja.[358, 359] One nisu statične, pogotovu u zajednici više članova, već se dugoročno razvijaju i menjaju u skladu sa vremenom, globalnim i regionalnim događajima i dinamikom međunarodnih

[354] Neslužbeni, ali rašireni naziv za višedecenijsku, institucionalizovanu grupu država engleskog govornog područja, koje su uspostavile formalni sistem razmene obaveštajnih informacija i servisa. Uključuje SAD, Veliku Britaniju, Kanadu, Australiju i Novi Zeland. Zajednica ovih država je zasnovana na više multilateralnih međunarodnih sporazuma. U nekim programima, ovoj grupi države su priključene i druge države, poput Holandije, Francuske, Norveške i Danske („Devet očiju“), odnosno Nemačka, Belgija, Italija, Švedska i Španija („Četrnaest očiju“). U nekim dokumentima je korišćen nezvanični naziv („41-oko“) za označavanje široke vojne koalicije američkih saveznika u savezničkoj vojnoj koaliciji protiv Talibana u Avganistanu.

[355] *United Kingdom – United States of America Agreement* (UKUSA). Reč je o seriji multilaterialnih međunarodnih sporazuma između Velike Britanije i SAD u oblasti saradnje u međunarodnom elektronskom nadzoru i obaveštajnom radu u svetu, kome su se priključile Kanada, Australija i Novi Zeland, a koji je započet još 1940. godine.

National Security Agency, „Ukusa Agreement Release 1940-1956“, June 24, 2010, https://www.nsa.gov/public_info/declass/ukusa.shtml (preuzeto 20. maja 2015).

[356] EuropeanValues.info Association, „Definition of the Most Basic European Values and Their Significance for Our Modern Society“, 4, http://europaeischewerte.info/fileadmin/templates/Documents/ewdef_en.pdf (preuzeto 29. januara 2016).

[357] Charles Grant, „What are European Values?,“ *The Guardian*, March 25, 2007, http://www.theguardian.com/commentisfree/2007/mar/25/whyvaluesmatterinawidere (preuzeto 10. oktobra 2015).

[358] Leibniz Institute for the Social Sciences, „European Values Study,“ *Gesis*, January 25, 2016, http://www.gesis.org/en/services/data-analysis/survey-data/european-values-study/ (preuzeto 22. januara 2016).

[359] Loek Halman, Inge Sieben and Marga van Zundert, *Atlas of European Values. Trends and Traditions at the Turn of the Century* (Leiden, Netherlands: Brill, 2011).

odnosa.[360] Međutim, nacionalni interesi su ipak ispred opštih zajedničkih vrednosti koje deli naddržavna zajednica.

Pošto je EU politička zajednica država koja je izrasla iz ekonomske zajednice, logično je da su zajednički interesi njenih članica prvenstveno ekonomske prirode, a da zajednička politika podržava te interese. To se odslikava i na zajedničku politiku u oblasti sajber bezbednosti i odbrane. EU je usvojila zajedničku strategiju sajber bezbednosti i formirala je civilnu *Evropsku agenciju za mrežnu i informacionu bezbednost* (ENISA)[361]. Međutim, EU kao zajednica država nema jedinstvenu vojsku, niti operativne kapacitete za odbranu u fizičkom okruženju ili sajber prostoru.[362,363] Odbrambene sposobnosti EU se stoga primarno razvijaju kroz uspostavljanje zajedničke politike odbrane[364] i funkcionisanje institucija za koordinaciju, interoperabilnost i razvoj vojnih sposobnosti, poput *Evropske odbrambene agencije*.[365] Navedena agencija je, između ostalog, nadležna i za razvoj sposobnosti EU za sajber odbranu.[366] Taj razvoj je prvenstveno usmeren ka upravljanju sposobnostima za obuku i trening, podizanju svesti u području informacione bezbednosti, unapređenju razvojno-istraživačkih kapaciteta i razvoju nekih specifičnih (neoperativnih) sposobnosti u oblasti sajber bezbednosti i odbrane, poput detekcije pretnji i zaštite

[360] Leibnitz Institute for the Social Studies, „EVS Waves – Study Overview," *Gesis*, December 21, 2015, http://www.gesis.org/en/services/data-analysis/survey-data/european-values-study/study-overview/ (preuzeto 22. januara 2016).

[361] European Union Agency for Network and Information Secuirty

[362] Neil Robinson, Agnieszka Walczak, Sophie-Charlotte Brune, Alain Esterle and Pablo Rodriguez, *Stocktaking Study of Military Cyber Defence Capabilities in the European Union (milCyberCAP) Unclassified Summary*, *RAND Europe*, 7, http://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR286/RAND_RR286.pdf (preuzeto 5. januara 2016).

[363] Jennifer Valentino-Devries and Danny Yadron, „Cataloging the World's Cyberforces", *The Wall Street Journal*", October 11, 2015, http://www.wsj.com/articles/cataloging-the-worlds-cyberforces-1444610710 (preuzeto 22. decembra 2015).

[364] Zajednička bezbednosna i odbrambena politika EU (eng. *Common Security and Defence Policy* – CSDP) deo zajedničke spoljne politike EU i formalno je definisana nizom dokumenata EU, EUR-Lex, *The EU's Common Security and Defence Policy*, *EUR-Lex*, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Aai0026 (preuzeto 22. decembra 2015).

[365] European Defence Agency – EDA, https://www.eda.europa.eu/

[366] Wolfgang Röhrig and Rob Smeaton, „Cyber Security and Cyber Defence in the European Union: Oportunities, Synergies and Challenges," *Cyber Security Review*, http://www.cybersecurity-review.com/articles/cyber-security-and-cyber-defence-in-the-european-union (preuzeto 14. novembra 2015).

informacija.[367] Međutim, ne i u stvaranje izvršnih zajedničkih operativnih kapaciteta za izvođenje operacija u sajber prostoru. Ključna kolektivna sposobnost EU koja je iskazana u njenoj zajedničkoj politici nije operativna sposobnost kolektivne odbrane od vojnog napada spolja, već očuvanje mira, učešće u mirovnim operacijama, prevencija sukoba i jačanje međunarodne bezbednosti.[368]

Međutim, odsustvo operativnih snaga ne znači da su države članice EU nebranjene od pretnji iz sajber prostora. Ključni dokument kojim je uspostavljena zajednička politika odbrane EU, Lisabonski sporazum, navodi da ta zajednička politika treba da vodi ka zajedničkoj odbrani i u tom pogledu predviđa učešće vodećih vojnih država EU u izgradnji zajedničkih vojnih snaga, sposobnih da izvode vojne operacije.[369] Pojedini predstavnici vlasti nacionalnih država u okviru EU smatraju čak da evropskim državama nije neophodan NATO, pored mogućnosti da na osnovu Lisabonskog sporazuma ostvare kolektivnu odbranu.[370]

Sve članice EU, osim šest vojno neutralnih država[371] su deo **Organizacije Severnoatlantskog sporazuma** (NATO)[372]. Čak i te neutralne države ostvaruju značajne političke, bezbednosne i odbrambene veze sa NATO[373]. Ova vojna organizacija se sastoji od jedinica i pripadnika nacionalnih armija članica. Shodno vojnom, političkom i ekonomskom uticaju SAD, ova država ima dominantnu ulogu i najveću zastupljenost na nivou donosioca odluka i u vojnoj strukturi saveza.[374] Finansijske resurse za odbranu

[367] European Defence Agency, *Cyber Defence Fact Sheet*, February 10, 2015, https://www.eda.europa.eu/docs/default-source/eda-factsheets/2015-02-10-factsheet_cyber-defence (preuzeto 14. novembra 2015).

[368] European Union External Action, „Security and Defence – CSDP," http://www.eeas.europa.eu/csdp/ (preuzeto 2. februara 2016).

[369] Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007, OJ C 306, 1–271, član 28, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12007L%2FTXT (preuzeto 15. novembra 2015).

[370] Andrew Rettman, „Sweden: Who Needs NATO, When You Have the Lisbon Treaty?" *EU Observer,* April 22, 2013, https://euobserver.com/news/119894 (preuzeto 22. april 2016).

[371] Švedska, Finska, Malta, Irska, Austrija i Kipar.

[372] North Atlantic Treaty Organization (NATO), http://www.nato.int/

[373] Stanley R. Roan, „NATO's 'Neutral' European Partners: Valuable Contributors or Free Riders?," *NATO Review Magazine*, 2013, http://www.nato.int/docu/review/2013/partnerships-nato-2013/NATOs-neutral-European-partners/EN/index.htm (preuzeto 22. februara 2016).

[374] NATO, „Military Organisation and Structures," July 15, 2014, http://www.nato.int/cps/en/natolive/topics_49608.htm (preuzeto 12. decembra 2015).

NATO savezu obezbeđuju države članice, prvenstveno kroz ulaganje u vlastite odbrambene kapacitete u skladu sa koordinisanim planovima i zajedničkim odlukama saveza. Po finansijskom izveštaju NATO iz 2015. godine, od ukupno 892,7 milijardi dolara, koliko je 28 država saveza izdvojilo za potrebe nacionalne odbrane i funkcionisanje vlastitih armija u 2015. godini, na SAD se odnosi čak 650 milijardi dolara ili 73% ukupno utrošenih finansijskih sredstava.[375] Posle SAD, članice NATO koje najviše izdvajaju budžetskih sredstava za odbranu su Velika Britanija sa 58,5 milijardi dolara; Francuska (42,1); Nemačka (37,5); Italija (17,5); Kanada (15,6); Turska (12,4); Španija (10,4); Poljska (10.3) i Holandija (10,5), dok ostale države saveza izdvajaju značajno manje iznose.[376] Brojčano, u živoj sili, SAD učestvuje sa ukupno 1,4 miliona aktivnih vojnika od ukupno 3.3 miliona vojnika NATO, [377] dok su u pogledu raspolaganja sa tehničkim borbenim sredstvima, primene mrežnocentrično orjentisanih sistema i naprednih informacionih tehnologija koji im omogućavaju sposobnosti za operacije u sajber prostoru daleko najrazvijenija članica saveza, ali i u globalnim razmerama. U pogledu kapaciteta za sajber odbranu u okviru NATO saveza, može se uočiti da države koje imaju najrazvijenije vojne snage i izdvajaju najveća sredstva za njihovo funkcionisanje i razvoj, ujedno imaju i najrazvijenije vojne kapacitete za izvođenje vojnih operacija u sajber prostoru.[378]

EU i NATO ostvaruju strategijsko partnerstvo u oblasti odbrane, uključujući i sajber odbranu[379]. Glavni centar za razvoj sposobnosti NATO u Evropi je **Kooperativni centar izuzetnosti za sajber odbranu** (CCDCOE) [380] u Talinu. Njegovi ključni ciljevi su obuka, istraživanje i razvoj u oblasti sajber odbrane. CCDCOE je uspostavljen u Estoniji 2008.

[375] NATO, „NATO Publishes Defence Expenditures Data for 2014 and Estimates for 2015: Financial and Economic Data Relating to NATO Defence," Communique PR/CP(2015)093-COR1, press release, Bruxelles, Belgique, NATO Press & Media, June 22, 2015, 4, http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2015_06/20150622_PR_CP_2015_093-v2.pdf (preuzeto 12. decembra 2015).

[376] Ibid.

[377] Ibid, 10.

[378] Jennifer Valentino-Devries and Danny Yadron, „Cataloging the World's Cyberforces", The Wall Atreet Journal", October 11, 2015, http://www.wsj.com/articles/cataloging-the-worlds-cyberforces-1444610710 (preuzeto 22. decembar 2015).

[379] NATO, „NATO-EU: A Strategic Partnership," September 28, 2015, http://www.nato.int/cps/en/natohq/topics_49217.htm (preuzeto 22. februara 2016).

[380] Eng. *Cooperative Cyber Defence Centre of Excellence* (CCDCOE)

godine, odmah nakon širokog DDoS napada[381] na estonske vladine i finansijske institucije u sajber prostoru. Taj napad su pokrenule ruske nacionalne patriotske snage[382] (nedržavne grupe, bez dokaza) u znak odmazde za uklanjanje spomenika ruskim vojnicima iz Drugog svetskog rata, 2007. godine[383]. Dakle, snaga sajber odbrane država članica EU ne leži niti u odbrambenim strukturama EU, niti u NATO savezu, već u sopstvenim kapacitetima, [384] kao i u odbrambenom „kišobranu" koji im pružaju SAD. Međutim, koliko to može imati negativnih posledica po ostvarivanje sopstvenih nacionalnih interesa i po nacionalnu bezbednost pokazuju (zvanično nepotvrđeni) dokumenti, objavljeni zaslugom uzbunjivača Edvarda Snoudena[385], o međusobnoj špijunaži saveznika u okviru NATO i EU.

[381] Eng. *Distributed Denial of Service*

[382] Nedržavne grupe, za koje na Zapadu postoji sumnja da su povezane sa Ruskom vladom, ali za to nikada nisu objavljeni dokazi o povezanosti sa ruskom vladom.

[383] Mladenović, *Međunarodni aspekt sajber ratovanja*, 176-178.

[384] James A. Lewis, Katrina Timin, Center for Strategic and International Studies, *Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization*, United Nations Institute for Disarmament Research - UNIDIR, 2011, http://unidir.org/files/publications/pdfs/cybersecurity-and-cyberwarfare-preliminary-assessment-of-national-doctrine-and-organization-380.pdf (preuzeto 13. decembra 2015).

[385] Edvard Snouden (eng. *Edward Snowden*) je bivši administrator mreže u centrali NSA na Havajima, koji je taj posao obavljao u svojstvu zaposlenog lica u kompaniji *Booz Alen Hamilton*. Za vreme obavljanja dužnosti izneo je veliku količini strogo poverljivih dokumenata američke obaveštajne agencije NSA (po nekim procenama čak oko 1.7 miliona dokumenata u elektronskom obliku) i prebegao prvo u Hong Kong, a zatim u Rusiji. Te dokumente je dostavio nekolicini medijskih glasila u SAD; Velikoj Britaniji i Nemačkoj, nanevši neprocenjivu štetu interesima SAD. Motiv za to delo mu je, po sopstvenom priznanju, bila želja da zaustavi neograničeno narušavanje ljudskih prava na privatnost od strane NSA i savezničkih agencija koje te agencije vrše u toku globalnog i nacionalnog nadzora aktivnosti domaćih i stranih građana u sajber prostoru. Većina objavljenih dokumenata koje je preuzeo iz NSA i predao medijima se može naći na nekoliko specijalizovanih portala na Internetu.

Glenn Greenwald, *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State* (New York, Henry Holt and Company, 2014).

„42 Years for Snowden Docs Release, Free All Now," *Cryptome*, https://cryptome.org/2013/11/snowden-tally.htm (preuzeto 13. decembra 2015);

Snowden Doc Search, https://search.edwardsnowden.com/ (preuzeto 13. decembra 2015).

Drugi karakterističan primer je *UKUSA* zajednica ili zajednica „*Pet očiju*“[386], koju čine: SAD, Velika Britanija, Kanada, Australija i Novi Zeland[387]. Zajednica „Pet očiju“ ima dugu tradiciju postojanja, koja datira od 1940. godine.[388] Zasnovana na zajedničkim interesima, ova zajednica je veoma čvrsta i elastična. Sukobi po pitanju zajedničkih interesa u okviru nje se brzo rešavaju. Tokom perioda njenog postojanja, svega dva puta je neka država privremeno izašla iz programa razmene obaveštajnih informacija i zajedničkih projekata: to se desilo 1986. godine, nakon što je Novi Zeland odbio da u svoju luku primi nuklearni ratni brod mornarice SAD i 2003. godine, kada se Kanada nije pridružila SAD u ratu protiv Iraka[389]. Međutim, od tog perioda veza između obaveštajnih i vojnih agencija SAD, Velike Britanije i Australije je postala još čvršća i bliža. Na primer, Velika Britanija i Australija imaju (ograničeni) pristup poverljivoj vojnoj obaveštajnoj mreži SAD, pod nazivom SIPRNet.[390]

Ova bezbednosna zajednica država je stvorena na osnovu niza bilateralnih i multilateralnih sporazuma i poseduje najrazvijenije kapacitete i sposobnosti za sajber

[386] Neslužbeni, ali rašireni naziv za višedecenijsku, institucionalizovanu grupu država engleskog govornog područja, koje su uspostavile formalni sistem razmene obaveštajnih informacija i servisa. Uključuje SAD, Veliku Britaniju, Kanadu, Australiju i Novi Zeland. Zajednica ovih država je zasnovana na više multilateralnih međunarodnih sporazuma, U nekim programima, ovoj grupi države su priključene Holandija, Francuska, Norveška i Danska („Devet očiju“), odnosno Nemačka, Belgija, Italija, Švedska i Španija („Četrnaest očiju“). U nekim dokumentima je korišćen nezvanični naziv („41-oko“) za označavanje široke vojne koalicije američkih saveznika u savezničkoj vojnoj koaliciji protiv Talibana u Avganistanu.

[387] Ewen MacAskill and James Ball, „Portrait of the NSA: No Detail too Small in Quest for Total Surveillance,“ *The Guardian*, November 2, 2013, http://www.theguardian.com/world/2013/nov/02/nsa-portrait-total-surveillance (preuzeto 12. avgusta 2015).

[388] National Security Agency, „Ukusa Agreement Release 1940-1956“, June 24, 2010, https://www.nsa.gov/public_info/declass/ukusa.shtml (preuzeto 20. maja 2015).

[389] Greg Sheridan, *The Partnership: The Inside Story of the US-Australian Alliance Under Bush and Howard* (Sydney, Australia, University of New South Wales Ltd., 2006), 108.

[390] Bob Brewin, „NSA Seeks to Open Classified Network to Allies,“ May 17, 2007, http://www.govexec.com/defense/2007/05/nsa-seeks-to-open-classified-network-to-allies/24458/ (preuzeto 20. maja 2015).

odbranu, obaveštajne aktivnosti elektronski nadzor u svetu.[391, 392] Njihove obaveštajne programe za elektronski nadzor u sajber prostoru razvijaju i predvode američka agencija NSA i britanske agencije za elektronski nadzor GCHQ (eng. *Government Communications Headquarters*). U poslednjoj deceniji su postigli veliki uspeh u praćenju elektronske komunikacije svake osobe u svetu u svakom trenutku. Dokumenti koje je obelodanio Edvard Snouden pokazali su da je samo britanska agencija GCHQ 2012. godine bila u stanju da dnevno presreće 600 miliona telefonskih poziva u svetu[393]. Te agencije su uz podršku agencija ostale tri države zajednice izgradile jedinstvenu supersilu u oblasti elektronskog nadzora i obaveštajnog rada u sajber prostoru, po kapacitetima i sposobnostima vodeću u svetu[394]. Na osnovu uvida u tajne dokumente agencije NSA, Snouden je dao ocenu da navedeni program saradnje NSA i GCHQ predstavlja „najveći program nadzora u ljudskoj istoriji“ [395]. Stepen njihove povezanosti, s jedne strane, je toliko visok, da države međusobno omogućavaju odgovarajućim stranim obaveštajnim agencijama iz zajednice da uzajamno nadziru čak i vlastito stanovništvo[396]. S druge

[391] U toku višedecenijske saradnje, navedena zajednica je ostvarila veliki broj projekata elektronskog nadzora celog sveta. Najpoznatiji među njima je raniji projekat pod nazivom Ešelon (eng. *Echelon*). Ovaj sistem zemaljskih i satelitskih stanica za nadzor elektronskih komunikacija u svetu je raspoređen širom planete i u stratosferi. Postoje indicije da se navedeni sistem koristio čak i za nadzor komunikacija bliskih saveznika, pa i u svrhe industrijske špijunaže. Evropski parlament je čak i osnovao privremeni komitet sa ciljem da razmotri izveštaje o obaveštajnim aktivnostima zajednice „Pet očiju“ usmerenim prema državama EU, dao direktive nadležnim agencijama za preduzimanje mera u cilju zaštite od špijuniranja i preporučio građanima evropskih država da koriste metode zaštite ličnih podataka u sajber i elektronskom prostoru. Izraz „bez opravdane sumnje“ podrazumeva da se prate osobe koje su učesnici komunikacija u elektronskom i sajber prostoru, a ne osobe koje su osumnjičene da su učinile protivzakonitu aktivnost.

Gerhard Schmid, "On the Existence of a Global System for the Interception of Private and Commercial Communications (ECHELON Interception System), 2001/2098(INI)," July 11, 2001, *European Parliament: Temporary Committee on the ECHELON Interception System*, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A5-2001-0264+0+DOC+XML+V0//EN (preuzeto 12. avgusta 2015).

[392] James Bamford, *The Shadow Factory: The Ultra-Secret NSA from 9/11 to the Eavesdropping on America* (New York: Anchor Books, 2008).

[393] Ewen MacAskill, Julian Borger, Nick Hopkins, Nick Davies and James Ball, „GCHQ Taps Fibre-optic Cables for Secret Access to World's Communications,“ *The Guardian*, June 21, 2013, http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa (preuzeto 11. avgusta 2015).

[394] Ibid.

[395] Edward Snowden (ispitanik), Glenn Greenwald (intervjuista), „Edward Snowden: NSA Whistleblower Answers Reader Questions,“ The Guardian, June 17, 2013, http://www.theguardian.com/world/2013/jun/17/edward-snowden-nsa-files-whistleblower (preuzeto 12. avgusta 2015).

[396] „GCHQ Broke the Law by Spying on UK Citizens,“ Channel 4, February, 6, 2015, http://www.channel4.com/news/gchq-nsa-broke-law-surveillance-prism-snowdown (preuzeto 12. avgusta 2015).

strane, uzajamno omogućavaju pristup internim bazama podataka koji su prikupljeni u tim programima. Britanski časopis Gardijan 2013. godine navodi da je broju od preko 850.000 pripadnika obaveštajne zajednice i privatnih kompanija koje po ugovorima rade za američku vladu omogućeno da pristupaju bazama podataka i servisima britanske agencije GCHQ[397]. Postoji više objavljenih slučajeva da su obaveštajni organi ovih država, pre svega SAD, usmeravali svoje špijunske aktivnosti ka ciljevima u savezničkim državama van ove ekskluzivne zajednice, poput institucija EU[398, 399], UN, i ključnih partnera u NATO savezu. Tokom 2015. godine u svetskoj javnosti su obelodanjeni dokumenti da je agencija NSA decenijama u kontinuitetu špijunirala predsednike i druge organe vlasti u Nemačkoj[400] i Francuskoj[401]. Takođe, bila je angažovana i na zadacima industrijske i finansijske špijunaže vodećih evropskih kompanija koje su bile konkurenti američkim kompanijama na više konkursa na trećim tržištima u svetu.[402, 403]

Zemlje zajednice „Pet očiju“ dele identične ili slične bezbednosne ciljeve, standarde, sisteme, i zajednički koriste poverljive informacione mreže za razmenu obaveštajnih podataka i servisa:

– intranet[404] informacionu mrežu agencije NSA opšte namene, pod nazivom *NSANet* (*National Security Agency Network*), koja omogućava više servisa za pristup i analizu obaveštajnih podataka;

---

[397] MacAskill, Borger, Hopkins, Davies and Ball, „GCHQ Taps Fibre-optic.“

[398] Ryan Gallagher, „Operation Socialist: The Inside Story of How British Spies Hacked Belgium’s Largest Telco,“ *The Intercept*, December 13, 2014, https://theintercept.com/2014/12/13/belgacom-hack-gchq-inside-story/ (preuzeto 12. avgusta 2015).

[399] „Belgacom Attack: Britain's GCHQ Hacked Belgian Telecoms Firm,“ *Spiegel Online International*, September 20, 2013, http://www.spiegel.de/international/europe/british-spy-agency-gchq-hacked-belgian-telecoms-firm-a-923406.html (preuzeto 12. avgusta 2015).

[400] Reuters, „NSA Tapped German Chancellery for Decades, WikiLeaks Claims,“ *The Guardian*, July 8, 2015, http://www.theguardian.com/us-news/2015/jul/08/nsa-tapped-german-chancellery-decades-wikileaks-claims-merkel (preuzeto 12. avgusta 2015).

[401] „US ‘Spied on French Presidents’ – Wikileaks,“ *BBC News*, June 24, 2015, http://www.bbc.com/news/33248484 (preuzeto 12. avgusta 2015).

[402] "Echelon: Big Brother without a Cause," *BBC News*, July 6, 2000, http://news.bbc.co.uk/2/hi/europe/820758.stm (preuzeto 12. avgusta 2015);

[403] Jack Epstein, "Big Surveillance Project For the Amazon Jungle Teeters Over Scandals," *The Christian Science Monitor*, January 25, 1996, http://www.csmonitor.com/1996/0125/25071.html/%28page%29/2 (preuzeto 12. avgusta 2015).

[404] Intranet je računarska mreža za razmenu digitalnih podataka koja koristi neki protokol za umrežavanje i razmenu podatka (na primer, najčešće koristi protokol TCP/IP poput Interneta,), s tim što je pristup njenim resursima ograničen samo za autorizovane članove organizacije/sistema koji je koristi.

- mrežu *PEGASUS* (do 2010. godine pod nazivom *GRIFFIN - Globally Reaching Interconnected Fully Functional Information Network*) koju koriste vojne agencije za ramenu podataka i podršku procesa rukovođenja i komandovanja u okviru zajednice „Pet očiju“;
- mrežu *STONEGHOST* koju kontroliše i održava američka *Vojna obaveštajna agencija* DIA (*Defense Intelligence Agency*), a koriste je vojne obaveštajne agencije država zajednice za razmenu sopstvenih podataka;
- mrežu *CFBLNet* (*Combined Federated Battle Laboratories Network*) koju koristi pet država zajednice i evropske članice NATO saveza za razmenu podataka, podršku razvojnim istraživačkim projektima, kao i za testiranja računarskih i elektronskih vojnih sistema koji se koriste u oblasti računarstva, komunikacija, elektronskog izviđanja i nadzora, komandovanje i slične aktivnosti,
- sistem više mreža[405] *CENTRIX* (*Combined Enterprise Regional Information eXchange System*), zasnovanih na WAN tehnologiji[406], koji se koristi za komunikaciju, razmenu digitalnih podataka, rad vojnih servisa, telefoniranje preko računarskih mreža (*Voice over IP – VoIP*) i druge servise.[407]

Pored ovih mreža u zajedničkoj upotrebi je i više specijalizovanih mreža za operativnu namenu koje koriste obaveštajne agencije država zajednice. Na primer, specijalizovana jedinica agencije NSA, *Tailored Acess Operations* – TAO, koristi posebni mreže za izvođenje specijalnih i obaveštajnih operacija u sajber prostoru, anonimizaciju sopstvenog identiteta i prikrivanje tragova sopstvenih operacija na Interentu, kao i za zaštitu vlastitih mreža.

Sagledavanjem šire slike funkcionisanja zajednice „Pet očiju“ može se zaključiti da je stepen njene strukturne, funkcionalne i operativne povezanosti u procesu izvođenja vojnih

[405] Sa Japanom, Južnom Korejom, ISAF koalicije u Avganistanu, snaga nacija koje učestvuju u programu *Global Counter-Terrorism Force* (GCTF), za kombinovane pomorske snage i druge.

[406] Wide Area Network

[407] „US Military and Intelligence Computer Networks,“ *Electrospaces*, March 11, 2015, http://electrospaces.blogspot.rs/2015/03/us-military-and-intelligence-computer.html (preuzeto 13. juna 2015).

i obaveštajnih operacija u sajber prostoru veći nego u slučaju različitih obaveštajnih agencija unutar mnogih pojedinačnih država[408].

Ova dva primera pokazuju da bliski nacionalni interesi u oblasti odbrane i bezbednosti i bliska nacionalna kultura predstavljaju važniji faktor uspeha funkcionisanja državnih zajednica u aktivnostima bezbednosti i odbrane u sajber prostoru nego bliski ekonomski i politički faktori povezivanja[409]. EU kao ekonomsko-politička zajednica država gotovo da nema nikakve zajedničke kapacitete za sajber odbranu i obaveštajni rad, za razliku od zajednice „Pet očiju", bez obzira što u oba slučaja postoji sličan društveno-politički kontekst. Nacionalni interes u području bezbednosti i odbrane u sajber prostoru je snažnije izražen u odbrambeno-bezbednosnoj, nego u ekonomsko-političkoj zajednici. Navedeni stav može dati doprinos zaključku iz specifičnog ugla bezbednosti i odbrane u sajber prostoru da su države centralni faktor međunarodnih odnosa u svetu, a ne zajednica država. Uspeh zajednica država u oblasti sajber odbrane primarno zavisi od nacionalnih interesa i spremnosti država da razviju zajedničke sposobnosti.

5.2. Države kao ključni učesnici sukoba u sajber prostoru

Države su složeni sistemi, koji imaju specifičnu društvenu i pravnu tradiciju, osnove i vrednosti na kojima su nastale, način organizacije, resurse, kapacitete i nacionalne interese. One su subjekti međunarodnih odnosa i sukoba. Ne postoji opšteprihvaćena definicija države. To potvrđuje činjenica da se države u međunarodno zajednici priznaju međusobno, na osnovu individualnih stavova vlada. U opštem smislu, države su politički organizovane grupe ljudi na određenoj teritoriji, čije granice se mogu vremenom menjati [410]. Konvencija o pravima i obavezama država (Konvencija u Montevideu) definiše državu u odnosu na skup karakteristika: „Država kao lice međunarodnog prava treba da poseduje sledeće kvalifikacije: a) stalnu populaciju; b) definisanu teritoriju; c) vladu i d) kapacitet da uspostavlja odnose sa drugim državama".[411] U pogledu odsustva nekog od

[408] Za razliku od država EU, države zajednice „Pet očiju" nisu u formalnoj političkoj ili ekonomskoj uniji, već samo u sporazumnoj, multilateralnoj bezbednosno-odbrambenoj uniji.

[409] Na osnovama takozvanih „zajedničkih vrednosti".

[410] *Merriam-Webster Dictionary*, s.v. „state", http://www.merriam-webster.com/dictionary/state (preuzeto 12. februara 2016).

[411] *Montevideo Convention on the Rights and Duties of States*, Montevideo, December 26, 1933, http://www.oas.org/juridico/english/treaties/a-40.html (preuzeto 12. februara 2016).

navedenih svojstava ili kao posledice njihovog posedovanja, međunarodni subjekti mogu imati međunarodno-pravni status koji je blizak predstavljenom osnovnom statusu nacionalne države, ali u pogledu pojedinih karakteristika odstupa od njega. U tom pogledu, mogu se prepoznati nacionalne države kao osnovni model državne organizacije, entiteti sačinjeni od više država,[412] već formirani entiteti koji imaju redukovan karakter ili samo pojedina svojstva država[413], i konačno, entiteti koji nisu države, ali teže da to postanu.[414] Same po sebi, države su već složeni sistemi, koji imaju specifičnu društvenu i pravnu tradiciju, osnove i vrednosti na kojima su nastale, način organizacije, resurse, kapacitete i nacionalne interese.

Pod strukturnim delovima država se smatraju pojedinačni organi, institucije i agencije koje izvršavaju neku specifičnu državnu funkciju i/ili aktivnost, ostvarivanjem neke državne nadležnosti, u cilju sprovođenja objedinjene (centralne) državne vlasti u okviru jedinstvene nadležnosti države. U praksi, svi ti elementi, nadležnosti i funkcije potpadaju pod jedinstvenu jurisdikciju državnih sudova. Ipak, važno je naglasiti da je međunarodno pravo dinamičan sistem. Međunarodno pravo oružanih sukoba se bavi oružanim sukobima u odgovornosti političkih subjekata međunarodnog prava, što znači ne samo uzajamno priznatih država.

Po Morgentau[415], krajnji cilj političkog procesa i ispoljavanja oružane sile je težnja ka ostvarenju nacionalnog interesa, koji je od prioritetnog značaja za svaku naciju, pa se nacije prema njemu odnose bez kompromisa, ali u skladu sa resursima i sposobnostima vlastite moći. Ispoljavanje nacionalne politike kroz vojnu moć je svojstveno za državu još od Vestfalskog mira[416]. Od tada ratovi se ne vode između religijskih zajednica (katolika

[412] Razne međunarodne organizacije i savezi država, poput, na primer, NATO saveza, Evropske Unije, Zajednice nezavisnih država, ili bivše Državne zajednice Srbija i Crna Gora.

[413] Na primer, Sveta stolica u Vatikanu i Malteški viteški red.

[414] Narodi, nacionalne manjine, teritorijalna područja u okviru država naseljena stanovništvom koje ne priznaje centralnu vlast države, i koji se nalaze u (oružanom) sukobu sa organima državne vlasti, samoproklamovane vlasti i drugi).

[415] Morgenthau, *In Defense of the National Interest*.

[416] Vestfalski mir (eng. Treaty of Westphalia) je skup sporazuma između cara Ferdinanda III, nekolicine kneževa samostalnih nemačkih kneževina, Holandije, Francuske i Švedske, potpisan 30. januara 1648. godine nakon Tridesetogodišnjeg rata između predstavnika protestantskih i katoličkih država u Evropi i Osamdesetogodišnjeg rata između Španije i Holandije. Ovim sporazumom su postavljeni temelji savremenom međunarodnom sistemu suverenih država, definisanjem četiri osnovna principa u međunarodnim odnosima: suvereniteta nacija uz pravo na samoopredeljenje; pravne jednakosti među nacijama; obavezujućih međunarodnih ugovora između država i međusobnog nemešanja država u njihove unutrašnje poslove. Ovi principi su postali osnova političkog uređenja Zapadne

i protestanata, na čije države su i ovaj sporazum odnosi), već između država. Stav o centralnoj ulozi države u međunarodnim odnosima, uključujući i odnose sukoba i ratova, je danas dominantan u svetu. Po njemu države imaju ključni uticaj na vođenje međunarodnih sukoba i na njihovo regulisanje, bez obzira na okruženje u kome se sukobi izvode i na primenjenu tehnologiju[417]. Osnovni savremeni subjekti sukoba, ujedno i osnovni subjekti međunarodnih odnosa su države.

Klauzevic[418] smatra da je rat proces koji predstavlja nastavak politike, što samo po sebi dozvoljava da učesnici rata mogu imati i državni i nedržavni karakter, uz uslov da bar jedan učesnik rata bude država. Po van Kreveldu[419], kada Klauzevic pominje takozvane "male ratove" (pod ovim pojmom se u savremenom dobu označavaju sukobi države sa nekim nedržavnim entitetom), on ne misli na protivpobunjeničke ratove, već na sukobe koje su (u ime država) vodile lako naoružane paravojne jedinice. Pojam je označavao sukobe koje su vodile lako naoružane paravojne jedinice kao podrška zvaničnim vojnim snagama, na primer, tradicionalno ratovanje stanovnika Krajine u borbama na strani Austrougarske carevine protiv Turske[420], ili angažovanje četničkih i komitskih narodnih jedinica koje su bile vojna podrška regularnim vojnim snagama Kraljevine Srbije u Balkanskim ratovima i Prvom svetskom ratu[421].

Po van Kreveldu, Klauzevic ističe tri glavna elementa svakog rata–- "trojstvo": vlada, vojska i narod[422]. Van Kreveld navodi da su pravni i vojni stručnjaci u periodu između Vestfalskog mira (1648) i Francuske buržoaske revolucije (1789) čak smatrali da narod (kao samostalan entitet, bez vođstva vlade) treba biti izuzet iz vođenja rata uopšte, s

---

Evrope, ali su brzo postali temelj celokupnih savremenih međunarodnih odnosa i međunarodnog prava, sadržani su u Povelji UN i važe i danas kao osnov funkcionisanja međunarodne zajednice.

Treaty of Westphalia, Peace Treaty between the Holy Roman Emperor and the King of France and their respective Allies, 1648, http://avalon.law.yale.edu/17th_century/westphal.asp (preuzeto 2. septembra 2015).

[417] Martin van Creveld, *The Rise and Decline of the State* (Cambidge, UK: Cambridge University Press, 1999).

[418] Beatrice Heuser, „Small Wars in the Age of Clausewitz: The Watershed Between Partisan War and People's War," *Journal of Strategic Studies*, 33, no.1 (2010): 139-162, http://dx.doi.org/10.1080/01402391003603623 (preuzeto 15. februara 2016).

[419] Martin van Creveld, *The Transformation of War* (New York, NY: The Free Press, 1991).

[420] Ibid.

[421] Branko Petranović, *Istorija Jugoslavije 1918-1988: Kraljevina Jugoslavija 1918-1941* (Beograd: Nolit, 1988).

[422] Ibid.

obzirom da je rat posao države, a ne naroda.[423] Stoga, tadašnji evropski vladari od sopstvenog naroda, odnosno od svojih podanika, ali i protivničkih, traže poniznost i poslušnost prema vladajućem sloju.[424] Ovakav stav u velikoj meri proističe iz straha da bi naoružani narod mogao ustati protiv svoje vlade, možda čak i pre nego protiv drugog naroda, u slučaju da postoji vertikalna društvena nestabilnost na relaciji između stanovništva i vlade. I drugi stručnjaci ističu angažovanje državnog aparata u procesu vođenja rata. Na primer, Jablonski[425], tumačeći Klauzevica, smatra da je uslov za uspeh u ratu ostvarivanje harmoničnog funkcionalnog povezivanja tog društveno-političkog "trojstva"[426], pri čemu ističe važan uticaj tehnologije na razvoj strategije ratovanja. Organizovan pristup izboru, organizaciji i primeni nove strategije ratovanja nacije leži na vladi. Nove tehnologije probiližavaju krajnjeg izvršioca-vojnika i strategijski nivo odlučivanja. Transformacija ratovanja novog doba nije posledica decentralizacije vlasti i rasta značaja novih, nedržavnih subjekata - učesnika sukoba, već je posledica novih mogućnosti koje pruža nova tehnologija. Nedržavne organizacije učesnici sukoba su posledica odsustva dovoljno jake vlasti centralne vlade (kao rezultat prethodnog ratnog poraza države, sloma strane vlasti ili unutrašnjih sukoba unutar društva).

Znači, država je centralni akter međunarodnih odnosa i međunarodnog prava[427]. Države su ključni suvereni u međunarodnim odnosima i u tom svetlu je nastalo savremeno međunarodno pravo. Po Goldsmitu i Posneru, izvor međunarodnog prava leži u moći i interesima države, pa se ključna metoda za razumevanje međunarodnog prava svodi na pravilnu primenu teorije racionalnog izbora, koja se odnosi na države.[428] Međunarodno pravo su stvorile države i ono se odnosi na sukobe u kojima učestvuju države. Ti sukobi se vode specifičnim sredstvima, karakterističnim samo za oružane snage. Ratne brodove, borbenu avijaciju, tenkove, obučene i uniformisane vojne jedinice u skladu sa državnim

[423] Van Creveld, *The Transformation of War*.

[424] Ibid.

[425] Pukovnik David Jablonski (eng. David Jablonsky) je istaknuti profesor nacionalne bezbednosti na Odseku za Nacionalnu bezbednosti i strategiju na Ratnom koledžu Karlajl u Pensilvaniji.

[426] David Jablonsky, "US Military Doctrine and the Revolution in Military Affairs," *Parameters* 24, no. 3 (1994): 18.

[427] Eric A. Posner and Alan O. Sykes, "Fundamentals of International Law," in *Economic Foundations of International Law* (Harvard, MA: Harvard University Press, 2013), 6-11.

[428] Jack L. Goldsmith and Eric A. Posner, *The Limits of International Law*, (New York, NY: Oxford University Press, 2005), 4.

ustavnim odredbama, generalno, mogu da imaju isključivo države, a specifično i privatne armije, ali su tada za njihovu upotrebu odgovorne države koje su ih autorizovale da koriste vojno naoružanje.[429] Ovu odgovornost pojačava činjenica da je Generalna skupština UN[430], na svom 72. plenarnom zasedanju usvojila Međunarodnu konvenciju protiv regrutovanja, upotrebe, finansiranja i obuke plaćenika.[431]

[429] U nekim državama u svetu legalno postoje i privatne armije, koje su veće i bolje su vojno opremljene od mnogih nacionalnih oružanih snaga. Najpoznatiji primer je američka kompanija Akademi (eng. *Academi*), čiji bivši nazivi su Blekvoter (eng. *Blackwater*) i *Xe Services*. Ova kompanija je aktivno učestvovala u vojnim aktivnostima (uglavnom fizičkog obezbeđenja) u Iraku i Avganistanu, tokom američkih vojnih operacija u ovim državama nakon 2003. godine. Tokom tog angažovanja, njeni pripadnici su koristili širok spektar pešadijskog i protivoklopnog naoružanja, oklopno-mehanizovanih sredstava, bespilotnih letelica, pa čak i aviona. Ministarstvo odbrane SAD redovno sklapa ugovore i dodeljuje poslove u vezi primene vojne sile, najčešće u poslovima podrške, obezbeđenja, obaveštajnih i specijalnih aktivnosti u raznim zonama operacija u svetu, uprkos više slučajeva ozbiljnih ratnih zločina koje su učinili pripadnici ovih jedinica u zonama operacija u kojima su angažovani. Ipak, oni su u skladu sa SOFA (eng. *Status of Forces Agreement*) bilateralnim sporazumima i američkim MEJA zakonom (eng. *Military Extraterritorial Jurisdiction Act*) sudski procesuirani u SAD za deo tih radnji koje su očigledno bile u suprotnosti sa odredbama Međunarodnog prava oružanih sukoba. Pored kompanije *Academi*, najveće najamničke kompanije u svetu su *Defion Internacional, Aegis Defense Services, Triple Canopy, DynCorp, Erinys, Unity Resources Group, G4S* i *Asia Security Group*. Većina ovih kompanija ima direktne ili indirektne veze sa SAD, Velikom Britanijom i Rusijom, pošto ove države nisu pristupile Međunarodnoj konvenciji protiv regrutovanja, upotrebe, finansiranja i obuke najamnika.

International Convention against the Recruitment, Use, Financing and Training of Mercenaries, G.A. Res. 44/34, U.N. Doc A/44/34 (Dec. 4, 1989), art. 5, para. 1, http://www.un.org/documents/ga/res/44/a44r034.htm (preuzeto 22. januara 2016).

Ali Gharib, „Pentagon Gives Blackwater New Contract“, *North America Inter Press Service*, 28 September 2007, http://ipsnorthamerica.net/news.php?idnews=1078 (preuzeto 22. januara 2016);

Tim Shorrock, „Blackwater: One of the Pentagon's Top Contractors for Afghanistan Training“, *The Nation*, 31 March 2015 http://www.thenation.com/article/blackwater-still-top-pentagon-contractor-afghanistan-training/ (preuzeto 22. januara 2016);

Nathan Hodge, „Layoffs at Blackwter Worldwide (Xe)“, *Wired*, 19 February 2009, http://www.wired.com/dangerroom/2009/02/more-trouble-at/#more (preuzeto 22. januara 2016);

Jeremy Scahill, *Blackwater: The Rise of the World's Most Powerful Mercenary Army* (London, UK: Serpent's Tail, 2007);

Robert O'Harrow Jr, „Blackwater contracts, short on detail“, *The Washington Post,* 8 December 2007, http://search.proquest.com.nduezproxy.idm.oclc.org/docview/410171424?accountid=12686 (preuzeto 22. januara 2016);

Joby Warrick, "CIA Hired Blackwater for Kill Program, Sources Say." *Los Angeles Times,* 20 August 2009, http://search.proquest.com.nduezproxy.idm.oclc.org/docview/422237061?accountid=12686; (preuzeto 22. januara 2016);

Jonathan Karp, "Contractors in War Zone Face Legal Front; Private Firms Like Blackwater could be Held Liable for Casualties during Military Tasks." *Wall Street Journal,* 8 March 2007, Eastern edition. http://search.proquest.com.nduezproxy.idm.oclc.org/docview/398964304?accountid=12686 (preuzeto 22. januara 2016).

[430] G.A. Res. 44/34, art. 5, para. 1.

[431] Ibid.

Realnost da su države centralni akteri međunarodnog prava potiče od činjenice da države stvaraju međunarodno pravo; stupaju u pravne odnose sa drugim državama i odlučuju da li će prihvatati određene ugovore i sporazume iz kojih proističu zakonske obaveze; one svojim postupcima poštuju ili krše obaveze koje proističu iz navedenih sporazuma, ili su žrtve takvog postupanja od strane drugih država i konačno, trpe posledice za učinjeno ponašanje ili dobijaju pravno zadovoljenje od strane međunarodnih tela.[432]

Države su i ključni subjekt međunarodnog prava oružanih sukoba i u pogledu regulisanja sukoba u sajber prostoru. Imajući u vidu ovu ulogu država, sajber sukobi se moraju regulisati pre svega kao sukobi koji se odvijaju između država u sajber prostoru, ali koji dostižu nivo, odnosno posledice oružanih sukoba.

Stav o ključnoj ulozi država kao faktoru koji utiče na formu sukoba nije jedinstven među stručnjacima. Pojedini stručnjaci negiraju stav da su međunarodni odnosi nakon Vestfalskog mira bitno uticali na prirodu sukoba. Ečevaria[433] i Osiander[434] navode da je Vestfalski mir između evropskih sila u sukobu u 17. veku više imao veze sa uspostavljanjem odnosa između sila na političkim, umesto na religioznim osnovama (koji su i doveli do tridesetogodišnjeg sukoba između katolika i protestanata u Evropi), nego sa uspostavljanjem nove strukture međunarodnog sistema zasnovanog na državama. Po Ečevariji, iako je Vestfalski sporazum dao pravo vladarima tadašnjih kneževina da objavljuju rat i sklapaju sporazume sa drugim kneževinama i kraljevinama, to pravo je bilo nepotpuno i relativno, jer sporazumi kneževina – novih država nisu mogli biti usmereni protiv cara Svetog Rimskog Carstva, niti protiv javnog (međunarodnog) mira, uz druge dodatne elemente vlasti cara nad kneževinama. Pored toga, sporazum između cara i kneževina nije mogao da spreči druge aktere (gradove, saveze gradova, organizovane grupe), koje nisu bile među stranama u sporazumu, da u praksi vode svoje oružane sukobe.[435] Dakle, još od Vestfalskog mira, države jesu osnovni faktori međunarodnog prava, ali to ne ometa druge (nedržavne) elemente da ulaze u sukobe, bilo u ime država (kao najamnici u vreme Vestfalskog mira ili kao patriotske, kriminalne ili

[432] Posner and Sykes, "Fundamentals of International Law."

[433] Antulio J. Echevarria II, „Fourth-Generation War and Other Myths," *Strategic Studies Institute, U.S. Army War College* (November 2005), 8-9.

[434] Andreas Osiander, "Sovereignty, International Relations, and the Westphalian Myth," *International Organization*, 55, 2001: 251-287.

[435] Echevarria, „Fourth-Generation War."

terorističke grupe u 21. veku), bilo samostalno, kao nacionalne, manjinske, političke, ili čak kriminalne grupe.

Nakon Vestfalskog mira, male države se ukrupnjuju u veće, organizovane na nacionalnoj, umesto na regionalno-feudalnoj osnovi, i konstantno teže daljem, nadnacionalnom organizovanju. Taj proces je dostigao svoj vrhunac uspostavljanjem sistema Ujedinjenih Nacija nakon Drugog svetskog rata. Međutim, nadnacionalne organizacije nemaju „vlast" nad svojim članicama, državama, niti imaju pravo da ograničavaju njihov suverenitet. To se odnosi čak i na Organizaciju Ujedinjenih Nacija. Sistem međunarodnog prava je zasnovan na političkoj moći država, a ne na univerzalnim ili prirodnim principima pravednosti. Navedeno se može videti na svim nivoima međunarodne organizacije, a ključni momenti su:

- ustrojstvo i odnosi Saveta bezbednosti UN, u kome pet svetskih država, pobednica Drugog svetskog rata, imaju pravo da blokiraju svaku izvršnu odluku od strane međunarodne zajednice koja nije u skladu sa sopstvenim političkim interesima,[436] pa čak i one koje se tiču pokretanja i međunarodnog pravnog regulisanja oružanih sukoba;[437]
- situacija u kojoj države po pravilu pokreću oružane ratove, čak i regionalnog karaktera, bez prethodne odluke Saveta bezbednosti UN;[438]
- osim Povelje UN i Ženevskih konvencija ni jedan drugi sporazum nije u celini prihvaćen i ratifikovan od strane svih država sveta; svaka država bira da li će i u kojoj meri prihvatiti odredbe nekog sporazuma u skladu sa sopstvenim interesima;
- čak i kada neka država prihvati sporazum ili postane članica međunarodne organizacije, ona ima mogućnost da se kasnije povuče iz tog sporazuma ili članstva u toj organizaciji, čiju nadležnost je samostalno priznala.

Ovo je značajno u pogledu ideje da se moguća rešenja za regulisanje odnosa država u sukobu uopšte mogu potpuno pravedno i saglasno opštim principama međunarodnog prava regulisati van sistema međunarodnog ugovornog prava na nivou UN, odnosno

[436] U skladu sa preciziranim načinom glasanja članica Saveta bezbednosti, definisanim članom 27. Povelje UN.

[437] Kao u slučaju blokiranja sprovođenja odluke Međunarodnog suda pravde u slučaju Nikaragva protiv SAD.

[438] Poput sukoba koje je NATO i koalicija oko SAD vodila na području Jugoslavije, Avganistana i Iraka.

najšire međunarodne zajednice, na primer, direktnim pravnim ugovorima i sporazumima između zainteresovanih strana u periodu pre izbijanja sukoba.

5.3. Organizacije kao ključni učesnici sukoba u sajber prostoru

Stvarnu ulogu u sajber prostoru nemaju samo državni organi i vojnopolitički savezi država, već i razne organizacije (na primer poslovne, naučno-istraživačke, akademske, kriminalne ili terorističke grupe), pa čak i individualna lica.

Na subnacionalnom nivou društvene organizacije istovremeno vladaju integrativne i dezintegrativne sile u raznim oblastima ljudskih aktivnosti koje su od značaja za bezbednost. To je posledica delovanja više faktora, među kojima razvoj transportnih i komunikacionih tehnologija i proces globalizacije zauzimaju ključna mesta. Integrativni faktori utiču da nacije i kulturne zajednice i pojedinci postaju sve bliži, a svet sve manji.[439] Ta relativna blizina im omogućava da dele iste resurse i da postaju sličniji u kulturnom pogledu. Međutim, povećana koncentracija interesa oko ključnih resursa povećava konkurenciju koja postaje izvor za nastanak novih sukoba na horizontalnom i vertikalnom nivou.

Skoro svi sajber napadi visoke važnosti u specijalnim i obaveštajnim operacijama u inostranstvu su koristili ranjivosti nultog dana. Tržište ranjivosti i eksploita nultog dana u informacionim sistemima se sve više širi i razvija, a ključni kupci podataka i informacija o njima su države, odnosno njihove obaveštajne agencije.

Po Kimu Ziteru[440] tržište ranjivosti i eksploita nultog dana[441] se sastoji iz tri segmenta:

- **„crno tržište“** na kome kriminalci trguju podacima i informacijama da bi omogućili buduće napade;

[439] Marshall McLuhan je koristio izraz globalno selo (eng. *global village*).

[440] Kim Zetter, „Hacker Lexicon: What is a Zero Day?“ *Wired*, November 11, 2014, http://www.wired.com/2014/11/what-is-a-zero-day/ (preuzeto 12. aprila 2016).

[441] Ranjivost nultog dana (engl. *Zero-day Vulnerability*) se odnosi na bezbednosni propust ili nedostatak u informacionom sistemu, najčešće softveru, koji je nepoznat njegovom proizvođaču, korisniku, ili široj zajednici koja se bavi informacionom bezbednošću. Iako ta ranjivost nije javno poznata, ona može biti poznata napadačima, koji informacije o njoj drže u tajnosti. što im i omogućava napad. Pošto je nepoznata svim subjektima od kojih zavisi odbrana od sajber napada, osim napadaču, informacija o ranjivosti nultog dana omogućava sajber napade. Eksploit nultog dana je izraz koji se koristi za softverski sistem koji priprema napadač u cilju iskorišćavanja ranjivosti nultog dana za neovlašćeni upad u sistem, odnosno sajber napad.

- **legalno ili „belo tržište“** na kome istraživači i hakeri prodaju podatke i informacije o ranjivostima informacionih tehnologija proizvođačima softvera kojima su one potrebne kako bi ih otklonili izradom bezbednosnih zakrpa (eng. *security patches*), kao i bezbednosnim kompanijama za upotrebu u *pentesting* (eng. *penetration testing*) proizvodima kojima utvrđuju da li je sistem klijenta podložan zloupotrebi ovih ranjivosti ili eksploita; i
- **„sivo tržište“**, na kome razni istraživači i privatne kompanije prodaju informacije o ranjivostima i eksploitima nultog dana raznim državnim organima (vojnoobaveštajnim bezbednosnim ili policijsko-istražnim agencijama) koji ih zatim koriste za svoju operativno-obaveštajnu primenu u nacionalnim okvirima ili u inostranstvu.

Potvrda za ovakvu upotrebu ranjivosti i eksploita nultog dana od strane država, može se naći i direktno, u saopštenju predsednika SAD. Po rečima Baraka Obame, informacija o svakom nedostatku u informacionom sistemu koji ima „jasnu upotrebnu vrednost u pogledu nacionalne bezbednosti ili sprovođenja zakona“ može ostati tajna, radi primene u svrhu nacionalne bezbednosti i odbrane.[442] Potvrda da ovakve informacije mogu imati čak i strategijski značaj za nacionalnu bezbednost i vođenje sukoba u sajber prostoru može poslužiti činjenica da je za preduzimanje najpoznatijeg sajber napada do sada u svetu, operacije Staksnet, upotrebljeno najmanje pet različitih eksploita nultog dana.[443]

Od svih drugih mesta za trgovinu podacima i informacijama o ranjivostima i softverom za preduzimanje napada, crno tržište ima najniži formalni prag za pristup, tako da na njemu mogu prikriveno da učestvuju svi, od pojedinaca iz kriminalne zajednice, preko predstavnika privatnog biznisa (bezbednosne kompanije), pa do organizacija iz državnog aparata (vojne, policijske, sudske i obaveštajno-bezbednosne agencije i organi). Ovakva mesta su uglavnom virtuelne prirode. Radi se o onlajn forumima koji u sličnoj formi postoje od kako postoji Internet. Razvojem „*Mračnog veba*“ (eng. *Dark Web*) njihov obim i značaj se veoma povećao. Na njemu se pojavljuju i nestaju razna neformalna, ali

[442] David E. Sanger, „Obama Lets N.S.A. Exploit Some Internet Flaws, Officials Say,“ *The New York Times*, April 12, 2014, http://www.nytimes.com/2014/04/13/us/politics/obama-lets-nsa-exploit-some-internet-flaws-officials-say.html?_r=0 (preuzeto 18. aprila 2016).

[443] Kim Zetter, „Obama: NSA Must Reveal Bugs Like Heartbleed, Unless they Help the NSA,“ *Wired*, April 15, 2014, http://www.wired.com/2014/04/obama-zero-day/ (preuzeto 18. aprila 2016).

vrlo razvijena i nelegalna „tržišta“ za trgovinu raznim nelegalnim stvarima, narkoticima, kriminalnim uslugama, informacijama o ranjivostima ili čak uslugama sajber napad, kao što su na primer *TheRealDeal Market, Silk Road* i druga. Ta tržišta su veoma dinamična, jer kratko traju s obzirom na svoju kriminalnu prirodu, a i same informacije koje su predmet razmene nemaju dugo trajanje, s obzirom da se mogu iskoristiti za napade samo dok nisu poznate u javnosti. Zbog toga je za efikasno trgovanje informacijama na njima potrebno stalno prisustvo i iskustvo učesnika. Pošto ovakva mesta imaju veliki potencijal za nabavljanje informacija od strane obaveštajnih i bezbednosnih agencija, uobičajeno je da pripadnici raznih državnih policijskih, bezbednosnih, pa i odbrambenih agencija prikriveno učestvuju u trgovini i praćenju aktivnosti na ovakvim forumima. Oni, po pravilima organizacije, obezbeđuju visok nivo anonimnosti svih učesnika (trgovaca, kupaca i administratora) u odnosu na većinu državnih agencija, sem onih koje su najefikasnije i imaju najveće resurse poput agencija FBI, NSA, CIA ili GCHQ[444]. Anonimnost se obezbeđuje primenom softvera za anonimizaciju aktivnosti (*Tor pretraživač*), plaćanjem u elektronskoj kriptovaluti (npr. u bitkoinima) ili pravilima da se pristup novim članovima dozvoljava isključivo na osnovu reputacije drugih, starijih članova.

Pored toga što je ovim kriminalnim forumima moguće pristupiti anonimno, ne postoji nikakva prethodna praksa o kvalitetu proizvoda i usluga kojim se trguje, niti garancija. Njih kriminalni forumi nadomešćuju organizacionim merama i savremenim poslovnim modelima, koji im osiguravaju dugo trajanje. Njihovi organizatori su prihvatili finansijske koncepte za obezbeđenje trgovine najpoznatijih komercijalnih trgovačkih ili finansijskih kompanija, koje predstavljaju čuvare poverenja u onlajn transakcijama, jer same osiguravaju uplate za stvarno isporučenu robu (kao *iBay*) ili garantuju povraćaj robe u slučaju da je kupac nezadovoljan (kao *Amazon*). Novac u elektronskoj valuti čeka kod administratora dok se ne dobije potvrda od kupca da je predmet trgovanja isporučen. Pri tome su transakcije višeučesničke (*multisignature*). Iznos u kriptovaluti je rezervisan na adresi koju zajednički i istovremeno kontrolišu kupac, prodavac i administrator berze u svojstvu posrednika. Da bi se izvršila isplata na prodavčev račun, saglasnost moraju da

[444] Andy Greenberg, „New Dark-web Market is Selling Zero-day Exploits to Hackers,“ *Wired,* April 17, 2015, http://www.wired.com/2015/04/therealdeal-zero-day-exploits/ (preuzeto 18. aprila 2016).

daju dva od tri učesnika u transakciji. Takvo posredničko ponašanje nudi svim učesnicima u trgovini sigurnost, a organizatorima omogućava sticanje značajnih provizija od transakcija između učesnika trgovine. U nekim slučajevima, predstavnici berze čak moraju da samostalno testiraju efikasnost eksploita da bi potvrdili njegovu valjanost. Ova okolnost čak pruža prednost organizatorima berze da pored zarade, i sami dođu do informacija o novim sajber napadima.

Informacije o ranjivostima i eksploitima u oblasti informacionih tehnologija na navedenim forumima se obično tiču poznatog i raširenog komercijalnog softvera opšte namene, poput operativnih sistema, internet pretraživača ili softverskih onlajn platformi, kao što su *Apple iClouda*, *WordPress*, ili *Google* onlajn servisa. Cene informacija o ranjivostima se najčešće kreću od nekoliko hiljada, pa sve do nekoliko stotina hiljada američkih dolara.[445]

Pošto su ovakve podzemne računarske mreže anonimne, njihov deo mogu sačinjavati bilo čiji računari, uključujući i agencije za sprovođenje zakona ili obaveštajne agencije raznih država. Zahvaljujući inherentnoj anonimnosti ovakvih mreža, postoji teoretska mogućnost da vladine agencije neke države čak i učestvuju u osnivanju i organizovanju rada ovakvih organizacija, sa ciljem da na lak način dođu do važnih informacija o ranjivostima i napadima. Ove informacije se kasnije mogu upotrebiti za važnije aktivnosti u pogledu odbrane i bezbednosti, poput ofanzivnih operacija u sajber prostoru protiv drugih, neprijateljskih nacija. Ta mogućnost postoji u svakom slučaju koji se zasniva na anonimnom funkcionisanju neformalnih i distribuiranih organizacija u sajber prostoru. Zbog toga nikada nije do kraja jasno ko u stvari stoji iza ovakvih kriminalnih berzi, takozvanih *wistleblower* veb-sajtova kao što je *Wikileaks*, ili hakerskih aktivnosti. Ovakve aktivnosti čak ne moraju ni da budu protivzakonite, jer se odvijaju u skladu sa zakonima za rad obaveštajnih agencija u inostranstvu, na serverima van nacionalnih granica, ili istovremeno na serverima koji se fizički nalaze u raznim državama, upotrebom distribuiranih servisa, pri čemu se ne može utvrditi nacionalna jurisdikcija nad njihovim radom. Te aktivnosti su uvek korisne svim stranama, jer pružaju priliku za sticanje prednosti nad opasnijim protivnikom nego što su kriminalci, neprijateljski nastrojenim

[445] Andy Greenberg, „Here's a Spy Firm's Price List for Secret Hacker Techniques," *Wired*, November 18, 2015, http://www.wired.com/2015/11/heres-a-spy-firms-price-list-for-secret-hacker-techniques/ (preuzeto 23. januar 2016).

državama. Pri tome su i efikasne, jer omogućavaju značajnu korist bez mnogo ulaganja. Stoga sličan način angažovanja vladinih organa u organizovanju kriminalnih aktivnosti predstavlja naročito pogodan model za države koje oskudevaju u resursima za uspostavljanje kapaciteta za sajber ratovanje i obaveštajni rad, ali i terorističkim organizacijama, pa i poslovnim kompanijama. Tako se dolazi do paradoksa da je učešće svih nivoa aktera u sajber prostoru u području bezbednosti i odbrane, kriminalni onlajn forumi na „tamnom vebu“ najefikasnije i potpuno pomešano na mestima gde u praksi ne važe nikakvi zakoni, ni nacionalni, ni međunarodni, već samo specifično „poverenje“, znanje i moć sile.

U vojnom i tehnološkom pogledu, sposobnost navedenih kategorija aktera za izvođenje napada u sajber prostoru kvalitativno zavisi od vrste i dubine relevantnog znanja za izvođenje napada, a kvalitativno od resursa da se to znanje razvije i praktično i efektivno primeni. Ključni značaj u procesu razvijanja sposobnosti za vođenje sajber sukoba nije u raspolaganju sa složenim tehničkim sistemima (oružjem) kao u tradicionalnim sukobima u fizičkom okruženju, već u organizaciji i upravljanju specifičnim znanjem iz oblasti informacione bezbednosti. Upravljanje znanjem i sposobnost specijalnog operativnog rada u velikoj meri zavise od državnih resursa i zakonskih mogućnosti koje države dodeljuju sopstvenim organima i agencijama (u oblasti odbrane, bezbednosti i obaveštajnih aktivnosti), ali nisu ograničene na države.

Mnoge terorističke organizacije izgrađuju organizacionu strukturu i sposobnosti koje im omogućavaju da prikriveno izvode terorističke operacije sa efektima koji su ekvivalentni efektima sukoba između država uprkos sveobuhvatnom nadzoru u elektronskom i sajber prostoru koji izvode mnogobrojne državne policijske, vojne i bezbednosno-obaveštajne agencije. Očit primer za to je napad Al-Kaide 11. septembra 2001. godine na SAD otimanjem i samoubilačkim napadima putničkim avionima, kao i brojni samoubilački napadi u Evropi i svetu izvedeni od strane islamskih terorističkih organizacija u poslednjoj deceniji. Takođe, i same države unajmljuju privatne organizacije za razvoj sistema i sposobnosti aktivnosti u sajber prostoru, koje to rade javno, u skladu sa nacionalnim zakonima, ili tajno, radi prikrivenog izvođenja specijalnih i špijunskih aktivnosti prema drugim državama. Konačno, u svetu postoji veći broj privatnih kompanija koje su razvile sposobnost istraživanja u oblasti informacione bezbednosti i

specijalizovale su se za istraživanje ranjivosti u informacionim sistemima i prodor u informacione sisteme[446]. One u skladu sa razvijenim poslovnim modelom prodaju informacije, znanje, usluge i proizvode državnim agencijama koje ih zatim koriste i za izvođenje napada u sajber prostoru. To čak čine i pojedinci kao samostalni istraživači u oblasti informacione bezbednosti, posebno u oblasti testiranja upada u sisteme i nalaženju i proceni ranjivosti informacionih sistema (softverskih i hardverskih). Po proceni privatne kompanije *ABI Research* to tržište je u 2015. godini na svetskom nivou dostiglo čak 10 milijardi američkih dolara[447].

5.4. Pojedinci kao ključni učesnici sukoba u sajber prostoru

Naravno i pojedinci utiču na mogućnost i način vođenja sukoba u sajber prostoru, i to ne samo kao pripadnici državnih i korporativnih institucija. Crno tržište ranjivosti, eksploita i kriminalnih hakerskih usluga je stvoreno od strane kriminalaca i namenjeno je kriminalcima. Međutim, i ono ima značajan uticaj na vođenje sajber špijunaže i sukoba između država. Međunarodno pravo oružanih sukoba se odnosi na radnje, postupke i aktivnosti u međunarodnim sukobima između država i drugih subjekata međunarodnog prava. Međutim, ono se odnosi i na krivična dela pojedinaca, organizacija i grupa koja su se desila u tom međunarodnom okruženju tokom oružanih sukoba. Na osnovu međunarodnog prava moguće je utvrditi krivicu pojedinca za krivična dela učinjena tokom međunarodnih sukoba za koja ne postoji odgovornost država. Za sve druge odnose (koji se ne tiču oružanih sukoba) nadležne su druge vrste međunarodnog prava, poput međunarodnog krivičnog i ugovornog prava, ili su nadležna pak unutrašnja prava država u skladu sa njihovim suverenim nadležnostima i jurisdikcijom nacionalnih sudova. Imajući u vidu navedenu ulogu država, sajber sukobi se moraju regulisati pre svega kao

[446] U javnosti su najpoznatije kompanije iz SAD, EU i Izraela (po abecednom redu): Ability, Cobham, Core Security, COSEINC, CrowdStrike, CSID, CyActive, Defense Group, DSquare Security, EiQ Networks, Endgame, Exodus Intelligence, FinFisher, Gamma Group, Hacking Team, Hyperion Gray, Juniper Networks, Keen Team, Leo Impact, Mitnick Security, Netragard, ReVuln, Synack, Tripwire, Verint, Vulnerabilities Brokerage International, Vupen, Zerodium i druge.

ABI Research, „$10 Billion Defense Cybersecurity Spending Boosts Cyberwarfare Technologies," London, UK, 12 November 2015, https://www.abiresearch.com/press/10-billion-defense-cybersecurity-spending-boosts-c/ (preuzeto 12. januara 2016).

[447] ABI Research, „$10 Billion Defense Cybersecurity Spending Boosts Cyberwarfare Technologies," November 12, 2015, https://www.abiresearch.com/press/10-billion-defense-cybersecurity-spending-boosts-c/ (preuzeto 12. januara 2016).

sukobi koji se odvijaju između država u sajber prostoru, i koji dostižu nivo, odnosno posledice oružanih sukoba.

6. SAJBER RATOVANJE

"Da sam pitao kupce šta žele, rekli bi mi da žele brže konje".
Henri Ford[448]

Sajber ratovanje predstavlja specifičnu formu vođenja sukoba koji se vodi u sajber prostoru putem primene informaciono-komunikacionih tehnologija. Tehnologija i rat oduvek su ostvarivali uzajamnu vezu. Izraelski vojni istoričar i teoretičar rata, van Kreveld navodi: "Ukoliko je tačno da je svaki deo rata pod uticajem tehnologije, ništa manje nije tačno da na svaki deo tehnologije utiče rat".[449] Sajber ratovanje predstavlja izrazit primer navedene ideje. I druge forme ratovanja u odnosu na područje vojnih dejstava ili na vrstu primenjenih sredstava, poput, na primer, pomorskog, kopnenog, vazdušnog, kosmičkog, oklopno-mehanizovanog, podmorničkog, informacionog ili psihološkog ratovanja su direktno ili posredno zavisne od specifičnih tehnologija. Međutim, retko koja vrsta tehnologije i odgovarajućeg ratovanja je u tolikoj meri tehnološki zasnovana i povezana sa svim aspektima društvenog života, kao što je to slučaj sa informaciono-komunikacionim tehnologijama. U savremenom svetu je teško naći čak i pojedinačnu delatnosti u kojoj informaciono-komunikacione tehnologije ne povećavaju efektivnost i efikasnost tehničkih, organizacionih i društvenih sistema ili ne omogućavaju nove sistemske funkcionalnosti. Ipak, van Kreveld[450] navodi da, iako je uzajamni uticaj ratovanja i tehnologije veliki, pomenuta dva fenomena funkcionišu po suprotstavljenim principima, te da se rat ne može dobiti vođenjem isključivo na osnovu tehnoloških principa, bez uticaja ljudske prirode.

Navedena tvrdnja istorijski jeste tačna, jer ljudi su oduvek donosili odlučujuće odluke o načinu vođenja rata. Ali, razvojem računarstva i informaciono-komunikacionih tehnologija čovečanstvo se približava takozvanoj tački singulariteta[451], koja će gotovo

[448] Iako ne postoje pisani tragovi da je Henri Ford izgovorio navedenu misao, u popularnoj kulturi ona se smatra njegovom izrekom, http://quoteinvestigator.com/2011/07/28/ford-faster-horse/ (preuzeto 24. marta 2016)

[449] Martin van Creveld, *Technology and War: From 2000 B.C: to the Present*, A Revised and Expanded Edition (New York, NY: The Free Press, 1991), 311.

[450] Van Creveld, *Technology and War*, 319.

[451] Singularity Institute for Artificial Intelligence, „What is the Singularity?," 8 September 2011, http://singinst.org/overview/whatisthesingularity/ (preuzeto 24. marta 2016. sa Interent Archive,

sigurno nastupiti u narednih nekoliko decenija, i u kojoj će ljudsku inteligenciju dostići i verovatno nadmašiti veštačka inteligencija sistema.[452, 453] Informacioni sistemi (računari, senzori i mreže) imaju sve veći kapacitet za stvaranje, obezbeđivanje, obradu i transport podataka. Logično je očekivanje da će sukobe između ljudi nakon dostizanja tačke singulariteta voditi tehnički sistemi, sposobniji u odnosu na ljude da prikupe, obrade i upotrebe informacije, da se kreću i borbeno deluju u uslovima i na način na koji ljudi to nisu u stanju da učine zbog prirodnih fizičkih ograničenja. Pri tome, tehnički informacioni sistemi, hardver i roboti (automatizovane, samostalne mašine koje rade u skladu sa instrukcijama softverskih sistema i ljudi) nemaju ljudski moral i volju, sem ukoliko one nisu tehnički programirane. Sa pojavom veštačkih inteligentnih sistema, tehnički borbeni sistemi dobijaju novu funkcionalnost, a vojnu pobedu odnose napredniji algoritmi.

Od svih vrsta tehnološki zasnovanih sukoba, sukobi u sajber prostoru najviše zavise od tehnologije jer postoje samo u tom tehnološki zasnovanom okruženju. Informaciono-komunikacione tehnologije su osnov na kome je nastao sajber prostor. Sposobnosti ovih tehnologija se neprekidno povećavaju u odnosu na očekivanje ljudi i društvene odnose. Rezultat navedenih okolnosti je da se područje vođenja sukoba u sajber prostoru rapidno razvija. Tehnološki napredak podrazumeva stvaranje „novih metoda proizvodnje postojećih proizvoda, novih dizajna koji omogućavaju proizvodnju proizvoda sa značajnim novim karakteristikama, novih tehnika organizacije, marketinga i upravljanja“[454]. U tome leži prava moć sajber ratovanja, njegova zasnovanost na informaciono-komunikacionim tehnologijama koje se neprekidno razvijaju, a ne u trenutnim efektima sajber napada. Pri tome značaj sajber prostora nije veći od značaja informaciono-komunikacionih tehnologija, već je obrnut slučaj.

Međutim, kako utvrditi zakonitosti razvoja i uticaja tehnologije? S obzirom da se radi o praksi ljudskih aktivnosti u industrijskoj proizvodnji, istraživanju i razvoju, potvrdu za to

---

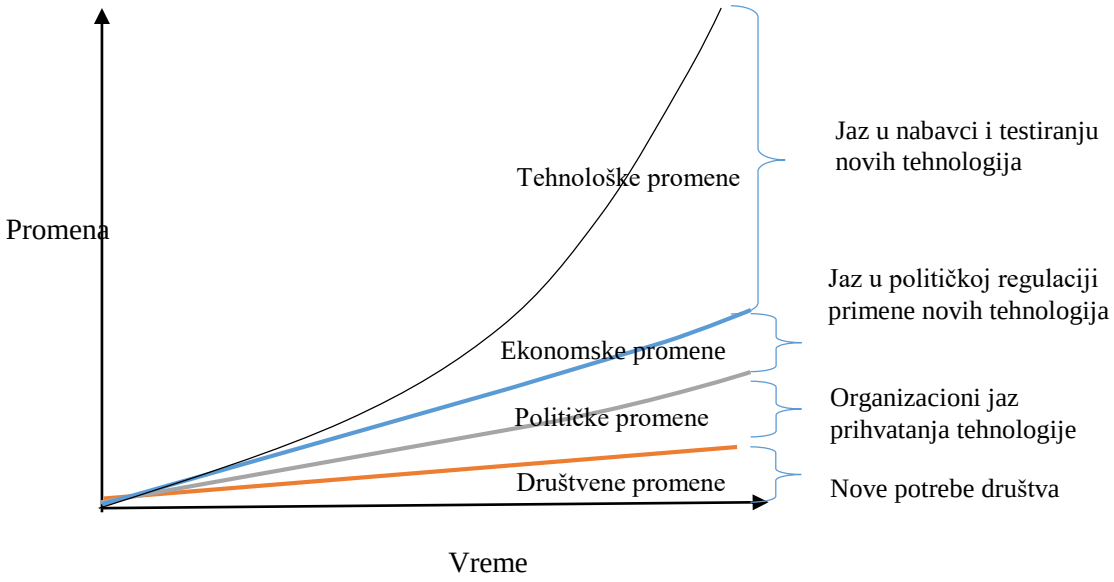
Wayback Machine). https://web.archive.org/web/20110908014050/http://singinst.org:80/overview/whatisthesingularity/

[452] Ray Kurzweil, *The Singularity is Near: When Humans Transcend Bilology* (New York, NY: Viking, 2005), 125.

[453] Vernor Vinge, „What is singularity?“, *Department of Mathematical Sciences, San Diego State University*, 1993, http://mindstalk.net/vinge/vinge-sing.html, (preuzeto 23. marta 2016).

[454] Edwin Mansfield, *Technological Change:An Introduction to a Vital Area of Modern Economics* (New York: Norton, 1971), 10.

ne mogu pružiti prirodni zakoni ili teorije, već opservacije stručnjaka. Po najpoznatijoj, takozvanom Murovom „zakonu“, broj tranzistora po kvadratnom inču industrijski proizvedenih procesora se udvostručuje svake dve godine.[455] Druga opservacije od značaja za sajber prostor, Metkalfov „zakon“ tvrdi da je vrednost komunikacione mreže proporcionalna kvadratu povezanih korisnika sistema (prvobitna verzija ovog stava se odnosila na uređaje)[456] Oba navedena „zakona“ tvrde da se ključni elementi informacionih tehnologija (procesori i mreže) razvijaju eksponencijalno. Međutim, po Daunsu, društveni, ekonomski i pravni sistemi se menjaju linearno postepeno. [457]



Slika 14. Eksponencijalna brzina razvoja tehnologije u odnosu na društvene, političke i ekonomske promene. Defense Information Systems Agency (DISA), DISA Industry Day [458]

[455] Intel Corporation, "Over 6 Decades of Continued Transistor Shrinkage, Innovation," novinsko saopštenje, May 1, 2011 http://www.intel.com/content/dam/www/public/us/en/documents/backgrounders/standards-22-nanometers-technology-backgrounder.pdf (preuzeto 5. oktobra 2015).

[456] Benjamin Metcalfe, "Metcalfe's Law After 40 Years of Ethernet," *Computer* 46, no. 12 (2013): 26-31.

[457] Larry Downes, *The Laws of Disruption: Harnessing the New Forces that Govern Life and Business in the Digital Age* (New York: Basic Books, 2009).

[458] Defense Information Systems Agency (DISA), DISA Industry Day, August 9, 2013, in Chris Scott, „DISA Industry Day: Times Have Changed,“ *CTOvision.com*, https://ctovision.com/2013/08/disa-industry-day-times-have-changed/ (preuzeto 7. novembra 2015).

To utiče na delovanje takozvanog „zakona poremećaja“, koji dovodi do toga da brza promena informacionih tehnologija narušava način na koji postojeće pravo reguliše odnose u mnogim područjima. Ta brzina promene dovodi do situacije u kojoj se stara pravila nasilno (suviše formalno) primenjuju na nove situacije uzrokovane tehnološkim razvojem, koje do tada nisu postojale, ali istovremeno pružaju i nove mogućnosti koje do tada nisu postojale.

Brzina izmene tehnologije i tehničkih sisteme zasnovanih na tehnologiji je u nekim slučajevima ekstremna. Na primer, savremene softverske veb platforme (sistemi), kao što su *Google, Amazon, eBay, Flickr* se ažuriraju na svakih nekoliko minuta.[459] Navedene kompanije imaju ogroman ekonomski uticaj na poslovanje pojedinaca i organizacija širom sveta, jer spadaju među najvrednije tehnološke kompanije u svetu, vrednije od mnogih kompanija iz područja teške i lake industrije.

Operativne sposobnosti savremenih armija (i njihovih protivnika, terorista, asimetričnih pretnji) sve više zavise od tehnologije, pa shodno tome, postoji potreba svih aktera u sukobima da povećavaju brzinu borbenih, obaveštajnih i neborbenih dejstava. Dostupnost i manipulacija podacima je sve više zasnovana na informaciono-komunikacionim tehnologijama. Na primer, prosečno vreme koje je bilo potrebno američkoj vojsci za određivanje cilja i dejstvo po cilju u operaciji „Pustinjska oluja“ 1991. godine je bilo oko četiri dana; u operaciji „Iračka sloboda“ 2003. godine to vreme je bilo oko 45 minuta, a od 2010. godine nakon uvođenja u operativnu upotrebu naoružanih bespilotnih letelica iznad zone operacija, to vreme je oko 10 minuta. [460] Kako navodi Virilio, u informacionom dobu, brzina je moć. [461, 462]

Tehnologija svakako ima presudan uticaj na sajber ratovanje. Međutim, šta to u praksi znači? Tehnologija predstavlja „praktičnu primenu znanja, posebno u nekom specifičnom

[459] Paul M. Duvall, Steve Matyas, and Andrew Glover, *Continuous Integration: Improving Software Quality and Reducing Risk* (New York: Pearson Education, 2007), 190.

[460] Dragan Mladenović, *Međunarodni aspekt sajber ratovanja* (Beograd, Srbija: Medija centar Odbrana, 2012), 22.

[461] Paul Virillio, *Speed and Politics* (New York, NY: Semiotext(e), 1977 [2006]).

[462] Paul Virillio, *Information Bomb* (London, UK: Sage, 2000).

području“[463], „sposobnost koju omogućava praktična primena znanja“[464] ili „način izvršavanja nekog zadatka upotrebom tehničkog procesa, metode ili znanja“[465], odnosno „primenu naučnog znanja u praktične svrhe“[466]. Tehnologiju ne čine samo tehnički sistemi ili metode, ona je „organizacija znanja sa ciljem ostvarenja praktičnih ciljeva“[467]. Dakle, tehnologija ne predstavlja samo sredstva, alate i metode primene znanja, već i sadržaje, strukturu i mreže društvenih odnosa[468]. Stoga, kada ljudi upotrebljavaju tehnologiju u bilo koju svrhu, oni primenjuju ljudsko znanje na organizovan način u cilju izvršenja nekog zadatka. Navedena karakteristika tehnologije je važnija za procenu namere strana u sukobu u toku bilo kog sukoba, bez obzira na okruženje u kome se vodi, nego okolnost da li oružje ima fizičku ili materijalnu prirodu.

6.1. Ratovanje četvrte generacije

Sa razvojem tehnologije menja se način organizacije sistema za ispoljavanje državne moći, kao i odnosi između država. U radu objavljenom u stručnom časopisu Marinskog korpusa Vojske SAD, grupa autora, predvođena Lindom[469] navodi da se na osnovu karakterističnih elemenata sukoba tokom određenih istorijskih epoha, poput primenjene tehnologije i odnosa između zaraćenih strana, forma ratova može podeliti na četiri sukcesivne vrste, odnosno etape ratovanja.[470] (Tabela 5). Navedeni konceptualni okvir Lind je nazvao *ČModerno ratovanje četvrte generacije* (eng. *Fourth Generation of Modern Warfare*)[471] .

[463] *Merriam-Webster*, s.v. „technology,“ http://www.merriam-webster.com/dictionary/technology (preuzeto 16. septembra 2015).

[464] Ibid.

[465] Ibid.

[466] *Oxford Dictionaries*, s.v. „technology“, http://www.oxforddictionaries.com/definition/english/technology (preuzeto 23. marta 2016).

[467] Emmanuel G. Mesthene, *Technological Change: Its Impact on Man and Society* (Harvard, MA: Harvard University Press, 1970), 25.

[468] David M. Kaplan, *Ricoeur's Critical Theory* (Albany, NY: SUNY Press, 2003), 167.

[469] William S. Lind, paleokonzervativni teoretičar i autor više knjiga o savremenom ratovanju.

[470] Lind, Nightengale, Schmitt, Sutton, and Wilson, „The Changing Face of War“: 65-68.

[471] William S. Lind, „Understanding Fourth Generation War,“ *Military Review,* (September-October 2004): 12-16.

Tabela 5. Karakteristike ratovanja po organizaciono-tehnološkim generacijama

Lind, W. S., Nightengale, K., Schmitt, J. F., Sutton, J. W., & Wilson, G. I., The changing face of war: Into the fourth generation, (2001), Marine Corps Gazette, 85(11), 65-68).

Generacija ratovanja	Od	Do	Ključni akteri sukoba	Karakteristična doktrina	Karakteristično oružje
1. Generacija	Vestfalski sporazum	1860	Pešadija	**Masovno ljudstvo** Pešadija gusto postrojena u redove i kolone; jaka vertikalna vojna hijerarhija i disciplina; bliska borba i sporo napredovanje	Musketa (puška sa barutnim punjenjem i glatkom cevi)
2. Generacija	Kraj 19. veka	Prvi svetski rat	Pešadija i artiljerija	**Vatrena moć** Linijska vatra i pokret; jaka formacijska disciplina, priprema bojišta	Puške, mitraljezi i topovi
3. Generacija	Prvi svetski rat	Drugi svetski rat	Mehanizovane snage	**Manevar**	Avioni, tenkovi, podmornice
4. Generacija	Hladni rat	Današnje vreme	Gerilske i pobunjeničke jedinice, nedržavni entiteti, religiozne i terorističke grupe	**Nelinearna - pobunjenička borba** Propaganda, podsticanje pobuna i nemira, tajno organizovanje, teroristički napadi, destabilizacija do urušavanja vlasti i države	Tehnološka razlika između suprotstavljenih strana; asimetrično delovanje; dezorganizacija i deligitimizacija državnog aparata protivnika; iniciranje jačeg protivnika da stalno troši svoje ljudske, materijalne i finansijske resurse radi očuvanja reda u državi do njegovog konačnog poraza

Po konceptu, sistem, organizacija i struktura ratovanja, primenjena taktika, operatika i strategija, forma sukoba, metode i tehnike ratovanja, kao i ciljevi strana u sukobu direktno zavise od okruženja, odnosno od primenjene tehnologije ratovanja:

a) **Ratovanje prve generacije** (17-19. vek) je bilo ratovanje pešadije u neposrednom frontalnom dodiru. Karakteriše ga zbijeni linijski poredak i snažna disciplina.
b) **Ratovanje druge generacije** (period zaključno sa Prvim svetskim ratom) karakteriše linijska (rovovska) borba uz masovnu primenu vatrenog dejstva velike gustine i podrške artiljerije iz pozadine.
c) **Ratovanje treće generacije** (period karakterističan za Drugi svetski rat) predstavlja primenu strategijskog manevra radi uklinjavanja u protivnički poredak ili zaobilaženja njegovog frontalnog borbenog dela u cilju izvođenja dejstva po dubini na njegovu pozadinu. Za ovu generaciju je karakteristična odbrana po dubini vlastitih kapaciteta uz masovno angažovanje ratne tehnike koja omogućava mobilnost, brzinu energičnog dejstva, zaobilaženje neprijateljskih tačaka otpora i uklinjavanje (poput tenkova, aviona, flota brodova i podmornica, primene koncepta "blickriga"[472], desanata iza neprijateljske linije, strategijskog bombardovanja duboko po industrijskim kapacitetima protivnika i presecanja pomorskih linija snabdevanja podmorničkim ratovanjem).
d) **Ratovanju četvrte generacije** nastupa u toku i nakon perioda Hladnog rata. Pošto zbog odvraćanja nuklearnim naoružanjem nije bilo moguće da vojni blokovi međusobno direktno ratuju, dosledno su davali podršku raznim nedržavnim pokretima i grupama u takozvanim „proksi" ratovima, po principu „neprijatelj mog neprijatelja je moj prijatelj". Takođe, kolonijalne sile su nastojale da zadrže

[472] Blickrig (ger. *Blitzkrieg*) – munjeviti rat, metoda ratovanja u kojoj napadač koristi koncentrisane oklopno-mehanizovane snage uz pešadiju i podršku avijacije da probije neprijateljsku odbrambenu liniju i energično prodre u dubinu njegovog borbenog poretka brzim i snažnim napadom, a zatim da izvrši strategijsko okruživanje i uništenje njegovog poretka.

Kenneth Macksey, *Guderian: Creator of the Blitzkrieg* (New York, NY: Stein and Day, 1976);

Andrew J. Pierre and Lucy Edwards Despard. "Guderian: Center of the Blitzkrieg," *Foreign Affairs* 55, no. 1 (October 1976): 216;

William J. Fanning Jr, "The Origin of the Term "Blitzkrieg": Another View," *The Journal of Military History* 61, no. 2 (1997): 283-302; http://search.proquest.com.nduezproxy.idm.oclc.org/docview/195641425?accountid=12686 (preuzeto 18. oktobra 2015).

> svoju vlast i uticaj u kolonijama preostalim nakon Drugog svetskog rata. Nacionalni i politički pokreti za oslobođenje u kolonijalnim i parakolonijalnim državama nisu raspolagali savremenom ratnom tehnikom, već su umesto toga intenzivno koristili ideologiju, propagandu, svest narodnih slojeva, izgradnju masovnih pokreta među stanovništvom, ali i terorizam, gerilske akcije i druge asimetrične oblike sukoba sa ciljem da nadomeste tehnološku razliku u odnosu na vojno jačeg protivnika.[473]

Ratovanje četvrte generacije ima nekoliko značajnih karakteristika, od kojih je ključna asimetrija borbenih dejstava tokom sukoba. U toj formi sukoba po pravilu se sukobljavaju nedržavni pokreti sa državama. Cilj njihovog delovanja u odnosu na jaču stranu je slom, dezorganizacija i delegitimizacija postojeće državne vlasti ili političke i vojne strukture i kampanje jače vojne sile i uspostavljanje vlastitog sistema vlasti. Uprkos tome što vojno razvijenija strana poseduje očiglednu vojnu nadmoć, asimetrično vojno slabiji protivnik napada konstantno, prikriveno i iznenadno, neprekidno pokušavajući da drži protivnika u fazi vanredne situacije, dezorganizuje ga i prisiljava da troši resurse na vlastitu odbranu[474]. Primenom asimetričnih dejstava vrši se neprekidan pritisak na vlast države da angažuje sve raspoložive resurse u cilju borbe, čime se u dužem periodu, dovodi do ekonomskog, društvenog i organizacionog sloma njenog sistema vladavine.

Ovakav model sukoba karakteriše period takozvanog "Rata protiv terora", koji je nastupio nakon terorističkog napada Al-Kaide na SAD 2001. godine. Zbog jednog terorističkog napada, SAD su pokrenule dve velika ratna sukoba (Irak, Avganistan) i čitavu seriju manjih, povremenih, ali konstantnih intervencija i specijalnih operacija u državama šireg regiona (Pakistan, Libija, Sirija, Jemen, Sudan, Somalija), i tako ušle u najduži ratni sukob u svojoj istoriji. Troškovi tih ratova po SAD, koji su pokrenuti kao odgovor na napad bez primene oružja (teroristički napada putničkim avionima) su bili ogromni i uticali su na ekonomsku krizu u SAD, pa čak i u svetu. Po objektivnim procenama, ti troškovi se kreću

[473] William S. Lind, „Understanding Fourth Generation War," *Military Review* (September-October 2004): 12-16.

[474] Lind, Nightengale, Schmitt, Sutton, Wilson, "Changing Face of War", 22-26.
Na primer, šiitski Hezbolah napada Izrael raketama, Tamilski tigrovi su napadali vladine vojne jedinice i naselja u Šri Lanki, Al-Kaida je napadala i pretila SAD.

od 1.700 milijardi dolara (do sredine 2014. godine)[475], što iznosi 14 miliona dolara na jedan sat u periodu od 13 godina,[476] pa do čak 5.000 milijardi dolara.[477] Pa ipak, u području ratnih operacija i u vremenu u kome se sukob vodio, terorizam ne samo da nije uništen, već je značajno ojačao, i dobio je formu nove organizacije sa svojstvom države, ISIL-a[478], koja je obuhvatila područja više bliskoistočnih država zahvaćenih sukobima.

Pošto akteri sukoba četvrte generacije najčešće nisu dve ravnopravne države, već neki nedržavni entitet (gerilska, pobunjenička ili teroristička organizacija) i država ili različiti nedržavni entiteti međusobno (religiozne, nacionalne ili političke grupe),[479] ni rat u ovoj vrsti sukoba se ne može smatrati međunarodnim sukobom u kome nužno učestvuju dve države/grupe država. Sukobi četvrte generacije često spadaju u nemeđunarodne sukobe za koje je nadležan zajednički član 3. Ženevskih konvencija i Dopunski protokol II (Slika 23, str. 237), kao i Međunarodno običajno humanitarno pravo.

Pošto nastoji da dezorganizuje veću vojnu silu, slabiji protivnik konstantno koristi faktor iznenađenja i napad, što za rezultat ima konstantnu primenu aktivnosti bliskih ili identičnih gerilskoj borbi i terorizmu, poput sukoba u Avganistanu, Iraku, Izraelu ili Palestini. U tom pogledu se može smatrati da je administracija američkog predsednika Džordža Buša bila u pravu kada je isticala sintagmu „Rat protiv terora“, iako ovu konstrukciju nije priznavao veliki deo stručne javnosti u svetu, koji smatra da se rat nužno vodi protiv država.

---

[475] Amy Belasco, *The Cost of Iraq, Afghanistan, and Other Global War* (CRS Report No. RL 33110) (Washington, DC: Congressional Research Service, 2014), https://www.fas.org/sgp/crs/natsec/RL33110.pdf

[476] Alex Ellefson, „$14 Million an Hour for 13 Years: War on Terror's Astounding Cost,“ *AlterNet*, 29 December 2014, http://www.alternet.org/world/14-million-hour-war-terror-has-cost-16-trillion (preuzeto 23. mart 2016).

[477] Watson Institute, International & Public Affairs, Brown University, *Cost of War*, http://watson.brown.edu/costsofwar/ (preuzeto 23. marta 2016);

Neta C. Crawford, *U.S. Costs of Warf Through 2014: $4.4 Trillion and Counting, Summary of Costs for the U.S. Wars in Iraq, Afghanistan and Pakistan*, 25 June 2014, http://watson.brown.edu/costsofwar/files/cow/imce/papers/2014/US%20Costs%20of%20Wars%20through%202014.pdf (preuzeto 23. marta 2016);

Mark Thompson, „The $5 Trillion War on Terror,“ *Time*, 29 June 2011, http://nation.time.com/2011/06/29/the-5-trillion-war-on-terror/ (preuzeto 23. marta 2016).

[478] Eng. *Islamic State of Iraq and the Levant*

[479] Sukobi četvrte generacije često imaju formu gerilskih ili pobunjeničkih sukoba i u zapadnoj vojno-političkoj teoriji se nazivaju takozvanim „malim ratovima“ (eng. *small wars*).

Ratovanje četvrte generacije se odvija istovremeno u više ravni, fizičkoj, informacionoj i kognitivno-psihološkoj. Za razliku od sve tri prethodne generacije ratovanja (koje predstavljaju tradicionalno ratovanje) vođama pobunjeničkih ili terorističkih grupa fizička komponenta direktnog sukoba je najmanje bitna. Kognitivno-psihološka komponenta sukoba je važnija, pa su teroristička dejstva usmerena ka svesti protivnika i urušavanju njegove volje da vodi sukob. Sukobi četvrte generacije se ne vode na frontu, već na holistički način: u medijskoj, političkoj, ekonomskoj, društveno-civilnoj i končano, u vojnoj sferi. Posledica toga je da organizaciona struktura asimetričnih učesnika u sukobu četvrte generacije ne teži svom širenju i učvršćivanju, već nestalnosti i elastičnosti. Ta struktura je po obliku mrežna, a po trajanju nestalna.

U ratovanju četvrte generacije smanjuje se vertikalna organizaciona (vojna) disciplina, formalna struktura organizacije i značaj direktnog vojnog nadmetanja oružanom silom. Istovremeno, stiče se fleksibilnost strukture i ponašanja, prikrivenost identiteta, postojanost i strpljivost protivnika, kao i mala veličina organizacionih elemenata struktura u sukobu. Naor, istraživač sa Univerziteta u Tel Avivu, navodi da čak i mala verovatnoća efikasnosti terorističkih akcija stvara veliki makroekonomski uticaj na društvo.[480] Po njemu, vlade država i stanovništvo koje je zahvaćeno asimetričnim terorističkim delovanjem pokazuju tendenciju da precenjuju realnu opasnost od terorističkog napada (verovatnoću od vlastite pogibije ili ranjavanja zbog napada) i da potcenjuju ishode sa realno velikom verovatnoćom (propast nacionalne i regionalne ekonomije, načina života, dugoročne posledice vanrednog stanja i slične).[481] Primarni cilj terorizma je simboličan, jer se njegovim dejstvima žele postići efekti čiji uticaj na ciljano društvo je značajno veći nego direktni efekti samog napada. Po Ekštajnu i Cidonu, takav uticaj je značajan, jer teroristi imaju cilj da ostvare povećanje straha u ciljanom društvu, a ne da ostvare što veći broj žrtava i što veću materijalnu štetu.[482] Sa povećanjem straha dolazi do posrednih posledica dugoročnog smanjivanja nacionalnog dohotka, investicija, potrošnje i konačno, sposobnosti za očuvanje bezbednosti i odbranu.[483] Strah je glavno sredstvo terorizma, a

[480] Ziv Naor, "Why a Small Probability of Terror Generates a Large Macroeconomic Impact," *Defence And Peace Economics* 26, no. 6 (December 2015): 583-599.

[481] Naor, "Small Probability of Terror," 598.

[482] Zvi Eckstein and Daniel Tsiddon. "Macroeconomic Consequences of Terror: Theory and the Case of Israel." *Journal Of Monetary Economics* 51, no. 5 (July 2004): 971-1002.

[483] Eckstein and Tsiddon. "Macroeconomic Consequences of Terror".

svaki instrument koji ga izaziva može biti upotrebljen. Efekat straha je značajan, posebno kada deluje u širokoj zajednici. Na primer, čak i lažni teroristički napadi[484] u kombinaciji sa stvarnim napadima mogu dugoročno dovesti do vrlo ozbiljnih posledica po stanje nacionalnog morala, volje za borbom i ekonomije.[485]

Po Lindu, pošto sve može biti upotrebljeno kao instrument dejstva, jedini način da se efikasno odgovori na strukturu protivnika u sukobu četvrte generacije je izgradnja adekvatnih snaga i sprečavanju protivnika da izgradi sopstvene snage. Dakle, borba nije u nadmetanju dejstava, već u nadmetanju u izgradnji borbene strukture. Teži se da sopstvene snage budu lakše, operativnije i brže. Tehnologija u tome igra ključnu ulogu. Upotreba novih oblika naoružanja, poput usmerene energije, robotizovanih borbenih sistema, bespilotnih letelica, bezbednih informacionih komunikacija i sistema veštačke inteligencije je očekivana. Cilj je izgraditi male, brze i inteligentne jedinice opremljene savremenom tehnologijom koja vojnim jedinicama omogućuje sposobnosti koje nema protivnik.[486] Pored navedenog, u sukobu četvrte generacije učesnici nisu samo naoružani vojnici protivnika, jasno obeleženi uniformama, već su i civili. Već na prvi pogled jasno je da se napadi u sajber prostoru mogu lako primeniti za vođenje sukoba četvrte generacije.

6.2. Tehnološki i društveni uzroci sajber sukoba i ratovanja

Hegre, Gisinger i Glidič su u istraživanju pod nazivom „Globalizacija i unutrašnji konflikti“ pokazali da je ekonomska otvorenost neke nacije povezana sa njenim ekonomskim rastom i stabilnošću političkog sistema, kao i da je ekonomska nejednakost unutar nacije snažno povezana sa nasilnim kriminalom, ali ne i sa izbijanjem unutrašnjih

[484] Anonimne informacije o postavljenim bombama u tržnim centrima, sudovima, vladinim institucijama, aerodromima, lažno podmetanje eksplozivnih naprava na prometnim i značajnim mestima, poput mostova, turističkih mesta, železničkih stanica i slične aktivnosti.

[485] John Robb, „How Fast, Frequent and FAKE Terrorism Could Sink the EU“, *Global Guerrillas Weblog*, 22 Marcht 2016, http://globalguerrillas.typepad.com/globalguerrillas/2016/03/index.html (preuzeto 25. marta 2016).

[486] Lind, Nightengale, Schmitt, Sutton, Wilson, "Changing Face of War", 25.

sukoba.[487] Takođe, navedena studija je pokazala i da postoji veća verovatnoća za izbijanje unutrašnjeg sukoba u nekoj državi u uslovima siromaštva i političke nestabilnosti.[488]

Tehnologija utiče na sukobe koje društvene grupe vode između sebe, ali taj uticaj nije linearan. Sama tehnologija ne utiče primarno na verovatnoću izbijanja sukoba, već na način kako se sukobi vode. Istovremeno, raspolaganje određenom tehnologijom utiče na društvene grupe da u skladu sa tom sposobnošću razvijaju i usmeravaju vlastite društvene ciljeve, uključujući i one, koji se odnose na agresivno ponašanje u širem okruženju. Dakle, osnov za vođenje sajber sukoba na nacionalnom nivou ne leži isključivo u tehnologiji, već u kombinaciji šireg skupa društvenih faktora. Zbog toga, pri analizi uzroka učestalosti sukoba u nekom regionu nije dovoljno uzeti u obzir samo tehnološki faktor, već je potrebno sagledati širi kontekst savremenog globalnog okruženja. Navedeno znači da u konkretnom slučaju istraživanja primene informaciono-komunikacionih tehnologija u cilju vođenja sukoba, faktori poput razvoja tehnologija, postojećih društvenih protivrečnosti i sukoba, političkih interesa grupa i njihove međusobne borbe za resursima, načina ispoljavanja društvenih ciljeva, kao i drugi, ne stoje u prostom, već u složenom odnosu.

Analizom vodeće akademsko-istraživačke baze podataka oružanih sukoba u svetu, *The Uppsala Conflict Data Program* (UCDP)[489]/ *Centre for the Study of Civil War* na *International Peace Research Institute*[490] iz Švedske, može se uočiti trend prirode sukoba u periodu moderne istorije nakon Drugog svetskog rata do danas. Po njemu se značajno povećava broj unutrašnjih i internacionalizovanih sukoba u odnosu na ukupan broj sukoba u svetu, kao i broj sukoba između više strana u odnosu broj sukoba između dve sukobljene strane.[491] Takođe, iako još uvek u svetu postoje države sa autoritarnim vladama, njihov

[487] Havard Hegre, Ranveig Gissinger, and Nils Petter Gleditsch. "Globalization and Internal Conflict," in *Globalization and Conflict,* eds. Gerald Schneider, Katherine Barbieri and Nils Petter Gleditsch (Boulder, CO: Rowman and Littlefield, 2003): 251-75.

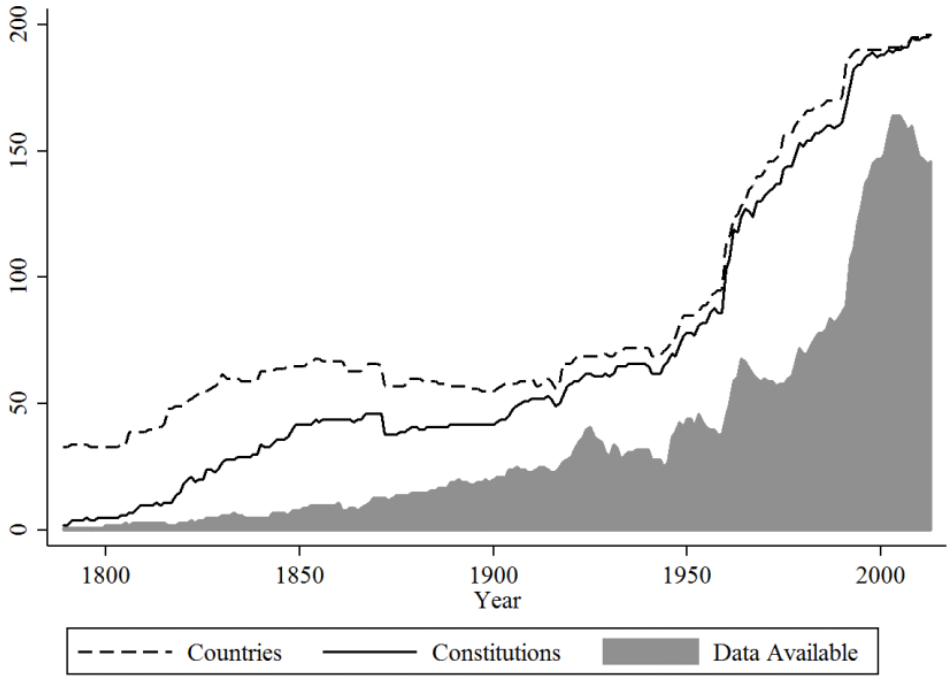
[488] Ibid.

[489] Uppsala Universitet, Department of Peace and Conflict Research, UCDP Datasets, http://www.pcr.uu.se/research/ucdp/datasets/ i http://www.ucdp.uu.se/ged/ (preuzeto 3. avgusta 2015).

[490] The International Peace Research Institute Sweden, Centre for the Study of Civil War, CSCW Annual Reports https://www.prio.org/Programmes/Extensions/Centre-for-the-Study-of-Civil-War/Annual-Reports/?xitem=4&handler=Programme (preuzeto 3. avgusta 2015).

[491] Therése Pettersson and Peter Wallensteen, „Armed Conflicts, 1946-2014," *Journal of Peace Research* 52, no. 4, (2015).

broj se vremenom smanjuje. Istovremeno, povećava se broj nezavisnih država i gotovo sve one imaju ustavno uređenje (Slika 15). Povećava se i broj država koje su pristupile osnovnim međunarodnim sporazumima u oblasti regulisanja oružanih sukoba i ratifikovale ih delom ili u celini. Za potrebe utvrđivanja uzroka i trendova primene sukoba u sajber prostoru potrebno je odgovoriti na pitanja: koji je ključni uzrok izbijanja povećanog broja unutrašnjih ratova u svetu i da li se može utvrditi veza između ovih ratova i rastuće primene informaciono-komunikacionih tehnologija u svetu?



Slika 15. Trend povećavanja broja država u međunarodnoj zajednici[492]
Comparative Constitutions Project, Chronology of Constitutional Events, Version 1.2,

Države koje svrsishodno i organizovano razvijaju vojne, bezbednosne i obrazovno-istraživačke kapacitete i sposobnosti za vođenje sukoba u sajber prostoru, ulažu velike

[492] Comparative Constitutions Project, Chronology of Constitutional Events, Version 1.2, http://comparativeconstitutionsproject.org/download-data/ (preuzeto 2. januara 2016).

finansijske resurse u tu svrhu[493, 494, 495, 496, 497]. One tako pokazuju spremnost da ostvarene sposobnosti za vođenje sukoba u sajber prostoru primene u praksi. U većini slučajeva, reč je o vodećim vojnim, političkim i ekonomskim silama u svetu, čiji su nacionalni interesi široki i odnose se na globalno okruženje. Shodno tome, primena vojnih i obaveštajnih aktivnosti u sajber prostoru je česta i odnosi se podjednako na situacije u stanju mira i rata. Po resursima i kapacitetima manji akteri na međunarodnoj sceni, koji ne raspolažu sa velikim resursima, uključujući države, kao i vojne, političke ili terorističke organizacije, su prinuđeni da koriste asimetrične metode i sredstva u sukobu sa većim silama, u vreme rata ili mira. S obzirom da su u inferiornom položaju, oni nastoje da razvijaju i primenjuju jeftinije, ali efikasne metode, tehnike i sredstva za protivdejstva i nanošenje udara po jačem protivniku. Kako navedena tendencija utiče na izbijanje sukoba u sajber prostoru može se analizirati na primeru nerazvijenih regiona „Trećeg sveta".

6.2.1. Primer nerazvijenih država i sajber prostora

Od koristi za dalju analizu može biti praćenje trenda sukoba u svetu u periodu nastanka i razvoja sajber prostora. Po bazi podataka Istraživačkog instituta za mir (*Peace Research Institute Oslo* – PRIO), nakon Drugog svetskog rata najveći broj sukoba u svetu, uz

[493] The White House, Office of the Press Secretary, „Fact Sheet: Cybersecurity National Action Plan," saopštenje za štampu, February 09, 2016, https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan (preuzeto 20. februara 2016).

[494] Government Communications Headquarters (GCHQ), „Chancellor's speech to GCHQ on cyber security," javno saopštenje, November 17, 2015, https://www.gov.uk/government/speeches/chancellors-speech-to-gchq-on-cyber-security (preuzeto 20. februara 2016).

[495]"France to invest 1 billion euros to update cyber defences," *Reuters*, 7 February 2014, http://www.reuters.com/article/france-cyberdefence-idUSL5N0LC21G20140207 (preuzeto 20. februara 2016).

[496] Eugene Gerden, „$500 Million for New Russian Cyber Army," *SC Magazine*, November 6, 2014, http://www.scmagazineuk.com/500-million-for-new-russian-cyber-army/article/381720/ (preuzeto 20. februara 2016); Greg Austin, „Russia's Cyber Power," New Europe, October 26, 2014, http://neurope.eu/article/russia%E2%80%99s-cyber-power/ (preuzeto 20. februara 2016).

[497] Global Times, Dong Zhaohui, ed, „China Upgrades Missile Force, Adds Space and Cyber War Forces," CHina Military News, January 1, 2016, http://english.chinamil.com.cn/news-channels/china-military-news/2016-01/01/content_6840089.htm (preuzeto 20. februara 2016).

„China Military Seeks to Bring Cyber Warfare Units Under One Roof," Bloomberg, October 23, 2015, http://www.bloomberg.com/news/articles/2015-10-22/china-military-chiefs-seek-to-unify-cyber-warfare-operations (preuzeto 20. februara 2016).

najveći broj žrtava, odvijao se u Podsaharskoj Africi i Jugoistočnoj Aziji.[498] Nakon dugog perioda života pod kolonijalnom vlašću raznih evropskih sila, proces sticanja nezavisnosti država navedenih regiona je završen do kraja šezdesetih godina 20. veka. Međutim, posledice dugotrajnog zaostajanja u razvoju zbog kolonijalizma su ostale. Čak i danas, *Indeks ljudskog razvoja* (*Human Development Index* – HDI)[499] i *Globalni indeks inventivnosti* (*Global Innovation Index* - GII) [500] država podsaharske Afrike i jugoistočne Azije su najnepovoljniji u svetu. Međutim, uprkos nepostojanju razvijene društvene i privredne infrastrukture, navedeni regioni prednjače po brzini prihvatanja, upotrebe i širenja Interneta i informaciono-komunikacionih tehnologija u svetu. U periodu od 2000. do 2015. godine, upotreba Interneta na Afričkom kontinentu, koji gotovo da i nema razvijenu informacionu i industrijsku infrastrukturu prethodne generacije, porasla je za čak 7.231 %[501].

Razloga za takav rast prihvatanja informaciono-komunikacionih tehnologija ima više. Usled prekida kontinuiteta u industrijskom i društvenom razvoju za vreme kolonijalizma, prethodne tehnologije nisu nikada razvijene u navedenim regionima, pa ne postoji odgovarajuća izgrađena infrastruktura. Drugi razlog je ekonomske prirode. Odnosi se na mogućnost lake izgradnje neophodne infrastrukture i na niske troškova uvođenja potrebnih tehnologija. Najveći broj informaciono-komunikacionih tehnologija u širokoj primeni u svetu je dostigao zreli nivo razvoja, što podrazumeva visoku efektivnost i efikasnost uz nisku cenu. Na primer, fiksna bežična mreža mobilne telefonije se na širokom području može ostvariti brže i jeftinije od tradicionalne žičano-kablovske komunikacione infrastrukture na kopnu. Pri tome je infrastruktura bežične mreže

[498] Peace Research Institute Oslo (PRIO), *ACLED - Armed Conflict Location and Event Data*, https://www.prio.org/Data/Armed-Conflict/Armed-Conflict-Location-and-Event-Data/ (preuzeto 21. februara 2016).

[499] Statistička zbirna mera indikatora za procenu nivoa razvoja država, koja se sastoji od indikatora o očekivanoj dužini života, obrazovanja i prihoda po glavi stanovnika, koju svake godine objavljuje Razvojni program Ujedinjenih nacija (*United Nations Development Programem* - UNDP). United Nations Development Programme, *Human Development Report 2015*, http://report.hdr.undp.org/ (preuzeto 21. februara 2016).

[500] The Global Innovation Index, *2015 Country Rankings*, https://www.globalinnovationindex.org/content/page/data-analysis/ (preuzeto 21. februara 2016). U izveštaju iz 2015 godine, region podsaharske Afrike je pretekao države Centralne i Južne Azije.

[501] Internet World Stats, *Internet Usage Statistics, The Internet Big Picture, World Internet Users and 2015 Population Statistics*, http://www.internetworldstats.com/stats.htm (preuzeto 17. januara 2016).

autonomija, jer ne zahteva čak ni razvođenje električne energije, pošto bazne stanice mobilne telefonije mogu koristiti generatore za samonapajanje.

Ipak, preskakanje tehnologija ne znači nužno i brz napredak. U razvijenim društvima, organizacije koje prve prelaze na napredne tehnologije, stiču konkurentniju poziciju u odnosu na one koje se zadržavaju na tradicionalnim tehnologijama i čiji značaj u budućnosti opada. U navedenom primeru država afričkog i dela azijskog kontinenta radi se o drastičnom slučaju sa drugačijim uzrokom. U navedenim regionima, nacije kreiraju potpuno novu tehnološku eru, jer prethodne tehnološke generacije gotovo i da nisu postojale. U njihovom slučaju, tehnološki napredak je uslovljen potrebom i predstavlja jedini način razvoja. Sva snaga daljeg razvoja novih tehnologija usmerava su u jednom pravcu, jer nema gde drugde. Proces preskakanja tehnologija u nerazvijenim ekonomijama je uslovljen nužnošću i zasniva se na tehnološkoj supstituciji onih infrastruktura koje su nedostajale u prošlosti. Taj proces je posledica situacione reakcije na odsustvo tradicionalne infrastrukture i dostupnost jeftinih tradicionalnih tehnologija, a ne sistematičnog strategijskog planiranja, kao, na primer, u slučaju razvijenih država Azije, koje su u prošlosti ostvarile veliki proboj u razvoju informaciono-komunikacionih tehnologija, poput Kine, Tajvana, Japana ili Južne Koreje.[502] U pojedinim nerazvijenim državama, taj proces ubrzavaju i same vlade navedenih regiona. Karakteristični projekti u pogledu razvoja sajber prostora su širenje bežičnog Interneta primenom stratosferskih balona (projekat *Google Loon* u saradnji sa vladom Šri Lanke) [503] i projekat *One Laptop per Child,* [504, 505] pokrenut na Masačusetskom tehnološkom institutu (*Massachusetts Institute of Technology* – MIT).

[502] The Reut Institute, *Israel 15 Vision: Principles and Guidelines for Achieving a Socioeconomic Leapfrog, Version B* (2009), http://www.reut-institute.org/data/uploads/Articles%20and%20Reports%20from%20other%20organizations/20090913%20-%20ISRAEL%2015%20Version%20B.pdf (preuzeto 12. septembra 2015).

[503] Početkom 2016. godine, kompanija Google je osnovala zajedničku kompaniju sa Vladom Sri Lanke koja će tehnologijom primene balona u stratosferi omogućiti pristup bežičnom 3G Internetu kapaciteta 1-15 Mbps na celoj površini ostrva. Sri Lanka Broadcasting Corporation, „Google Loon Project to Cover Sri Lanka with 3G Internet“, http://www.slbc.lk/index.php/tamil-news-update/1361-google-loon-project-to-cover-sri-lanka-with-3g-internet.html (preuzeto 17. februara 2016);

The Guardian, „Project Loon: Google Baloon that Beams Down Internet Reach Sri Lanka,“ 16 February 2016, http://www.theguardian.com/technology/2016/feb/16/project-loon-google-balloon-that-beams-down-internet-reaches-sri-lanka (preuzeto 17. februara 2016).

[504] One Laptop Per Child, http://one.laptop.org/.

[505] Nicholas Negroponte, http://one.laptop.org/about/people/negroponte.

Nezavisno od prihvatanja novih informaciono-komunikacionih tehnologija, navedeni regioni su ujedno i vodeći svetski regioni po izbijanju broja sukoba u svetu, a razlozi za to su različiti i složeni. Oni se odnose prvenstveno na negativno kulturno nasleđe, ekonomsku i društvenu nerazvijenost, istorijsku društvenu netrpeljivost, sukob interesa različitih društvenih zajednica (plemenskih, religijskih ili nacionalnih), i posebno na smanjivanje dostupnih resursa za život, koje je posledica brzog povećanja populacije.

Države Podsaharske Afrike i Jugoistočne Azije imaju najveću stopu rasta populacije u svetu.[506] Ona dovodi do neravnomerne distribucije resursa i borbe za njih. Kao posledica globalizacije i tehnološkog razvoja, neautomatizovana poljoprivredna i zanatska proizvodnja postaju nerentabilne, što uz proces ukrupnjavanja velikih obradivih površina na koji utiče strani kapital, dovodi do situacije u kojoj ruralno stanovništvo masovno migrira u velike gradove. U nerazvijenim sredinama, ta urbanizacija je najbrža u regionima u kojima postoji veći nivo siromaštva. Podsaharska Afrika je i u tome lider u svetu. Glavni grad Demokratske Republike Kongo, Kinšasa se nalazi u stanju brzog rasta od grada sa 200.000 stanovnika u 1950. godini do projektovanog broja od 20.000.000 stanovnika u 2030 godini, što predstavlja rast od 100 puta.[507] Po projektovanom očekivanju, glavni grad Nigerije, Lagos će u skoroj budućnosti imati čak 23 miliona stanovnika, a pored njega će u Podsaharskoj Africi postojati još čak pet mega gradova.[508]

Iako navedeni regioni prednjače u broju međunarodnih i internih sukoba, i istovremeno imaju visoku stopu uvođenja informaciono-komunikacionih tehnologija u njihova društva, u njihovom slučaju nema poznatih primera sukoba u sajber prostoru na međunarodnom nivou. U navedenim regionima postoji relativno razvijena upotreba sajber prostora u svrhu izvođenja kriminalnih ili medijsko propagandnih ciljeva, ali na ekstenzivnom i tehnološki nezahtevnom nivou. Ti slučajevi kriminala su razvijeni na prilično niskom nivou znanja. Na primer, na ponekad banalnom socijalnom inženjeringu („Nigerijska prevara“) ili na političkom agitovanju u sajber prostoru koji je usko usmeren

[506] United Nations, *Department of Economics and Social Affairs, Population Division, World Populati prospects the 2015 Revision*, http://esa.un.org/unpd/wpp/Graphs/Probabilistic/POP/TOT/ (preuzeto 12. septembra 2015).

[507] „Bright Lights, Big Cities,“ *The Economist*, February 4, 2015, http://www.economist.com/node/21642053 (preuzeto 15. septembra 2015).

[508] United Nations, *Economic and Social Affairs, World Urbanization Prospects, 2014 Revision*, http://esa.un.org/unpd/wup/Publications/Files/WUP2014-Report.pdf (preuzeto 15. septembra 2015).

na određenu populaciju ili zajednicu (u slučaju propagande Tamilskih tigrova na Internetu u Šri Lanki). Međutim, ne postoji utvrđena situacija organizovane i sistematične primene sukoba u sajber prostoru između nacija navedenih regiona, uprkos velikom broju sukoba.

Navedeni primer potvrđuje stav da za primenu napada u sajber prostoru moraju postojati tri ključna uzroka, kojih nema u posmatranim regionima:

- dovoljno visok nivo razvijenih sistematičnih **znanja i veština** neophodnih za planiranje, pripremu i izvođenje sajber napada;
- potreban nivo **organizovanog pristupa** državnih struktura u cilju primene operacija i dejstava u sajber prostoru, i
- **tehnološka zavisnost napadnute strane** od informaciono-komunikacionih tehnologija podložnih sajber napadima.

Dakle, u skladu sa prethodnim primerom, tehnologija sama po sebi ne donosi nove vrste sukoba. Za njihovo izbijanje neophodni su društveni i političku uslovi koji univerzalno dovode do sukoba. Jednostavno prihvatanje novih tehnologija u cilju preskakanja tehnoloških generacija ne može biti zamena za održiv razvoj društva. Nužan uslov za održiv razvoj društva je uspostavljanje neophodnog nivoa znanja i društvene organizacije. Takođe, prosto prihvatanje tehnologije ne izaziva nastajanje novih formi sukoba. Ono što izazva sukobe su unutrašnji i spoljni sukobi interesa između nosilaca društvene moći. Tehnologija je sredstvo, odnosno skup instrumenata kojim nosioci moći ostvaruju svoju nameru. Da bi ljudi koristili borbene tehničke sisteme za sukobe, moraju da vladaju njihovom tehnologijom. Takođe, ta tehnologija mora biti primenjiva u konkretnom slučaju sukoba. To je opšti slučaj koji važi za sve vrste sukoba, uključujući i primenu sukoba u sajber prostoru.

Vođenje sukoba u sajber prostoru se zasniva na postojanju društvenih protivrečnosti (u društvenom kontekstu) i na mogućnosti primene informaciono-komunikacionih tehnologija (u tehnološkom kontekstu). Sama brzina razvoja informaciono-komunikacionih tehnologija ne omogućava konstantnu primenu razvijenih tehničkih informacionih sistema u svrhu sukoba, kao što je to slučaj sa mehaničko-elektronskim borbenim sistemima. Suštinski značaj u toku sajber sukoba ima znanje (i organizovano upravljanje informacijama), a ne tehnički sistemi koji su razvijeni na osnovu tog znanja.

6.3. Pojam sajber ratovanja

Pojam sajber ratovanja je jasan, međutim u vezi njegove praktične primene postoji dosta nedoumica. Sajber ratovanje je ratovanje u sajber prostoru. Kao i svako ratovanje, ono predstavlja organizovani sukob između međunarodnopravnih subjekata. Pošto se sajber ratovanje ne vodi konvencionalnim oružjem koje ostvaruje svoje dejstvo u fizičkom okruženju, potrebno je utvrditi druge kriterijume za njegovo određenje. Najčešći kriterijum koji većina država i akademika prihvata jeste kriterijum efekata i nastojanja (pokušaja, aktivne namere) izazvanja efekata kojim se izvršava pretnja primenom i primena sile[509], odnosno agresija na neku država. Međutim, oko toga šta predstavlja primena sile u međunarodnim odnosima ima dosta nedoumica i neslaganja u mišljenjima. Kada se te nedoumice prenesu u područje sajber prostora, koji je izgrađen funkcionisanjem informaciono-komunikacionih tehnologija i isprepletan stanjima, procesima i odnosima, koji se manifestuju u sajber prostoru, uz druge probleme koji dolaze sa primenom ovih tehnologija, a koji potiču od njihove prirode i kompleksnosti njihove primene (kao što je mogućnost uspostavljanje anonimnih i prikrivenih aktivnosti u sajber prostoru), dolazi se do situacije u kojoj je teško čak i utvrditi postojanje primene sile, a kamo li njene efekte.

Pored pravnog poimanja, sajber ratovanje se može definisati i u vojnom pogledu. Po *Nacionalnom strategijskom okviru za bezbednost u sajber prostoru* Vlade Italije, u vojnom pogledu, sajber ratovanje predstavlja: „aktivnosti i operacije preduzete u sajber području sa ciljem ostvarivanja operativne prednosti od vojnog značaja“[510]. Po stavu vlade Južne Afrike, centralna aktivnost sajber ratovanja je preduzimanje ofanzivnih sajber operacija[511].

Prethodno navedene definicije jasno pokazuju ključne karakteristike sajber ratovanja: ono predstavlja vojnu aktivnost usmerenu ka ostvarivanju ciljeva od vojnog značaja, primenom težišno ofanzivnih aktivnosti (jer su svi sajber napadi zasnovani na

[509] Povelja UN, član 4 poziva sve članice UN da se uzdrže od pretnje silom ili primene sile protiv teritorijalnog integriteta, političke nezavisnosti ili na drugi način u suprotnosti sa Poveljom.

[510] Government of Italy, Presidency of the Council of Ministers, „National Strategic Framework for Cyberspace Security“, 2013, 13, https://www.ccdcoe.org/strategies-policies.html

[511] South Africa, Department of Defence Republic of South Africa, South African Defence Review, 2012, 79, http://www.sadefencereview2012.org/publications/publications.htm

iskorišćavanju ranjivosti u protivničkim sistemima). Imajući u vidu da se stanje (međunarodnog) ratovanja odnosi isključivo na aktere koji imaju međunarodnopravni subjektivitet (rat se izvodi između međunarodnih subjekata, pri čemu je najmanje jedna strana u sukobu država), od značaja za određivanje pojma „sajber ratovanje“ je i taj uslov, da su sajber napadi pokrenuti od strane nekog državnog organa. Institut *EastWest* definiše sajber ratovanje kao: „sajber napade autorizovane od strane državnog učesnika pokrenute protiv sajber infrastrukture istovremeno sa (odgovarajućom) vladinom kampanjom“[512]. Naravno postavlja se pitanje, da li sajber napadi mogu biti preduzeti, samostalno, van šire akcije vojnih snaga neke države, van ratnog sukoba, u stanju mira, sa ili bez angažovanja regularnih naoružanih vojnih snaga (boraca), bez primene tradicionalnog oružja čije se dejstvo manifestuje u fizičkom okruženju? Odgovor je potvrdan, i štaviše, predstavlja najverovatniji oblik primene sile u sajber prostoru između država. Imajući navedeno u vidu, sajber ratovanje predstavlja ratovanje koje je izvedeno u sajber prostoru. Ono ima sve karakteristike tradicionalnog ratovanja, ali i neke dodatne, jer je tehnološki zavisno od primene informaciono-komunikacionih tehnologija, koje omogućavaju dejstvo koje je anonimno i prikriveno, i drugačije zavisi od vremena i prostora. Ono je zasnovano na primeni specifičnog znanja, a ne nužno na posedovanju sistema naoružanja za dejstva u sajber prostoru. To znači da je sa vođenje sajber ratovanja osposobljen onaj akter koji poseduje znanje o načinu narušavanja informacione bezbednosti informacionih sistema i informacija protivnika, a ne onaj ko je nabavio sisteme koji su namenjeni za automatizovana upućivanje ograničenog skupa sajber napada.

Iako se odvija u sajber okruženju, u pogledu mogućeg vojnog doprinosa, sajber ratovanje je vrlo realno. O tome svedoči uspostavljanje strategijskih komandi za izvođenje sajber operacija u Vojsci SAD i Narodnooslobodilačkoj armiji Kine, operativno-strategijskih i taktičkih vojnih i obaveštajnih struktura u brojnim armijama sveta. NATO je na samitu u Velsu 2014 godine doneo odluku da će „sajber napad voditi ka primeni člana 5 u skladu sa odlukom Severnoatlantskog veća na osnovu individualne procene slučajeva“[513]

[512] EastWest Institute, *Critical Terminology Foundations 2*, 43.

[513] North Atlantic Treaty OrganizationNATO, Wales Summit Declaration [Press release 120, September 5, 2014], http://www.nato.int/cps/en/natohq/official_texts_112964.htm (preuzeto 22. decembra 2015).

Ključne karakteristike sajber ratovanja su:

- ono predstavlja namernu i organizovanu aktivnost primene sile prema protivniku u cilju nanošenja štete njegovim resursima, vrednostima, stanju i interesima;
- ostvaruje se u sajber prostoru i iz sajber prostora, što znači primenom informacionih sistema i informacija u njima i dejstvom na informacione sisteme i informacije u njima;
- preduzima se od strane države ili organa u ime države;
- izvodi se u cilju ostvarivanja vojnih i političkih ciljeva;
- primena sile u sajber prostoru treba biti ekvivalentna po efektima, intenzitetu; međutim ona ne mora biti ekvivalentna po trajanju, s obzirom da dejstvo napada može biti neograničeno dugo odloženo, trenutno, usmereno ili najšire distribuirano, a pored toga, može imati i naknadne, odnosno kaskadne efekte;
- sajber napad kao deo sajber ratovanja može biti deo šire vojne operacije, ali ne mora uopšte biti preduzet od strane vojnih snaga, već i od strane plaćenih grupa, privatnih kompanija, hakerskih, pa čak i kriminalnih grupa i pojedinaca u ime i po nalogu državnih organa;
- sajber ratovanje se odvija u sajber prostoru i time utiče na sva tri sloja sajber prostora (fizički, logički i kognitivni), ali je za njega ključno da se ostvaruje narušavanjem informacione bezbednosti protivničkog sistema.
- dejstva u sajber ratovanju imaju direktne i indirektne ciljeve[514]; direktni ciljevi se odnose na narušavanje informacione bezbednosti napadnutog sistema i informacija u njemu; indirektni ciljevi se ostvaruju prenošenjem dejstva između slojeva sajber prostora (logičkog, fizičkog i kognitivnog) i mogu biti sva lica, sistemi, vrednosti, procesi, informacije i samo okruženje u fizičkom, logičkom i kognitivnom sloju, odnosno u fizičkom i informacionom okruženju).

[514] Dragan Mladenovic, Danko Jovanović, Mirjana Drakulić „Definisanje sajber ratovanja“, *Vojnotehnički glasnik,* 60, no. 2 (2012): 84-117.

7. SAJBER NAPADI

Da bi se utvrdila priroda sajber sukoba i mogućnost njegove međunarodnopravne regulacije, neophodno je utvrditi koji su ključni elementi svakog oružanog sukoba, koji postoje i u sajber sukobu, a od značaja su za njegovo svrstavanje u kategoriju primene Međunarodnog prava oružanih sukoba.

Dakle, u pogledu svakog sukoba, tradicionalnog ili sajber, treba razlikovati sledeće elemente sukoba:

- učesnike (strane u sukobu i neutralne strane)
- sredstva (oružje),
- metode (način preduzimanja napada, vojnu organizaciju vođenja sukoba) i
- uzroke i ciljeve sukoba (razloge zbog kojih je sukob pokrenut i ciljeve koje treba da ostvari).[515]

U tehničkom pogledu, od ključnog značaja su sledeće kategorije od značaja:

- sajber oružje
- sajber napad
- sajber agresija

U skladu sa dosadanjom analizom, sajber napad načelno predstavlja akt agresije unutar sajber prostora ili kroz sajber prostor na informacioni sistem drugog entiteta. On je oblik vojnog dejstva ekvivalentan primeni oružane sile, pa se može preduzimati i u ofanzivnom i u defanzivnom smislu. Sajber napadi su vezani za narušavanje informacione bezbednosti. Sajber prostor je elektronsko okruženje u kome se primenom informaciono-komunikacionih tehnologija i elektromagnetnog spektra kreiraju, čuvaju, razmenjuju, obrađuju i uništavaju podaci i informacije. Ključni sadržaj sajber prostora su informacije u elektronskom obliku, a faktor koji ga omogućava jesu informaciono-komunikacione tehnologije. U svakom slučaju, sajber napad je napad i stoga je potrebno analizirati šta oba pojma znače u kontekstu primene informaciono-komunikacionih tehnologija u sajber

[515] Mladenovic, „International Legal Regulation.“

prostoru, u smislu informacione i sajber bezbednosti, i u smislu vojno-političke i međunarodnopravne primene.

Iako postoje greške u softveru i nedostaci u dizajnu, u implementaciji i upotrebi informacionih sistema na svim nivoima sajber prostora, postavlja se pitanje kako napadači uspevaju da ih iskoriste i zloupotrebe za izvođenje sajber napada, ukoliko im svi ti sistemi nisu uvek dostupni?

Savremeni vojni borbeni sistemi su izolovani sistemi u pogledu informacione bezbednosti. Međutim, zbog unapređenja njihove funkcionalnosti postoji potreba direktnog, indirektnog ili kontrolisanog umrežavanja sa brojnim telekomunikacionim sistemima za podršku u vidu geolokacijskih servisa, komandne komunikacije, upravljanja vatrom, praćenja ciljeva, identifikacije protivnika i sopstvenih snaga, pa čak i radi jednostavne sinhronizacije sistemskog vremena, datuma i vremenske zone[516][517]. U svim vojnim, kao i eksterno umreženim sistemima postoje softverske, hardverske i organizacione greške koje omogućavaju dejstvo napadača, čak i kada je to ne izgleda očigledno. Neautorizovan pristup sistemima se može ostvariti na različite načine, poput radio-ometanja, infiltriranjem u sisteme za podršku i komunikacione veze, detektovanjem i analizom elektromagnetnog zračenja, zvučnih i infracrvenih (toplotnih) talasa oko delova sistema i druge.

Mere kojima se uspostavlja bezbednost sistema je moguće zaobići prethodnim infiltriranjem zlonamernog softvera i hardvera u sisteme, uticajem na sadržaj kriptografskih proizvoda, ili uz pomoć insajdera (kao u slučaju operacije Staksnet u Iranu). U nekim armijama su u upotrebi specijalni elektronski sistemi čija primena predstavlja kombinaciju elektromagnetnog i sajber ratovanja, koji su dizajnirani za ometanje u elektromagnetnom spektru i injektovanje logičkih instrukcija ili softverskog koda u sisteme za detekciju, identifikaciju i komunikaciju (poput savremenih radarskih

[516] Brandon Hill, „Lockheed's F-22 Raptor Gets Zapped by International Date Line," *Daily Tech*, February 26, 2007, http://www.dailytech.com/Lockheeds+F22+Raptor+Gets+Zapped+by+International+Date+Line/article6225.htm (preuzeto 12. aprila 2015).

[517] „F-22 Squadron Shot Down by the International Date Line," *Defense Industry Daily*, March 1, 2007, http://www.defenseindustrydaily.com/f22-squadron-shot-down-by-the-international-date-line-03087/ (preuzeto 12. aprila 2015).

sistema). Primeri tih sistema su *Suter*[518] i *CHAMP* (engl. *Counter-electronics High-powered Microwave Advanced Missile Project*)[519]. Sve ove metode se mogu kombinovati sa sajber napadima iz razloga što su savremeni tokovi komunikacija u sistemima i između njih digitalne prirode, kao i transmisija podataka koja je zasnovana na protokolima koji se koriste na Internetu.

Čak i kada nema mnogo uslova za ostvarivanje povezanosti između delova izolovanih sistema, uvek treba imati u vidu vremensku dimenziju. Na primer, jedan izraelski istraživač je 2015. godine u svim operativnim sistemima kompanije *Microsoft*, od *WindowsXP* do *Windows 10*, otkrio postojanje dela softvera koji u prethodnih 15 godina nije imao nikakvu funkciju, a bio je stalno prisutan u sistemima, kao njihov atavistički deo[520]. Navedeno otkriće pokazuje da se sajber napad može planirati i dizajnirati godinama unapred, pre započinjanja sukoba ili poznavanja protivnika.

Radi određivanja pojma i karakteristika sajber napada mora se poći od 2 ključne činjenice:

- postoje različiti aspekti definisanja ovog fenomena (npr. Tehničko, vojno, političko-bezbednosno, pravno i sl.);
- priroda sajber napada je složena i višeslojna i zavisi od mnoštva faktora.

7.1. Definicije sajber napada

Sajber napad načelno predstavlja akte agresije unutar sajber prostora ili kroz sajber prostor na informacioni sistem drugog entiteta. On je oblik vojnog dejstva ekvivalentan primeni oružane sile, pa se može preduzimati i u ofanzivnom i u defenzivnom smislu. Sajber napadi su vezani za sajber prostor. Ključni sadržaj sajber prostora su podaci i informacije u elektronskom obliku, a faktor koji ga omogućava jesu informaciono-komunikacione tehnologije. U svakom slučaju, sajber napad je napad i stoga je potrebno

[518] „Jam. Bomb. Hack? New U.S. Cyber Capabilities and the Suppression of Enemy Air Defenses," *Georgetown Security Studies Review*, April 07, 2014, http://georgetownsecuritystudiesreview.org/2014/04/07/jam-bomb-hack-new-u-s-cyber-capabilities-and-the-suppression-of-enemy-air-defenses/, (preuzeto 23. marta 2015).

[519] James Drew, „USAF Nominates JASSM Missile to Host New Computer-killing Weapon," *Fight Global*, May 14, 2015, https://www.flightglobal.com/news/articles/usaf-nominates-jassm-missile-to-host-new-computer-killing-412348/, (preuzeto 12. novembra 2015).

[520] Yu Wang, „A New CVE-2015-0057 Exploit Technology", September 2015, 2015, https://www.exploit-db.com/docs/39660.pdf (preuzeto 18. novembra 2015).

analizirati šta oba pojma znače u kontekstu primene IKT u sajber prostoru, u smislu informacione i sajber bezbednosti, i u smislu vojno-političke i međunarodnopravne primene.

7.1.1. Vojno definisanje sajber napada

Sajber napadi ugrožavanjem informacione bezbednosti u zavisnosti od konteksta u kome se posmatraju, mogu imati različit karakter. U pogledu prava, isti napad može biti krivično delo, ili legitimni akt primene sile (na primer, kao legitimna primena sile u toku oružanog sukoba u skladu sa principima i normama Međunarodnog prava oružanih sukoba). Napadi koji su izvedeni na identičan način u tehničkom pogledu u vojnom pogledu mogu imati potpuno drugačiji karakter: mogu biti ofanzivna dejstva, obaveštajne akcije ili operacije borbene podrške. Napad u tehničkom i vojnom pogledu nemaju isto značenje. Na vojnu prirodu sajber napada, pored tehničkog njegovog tehničkog karaktera utiču i sekundarni ciljevi napadača i posledice napada. Vojni rečnik Ministarstva odbrane SAD definiše **računarske mrežne operacije** kao „akcije preduzete upotrebom računarskih mreža sa ciljem da se onemoguće, onesposobe, oštete ili unište informacije koje se nalaze u računarima i računarskim mrežama ili sami računari i mreže“[521].

Talinski priručnik definiše **računarski mrežni napad** na isti način kao i vojska SAD, sa napomenom da je ovaj napad vrsta sajber napada[522].

Italijanski Nacionalni strategijski okvir za bezbednost u sajber prostoru pod pojmom **računarski mrežni napad** smatra: „aktivnosti koje su izvede kroz i u sajber prostoru sa ciljem da izvrše manipulaciju, opstrukciju, onemogućivanje, narušavanje ili uništavanje informacije pohranjene u IKT mrežama ili računarskim sistemima ili same IKT mreže i računare“[523].

---

[521] United States of America, Department of Defense Dictionary of Military and Associated Terms, 2011, p. 73 (JP 3-13) AND United States of America, NIST Glossary of Key Information Security Terms, 2013, p. 41

[522] Schmitt, Michael N., „The Tallinn Manual on International Law Applicable to Cyber Warfare“, NATO Cooperative Cyber Defence Center of Excellence, 2013, http://www.ccdcoe.org/tallinn-manual.html

[523] Government of Italy, Presidency of the Council of Ministers, „National Strategic Framework for Cyberspace Security“, 2013, p. 41, 2013, https://www.ccdcoe.org/strategies-policies.html

Vojne definicije napada su usmerene na dejstva vojnih sistema (računarskih mreža, računara i informacija u njima) i način i vrstu dejstva koje napadi ostvaruju na te sisteme. U vojnom smislu napadi u sajber prostoru se izvode primenom sredstava informaciono-komunikacionih tehnologija, primenom računara i računarskih mreža, sa ciljem izmene ili uništavanja informacija u informacionim sistemima ili samih sistema. One u prvi plan ne ističu tehniku kojom je izveden napad, već njegovu vojnu nameru, kojom se ostvaruje vojni doprinos napada.

7.1.2. Političko-bezbednosno definisanje sajber napada

U političko-bezbednosnom pogledu, sajber napadi se najčešće definišu u smislu namere napadača i posledica koje su izazvali, ali u širem kontekstu nego vojne definicije.

Novozelandska Strategija sajber bezbednosti navodi da je **sajber napad** „pokušaj da se naruše ili oštete funkcije sistema koji zavise od računara, pristup informacijama, ili pokušaj da se prate onlajn aktivnosti pojedinaca bez njihovog dopuštenja“[524].

Rumunska strategija sajber bezbednosti definiše **sajber napad** kao „neprijateljsku akciju preduzetu sa ciljem da ugrozi sajber prostor i sajber bezbednost“[525].

Po nemačkoj BSI, **sajber napadi** su „napadi preduzeti u sajber prostoru putem alata, servisa, aplikacija u sajber prostoru; u procesu, sajber prostor može biti izvor, meta ili okruženje napada“[526].

Po NIST-ovom rečniku, sajber napad je „napad putem sajber prostora koji napada upotrebu sajber prostora od strane neke organizacije u cilju narušavanja, onesposobljavanja, uništavanja ili zlonamernog kontrolisanja računarskog

[524] New Zealand, Ministry for Communications and Information Technology, „New Zealand’s Cyber Security Strategy“, Ministry for Communications and Information Technology, 2011, 12,http://www.dpmc.govt.nz/sites/all/files/publications/nz-cyber-security-strategy-june-2011_0.pdf

[525] CERT Romania, Hotărârea nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României şi a Planului de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică, CERT Romania, 2013, 7, http://www.cert-ro.eu/files/doc/StrategiaDeSecuritateCiberneticaARomaniei.pdf

[526] Germany Federal Office for Information Security (BSI), „Glossary/Terminology, Bundesmat fur Sicherheit in der Informationstechnik, 2014,https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Glossar/cs_Glossar_A.html;jsessionid=C8733A22C9EABECEC04B7FDDDE34C451.2_cid294

okruženja/infrastrukture ili uništavanja integriteta podataka ili krađe kontrolisanih informacija“[527].

Konačno, EastWest institut definiše **sajber napad** kao „ofanzivnu upotreba sajber naoružanja sa namerom da se ošteti odabrani cilj“[528]. Navedena definicija pored pojma sajber prostora uvodi i pojam sajber naoružanje, praveći analogiju sa tradicionalnim sukobima. Iako je u teorijskom pogledu tačna, diskutabilna je njena praktična promenljivost, s obzirom na to da se koncept naoružanja u fizičkom i sajber prostoru imaju potpuno drugačiju prirodu.

Navedene definicije se odnose više na proces sukoba (oružanog i neoružanog), a ne na proces ratovanja, koji karakteriše oružana primena sile. Po njima, cilj napada je ugrožavanje bezbednosti u cilju ostvarivanja efekata na cilj napada. Njihova zajednička karakteristika je da se izvode u sajber prostoru primenom specifičnih sredstava.

7.1.3. Tehničko definisanje sajber napada

Sajber ratovanje se izvodi preduzimanjem sajber napada. Njih omogućava prisustvo ranjivosti u svim informacionim sistemima, kao i sama priroda informacionih tehnologija, koja omogućava beskonačno kopiranje elektronskih podataka i umrežavanje između sistema na nivou podataka. Pored toga, sajber prostor je tehnološki stvoreno okruženje, pa je stoga značaj tehničko-tehnološki orjentisanog pristupa razumevanju njegovih fenomena od primarne važnosti. Od suštinske važnosti za razumevanje prirode sajber napada je njihov tehnički i tehnološki kontekst, a ne pravni.

Po američkom Nacionalnom institutu za standarde i tehnologiju napad predstavlja: „pokušaj da se ostvari neautorizovani pristup sistemskim servisima, resursima ili informacijama, ili pokušaj da se naruši integritet sistema“[529].

---

[527] U.S. Department of Commerce, Richard Kissel, , „National Institute of Standards and Technology Glossary of Key Information Security Terms, 2013. http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf, 57

[528] James B. Godwin III, Andrey Kulpin, Karl Frederick Rauscher and Valery Yaschenko, EastWest Institute, "Russia-U.S. Bilateral on Cybersecurity: Critical Terminology Foundations 2, Issue 2", The EastWest Institute, 2011, 44, http://www.ewi.info/idea/critical-terminology-foundations-2

[529] Richard Kissel, „National Institute of Standards and Technology Glossary of Key Information Security Terms“, U.S. Department of Commerce, 2013, http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf, 11.

Nemačka Federalna kancelarija za informacionu bezbednost (BSI), napad je definisala kao: „oblik namerne pretnje, koja predstavlja neželjenu ili neautorizovanu akciju sa ciljem da ostvari prednost ili oštećenje treće strane. Napadači mogu preduzimati napad u ime trećih strana u cilju sticanja prednosti“[530].

Međunarodna telekomunikaciona unija (ITU) pod sajber napadom podrazumeva: „aktivnosti preduzete da se zaobiđe ili iskoristi nedostatak u bezbednosnim mehanizmima sistema. Direktnim napadom na sistem iskorišćavaju se nedostaci u algoritmima, principima, ili stanjima bezbednosnih mehanizama. Indirektni napadi se izvode kada zaobilaze mehanizme ili kada uzrokuju da sistem koristi mehanizme nepravilno“[531]. Definicija iste međunarodne organizacije iz 2007. godine je vrlo značajna. Ona je jedna od retkih definicija koja razlikuje napade koji su poznati napadnutima ili to nisu. Po toj definiciji „napad može biti poznat ili nepoznat. Poznat napad znači da je obrazac ili paket kojim se izvodi napad otvoren. Iako se obrazac napada ili paket napada nije otvoren u slučaju nepoznatog napada, on se odnosi na ponašanje koje otežava mrežnu situaciju“[532].

ISO/IEC 18043:2006 standard definiše napad kao: „nastojanja da se uništi, izloži, izmeni ili onesposobi informacioni sistem i/ili informacije u njemu ili na drugi način prekrši bezbednosna politika“[533].

---

[530] Federal Office for Information Security (BSI), „Glossary/Terminology“, Bundesmat fur Sicherheit in der Informationstechnik, Germany, 2014, https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Glossar/cs_Glossar_A.html;jsessionid=C8733A22C9EABECEC04B7FDDDE34C451.2_cid294

[531] International Telecommunication Union, „ITU Terms and Definitions“, ITU-T, Rec. H.235.0 (01/2014), 2014, 3.2.2, http://www.itu.int/ITU-R/index.asp?redirect=true&category=information&rlink=terminology-database&lang=en&adsearch=&SearchTerminology=exploit&collection=both&sector=all&language=all&part=abbreviationterm&kind=anywhere&StartRecord=1&NumberRecords=50

[532] International Telecommunication Union, ITU-T X.1036 (11/2007), 2007, „ITU Terms and Definitions“, http://www.itu.int/net/ITU-R/index.asp?redirect=true&category=information&rlink=terminology-database&lang=en&adsearch=&SearchTerminology=attack&collection=both&sector=all&language=all&part=abbreviationterm&kind=anywhere&StartRecord=1&NumberRecords=50#lang=en

[533] International Organization for Standardization, „ISO/IEC Glossary of IT Security Terminology“, ISO/IEC, 2013, http://www.jtc1sc27.din.de/cmd?level=tpl-bereich&menuid=64540&languageid=en&cmsareaid=64540

Rečnik *Internet Engineering Task Force* (IETF) definiše napad kao: „namerni akt kojim neki entitet nastoji da zaobiđe bezbednosne servise i naruši bezbednosnu politiku sistema. To je stvarno napadanje bezbednosti sistema koje potiče od neke inteligentne pretnje“[534].

Dakle, u tehničkom pogledu, sajber napad predstavlja **namerno ugrožavanje informacione bezbednosti nekog sistema ili informacija sadržanim u njemu, preduzeto od strane nekog entiteta, zaobilaženjem bezbednosnih mehanizama sistema, zloupotrebom nedostataka u sistemu tehničke ili netehničke prirode.**

Dakle, sajber napadi u tehničkom pogledu predstavljaju primenjeno narušavanje informacione bezbednosti, čiji je direktni cilj narušavanje informacione bezbednost sistema, a indirektni otkrivanje podataka i informacija, uništenje, oštećenje ili onesposobljavanje informacionih sistema, kao lica i sistema koji zavise od primarno napadnutog sistema.

7.2. Sadržaj i karakter sajber napada

Na osnovu navedenih definicija sajber napada moguće je izvršiti analizu ključnih zajedničkih karakteristika koje one nude, a zatim i sintezu njihovog opšteg, suštinskog značenja. U svim slučajevima, sajber ratovanje se vodi preduzimanjem sajber napada na protivničke informacione sisteme, resurse, vrednosti i sposobnosti. Takođe, u svim slučajevima, sajber napadi se izvode u sajber prostoru i predstavljaju namerno narušavanje informacione bezbednosti protivnika. Bez obzira da li se taj napad na informacionu bezbednost odnosi na društvenu ili tehničku sferu, uvek neki faktori pretnje sa namerom i na organizovan način iskorišćavaju postojeće ranjivosti napadnutog sistema. U skladu sa stavom o tome šta predstavlja informaciona bezbednost, i ranjivosti imaju drugačiji karakter. Njihova priroda može imati široko značenje, od softverskih nedostataka, do načina društvene organizacije. Takođe, direktni cilj sajber napada retko je i konačni. Gotovo uvek postoji neki viši, naredni cilj, koji je od primarnog značaja za proces vođenja sukoba.

[534] Internet Engineering Task Force, „Internet Security Glossary Version 2“, The IETF Trust, 2007, http://tools.ietf.org/html/rfc4949

Ono što se razlikuje u pogledu definisanja sajber napada i sajber ratovanja jeste odgovor na pitanje, šta se podrazumeva pod pojmom "Informaciona bezbednost"? Po tehnički orjentisanim standardima u području informacione bezbednosti, narušavanje informacione bezbednosti napadnutog sistema se ostvaruje tako što napadač ugrožava - "napada" informacije i informacione sisteme svog cilja putem "neovlašćenog pristupa, upotrebe, objavljivanja, narušavanja, izmene ili uništavanja"[535], čime narušava njegova svojstva koja ga čine informaciono bezbednim: poverljivost, integritet i dostupnost, uz autentičnost, odgovornost, neporecivost i pouzdanost[536].

Međutim, po stavu nekih relevantnih međunarodnih organizacija, informaciona bezbednost ima drugačije značenje, koji se ne posmatra primarno iz tehničkog, već iz društveno-političkog konteksta. Na primer Šangajska organizacija za saradnju[537], definiše informacionu bezbednost u međunarodno-političkom smislu kao: "bezbednost pojedinaca, društva, države i njihovih interesa od pretnji, destruktivnih i drugih negativnih uticaja u informacionom prostoru"[538]. Pri tome "informacioni prostor" za ovu organizaciju predstavlja: "područje aktivnosti koje se odnosi na stvaranje, menjanje, transfer, upotrebu i čuvanje informacija koje ostvaruje uticaj na individualnu i javnu svest, informacionu infrastrukturu i informacije"[539], što ima prilično sličan smisao kao i pojam sajber prostora, prethodno definisan kao područje sačinjeno iz tri sloja.

Ono što razlikuje oba pristupa je okolnost, koja se tiče toga, gde je svrstan primarni cilj sajber napada. Ono što države Šangajske organizacije primarno smatraju sajber napadom, po svom predmetu i sadržaju u stvari je deo informacionih operacija. Informacione operacije se izvode u informacionom području, koje se u velikoj meri poklapa sa sajber područjem, ali nije isto. Osim informacija u sajber prostoru, postoje i druge informacije,

[535] CNSS, , *National Information Assurance (IA) Glossary*, 37.

[536] International Organization for Standardization and International Electrotechnical Commission, *ISO/IEC 27000:2016(en), Information technology — Security techniques — Information security management systems — Overview and vocabulary*, (Geneva, Switzerland: ISO/IEC, 2016).

[537] Međunarodna politička, vojna i ekonomska organizacija Kine, Rusije, Kazahstana, Kirgistana, Tadžikistana i Uzbekistana, dok su u procesu pridruživanja Indija i Pakistan. Ova organizacija nema visok nivo institucionalne kohezije poput država evroatlantskih integracija (NATO, EU, UKUSA), ali predstavlja većinu svetskog stanovništva i značajan privredni centar moći, pri čemu su im međunarodni stavovi bliski drugim svetskim država u brzom razvoju (poput Brazila, Južne Afrike i drugih).

[538] Соглашение между правительствами государств, Приложение 1.

[539] Ibid.

na primer, u štampi, literaturi na televiziji ili radiju (u smislu analognih ili nedigitalizovanih medija), pa čak i u usmenoj komunikaciji. Informacije mogu biti u formi digitalnih informacija u sajber prostoru, ali im to nije primarna svrha i priroda. Za informacije je važno kakvu informativnu poruku i smisao prenose, a ne da li su zapisane u kamenu, na papiru ili u digitalnom obliku.

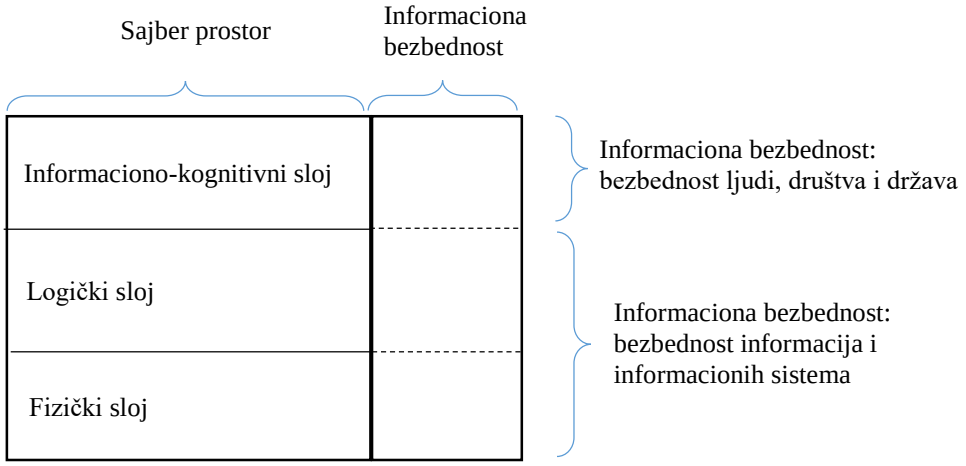
Ministarstvo odbrane SAD definiše Informacione operacije kao: "integrisanu primenu informaciono-zasnovanih sposobnosti tokom vojnih operacija zajedno sa drugim vrstama operacija sa ciljem uticaja, prekidanja, remećenja ili prisvajanja procesa donošenja odluka protivnika i potencijalnih protivnika istovremeno štiteći vlastiti proces donošenja odluka".[540] Međutim, ne tako davno, 1998. godine, ista institucija je istim pravilom informacione operacije definisala kao "akcije preduzete sa ciljem uticaja na neprijateljske informacije i informacione sistema i odbranu vlastitih informacija i informacionih sistema"[541] Dakle, u okviru samog sistema odbrane SAD, razlika u shvatanju pojma informacionih operacija nije bila ništa manja, nego što je ona danas u shvatanju pojma sajber ratovanja između SAD i Rusije. Međutim, kapaciteti i sposobnosti za izvođenje operacija u sajber prostoru, kao i pretnje, razvijane su različitim tempom i pravcem, pa je stoga razlika u stavu razumljiva. Svaka država poseduje sopstvene kapacitete, sposobnosti, kao i ranjivosti u informacionom i sajber području, a u skladu sa svojim nacionalnim ciljevima ispoljava akcije na način koji joj najviše odgovara u cilju ostvarivanja sopstvenih interesa i odbrane.

Takođe, u oba slučaja je bitno kako međunarodno pravo gleda na primenu tih aktivnosti, bez obzira na to kako su one definisane nacionalnim politikama. U tom pogledu, bitne su posledice napada u sajber prostoru i objektivna ocena da li se one mogu svrstati u akcije primene oružane sile, odnosno agresije. Imaju to u vidu, očigledno je da je stav zasnovan na tehnološkoj prirodi informacione bezbednosti mnogo bliži odredbama i smislu normi i pravila međunarodnog prava, nego stav zasnovan na društveno-političkoj prirodi i

[540] *Information Operations, Joint Publication 3-13.*

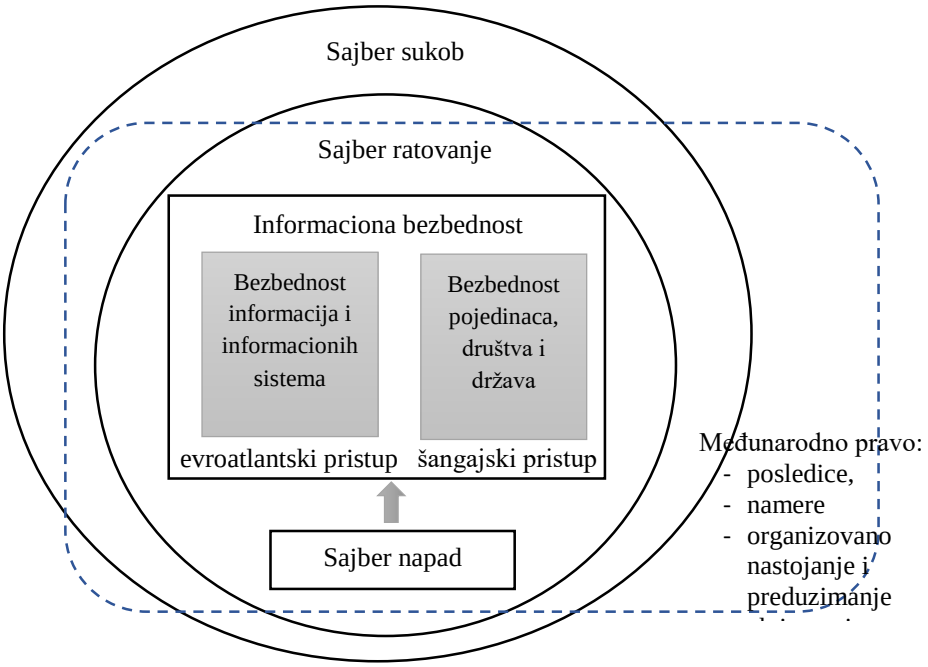
[541] Joint Doctrine for *Information Operations, Joint Publication 3-13*. Washington, DC: U.S. Joint Chiefs of Staff, 1998, VII, http://www.c4i.org/jp3_13.pdf (preuzeto 19. novembra 2015).

posledicama. Jednostavan razlog za to nije političko usmerenje međunarodnog prava, već sama priroda prava.



Slika 16. Razlike u međunarodnim gledištima u odnosu na karakter informacione bezbednosti

Međunarodno pravo reguliše primenu oružene sile, kao i efekte koji se na dokaziv način mogu povezati sa praktičnom primenom sile, a ne psihološke ili prikrivene operacije, koliko god one izgledale očigledne široj javnosti.



Slika 17. Različiti međunarodni pristupi pojmu sajber ratovanja.

Postupak dokazivanja veze između počinioca, dela i posledice mora imati materijalnu prirodu, a ta priroda se mnogo lakše može naći u tehnološki orjentisanoj prirodi sajber napada.

7.3. Izbor kriterijuma za određivanje prirode sajber napada

Svojstva informacione bezbednosti, na način kako ih definišu međunarodni standardi u području informacione bezbednosti se odnose na svojstva bezbednosti informacija i informacionih sistema bez obzira na način kako se ona ugrožavaju, fizičkim ugrožavanjem, informacionim delovanjem, ili na bilo koji drugi način. Na primer, Hetovej i grupa autora predlažu da se sajber napad definiše kao: "svaka akcija preduzeta sa ciljem narušavanja funkcije računarskih mreža u političku ili svrhu nacionalne bezbednosti"[542]. Pri tome, navedeni autori zauzimaju pristup zasnovan na cilju napada, a ne na sredstvima kojima je napad izvršen. Rezultat takvog pristupa je zaključak da "sajber napad može biti preduzet sredstvima svake akcije – hakingom, bombardovanjem, sečenjem, inficiranjem i tako dalje – ali da bi bio sajber napad mora imati za cilj narušavanje ili prekid funkcionisanja računarske mreže"[543].

Ovakva definicija je pogrešna u metodološkom i tehničkom pogledu. Pojedine vrste ratovanja mogu se klasifikovati i prema cilju dejstva[544], prema sredstvu[545] ili prema području dejstva[546]. Pri tome, ne postoji neka striktna usvojena metodologija za podelu, već se kao kriterijum bira ono što najviše karakteriše datu vrstu ratovanja, odnosno ono što najviše odgovara njegovoj suštini i prirodi, odnosno osnovnoj nameni. Kinetička sila se može upotrebiti i za uništenje računarskog sistema, ali joj to nije osnova namena, već fizičko onesposobljavanje ili uništenje bilo kog cilja dejstva.

Većina drugih autora, sajber napade karakteriše po sredstvu kojim je napad izvršen, a ne po prirodi mete klasičnog napada.[547]

---

[542] Hathaway et al., "The Law of Cyber-Attack," 826.

[543] Ibid.

[544] Na primer, ekonomsko, psihološko, medijsko ratovanje, elektronsko ratovanje i druge vrste.

[545] Na primer, konvencionalno, nuklearno, pešadijsko, oklopno-mehanizovano, hemijsko ratovanje i druge vrste.

[546] Na primer, pomorsko, kopneno, vazdušno, kosmičko, urbano, ili sajber ratovanje.

[547] Lachow, "Cyber Terrorism: Menace or Myth?"

Po Lačovu[548], sajber napadi se karakterišu isključivo po sredstvu. Ovom pristupu klasifikacije sajber napada, koji je saglasan sa tehničkom i vojnom prirodom sajber sukoba, treba još samo dodati primarnu ili osnovnu svrhu dejstva.

U sajber ratovanju ne postoji univerzalno oružje, niti univerzalne metode napada. Svaki pojedinačni sajber napad tehnički više zavisi od mete (njenih ranjivosti), nego od napadača. Izvor napada je tako više sadržan u samoj prirodi cilja napada nego u eksternim sposobnostima napadača. Ranjivost je:

a) nedostatak ili slabost[549]
b) u dizajnu sistema, implementaciji, radu i upravljanju[550] bezbednosnim procedurama i internim kontrolama[551], podložna namernom[552] ili slučajnom iskorišćavanju od strane agenta pretnje
c) sa posledicom narušavanja sistemske politike bezbednosti[553] ili neočekivanim ili neželjenim događajem.[554]

Međutim, u smislu međunarodnog prava ne može se napad na protivnika procenjivati svojstvom informacione bezbednosti cilja. Cilj nema odgovornost za vrstu i posledice napada koji je preduzeo napadač. Međunarodno pravo oružanih sukoba ne može ocenjivati i opravdati neki napad time što napadnuta strana nije uspostavila neophodan sistem informacione bezbednosti vlastitih informacija i sistema, ili nije imala sposobnosti da to učini. Konačno, to nije predmet procene samo Međunarodnog prava oružanih sukoba, već prava u opštem smislu.

Sajber oružje predstavlja sredstvo kojim se izvršava povreda informacione bezbednosti cilja, bez obzira u koju svrhu, špijunsku, kriminalnu, odbrambenu ili drugu.[555] Arimatsu

[548] Lachow, "Cyber Terrorism: Menace or Myth?"

[549] Robert W. Shirey, *Internet Security Glossary*, ver. 2nd, IETF Network Working Group, https://tools.ietf.org/html/rfc4949#page-3 (preuzeto 29. septembra 2015).

[550] Ibid.

[551] CNSS, *National Information Assurance (IA) Glossary.*

[552] International Organization for Standardization, *ISO 27005:2011 Information technology -- Security techniques -- Information security risk management,* (Geneva, Switzerland: ISO, 2011).

[553] National Institute of Standards and Technology, *Managing Information Security Risk, Organization, Mission, and Information System View* (Gaithersburg, MD: National Institute of Standards and Technology, 2012).

[554] Mladenović, „International Legal Regulation," 36.

[555] Thomas Rid and Peter McBurney, "Cyber-weapons," *RUSI Journal* 157, no. 1 (2012): 6-13.

smatra da sajber oružje ni ne postoji u smislu tradicionalnog oružja, jer u direktnom dejstvu ne ostvaruje efekat fizičkog uništenja, ranjavanja ili ubijanja.[556] Iako navedena tvrdnja ne odgovara stvarnosti, ona ipak pokazuje da pojam sajber oružja i napada nije definisan i jasan.

Imajući navedeno u vidu, Šmit i autori Talinskog priručnika[557] su stava da sama priroda sajber napada i sajber oružja nije primarno pitanje, već efekti koji se njihovom primenom ostvaruju. Ipak, u tom pogledu, treba se imati u vidu da efekat dejstva sajber napada ne mora uvek biti ostvaren, a da namera napadača i tada postoji.

Ni primarnost dejstva ne može biti relevantan kriterijum za ocenu sajber napada, jer oružje biti sve što može biti upotrebljeno za napad. Na primer, u terorističkom napadu na SAD, teroristi su upotrebili putničke avione za napad u kome je poginulo više od pet hiljada ljudi.

Imajući u vidu brzinu razvoja informaciono-komunikacionih tehnologija i sajber prostora, koji u skoroj budućnosti ostavljaju mnogo mogućnosti za nove oblike vojnog dejstva u cilju napada, kao i trend digitalizacije svega, koji znači da su informaciono-komunikacione tehnologije uključene u sva druga tehnološki zasnovana područja i aktivnosti, najpodesniji kriterijum za određivanje prirode sajber ratovanja, neophodna je specijalizacija i dodatno određenje područja aktivnosti istovremenim uključivanjem više kriterijuma:

- kriterijuma sredstva (primena informaciono-komunikacionih tehnologija)
- kriterijuma funkcije ili namere (namerno ugrožavanje informacione bezbednosti ciljanog sistema)
- kriterijuma područja vođenja sukoba (dešava se u sajber prostoru)

Pri tome treba uvek imati u vidu primarni cilj dejstva. U slučaju sajber napada on je narušavanje informacione bezbednosti informacija i sistema delovanjem u sajber prostoru i kroz sajber prostor.

---

[556] Louise Arimatsu, "A Treaty for Governing Cyber-weapons," in *2012 4th International Conference on Cyber Con, Proceedings*, eds. Christian Czosseck, Rain Ottis and Katherina Ziolkowski, 91-109 (Tallinn: NATO CCD COE Publications, 2012), https://ccdcoe.org/cycon/2012/proceedings/d3r1s6_arimatsu.pdf (accessed September 23, 2015).

[557] Schmitt, *Tallinn manual*, 54.

7.4. Sajber napad kao proces

Kako je navedeno u prethodnoj analizi, sajber napad nije proizvod, konkretan sistem, sredstvo koje univerzalno služi za primenu "oružane sile" prema protivniku, već je proces namernog i planiranog narušavanja informacione bezbednosti protivničkih sistema. Razvijeno je više modela procesa sajber napada, koji se međusobno razlikuju po fazama (etapama) napada, sadržaju, okruženju u kome se izvode i drugim kriterijumima. Kako navode Hatčins, Klopert i Amin[558], modeli procesa sajber napada se prvenstveno koriste u cilju razumevanja procesa napada, opisivanja faza napada, identifikaciju kritičnih aktivnosti napadača, utvrđivanja obrazaca za detekciju napada, i razumevanja njihove (tehnološke) prirode. U tom pogledu postoji nekoliko karakterističnih modela sajber napada, koji se razlikuju po broju i sadržaju faza napada, ali svi sadrže ključne aktivnosti napada i njihov redosled.

7.4.1. Lokid-Martin model sajber napada

Istraživači kompanije Lokid Martin (eng. *Lockheed-Martin*), Hatčins, Klopert i Amin[559] su 2011. godine objavili poznati model sajber napada, takozvani „sajber lanac ubijanja" (eng. *cyber kill chain*), tačnije, model sajber upada u protivnički sistem. Po predloženom modelu, sajber upad u protivnički sistem ima sedam etapa (Slika 18): izviđanje, naoružavanje, dopremanje, iskorišćavanje, instaliranje, rukovođenje i upravljanje i aktivnost na ostvarivanju cilja.[560] Navedeni model napada je predstavljen kao proces koji napadači moraju ostvariti po datom redosledu, kako bi otkrili i iskoristili ranjivosti napadnutog sistema, upali u njega i ostvarili cilj napada. Primenom navedenog modela moguće je opisati širok skup različitih vrsta napada u realnom okruženju, od obaveštajnih napada, preko specijalnih operacija, do *BotNet* i čak insajderskih napada. Etape predloženog modela ne zahtevaju striktno sukcesivno izvršavanje.

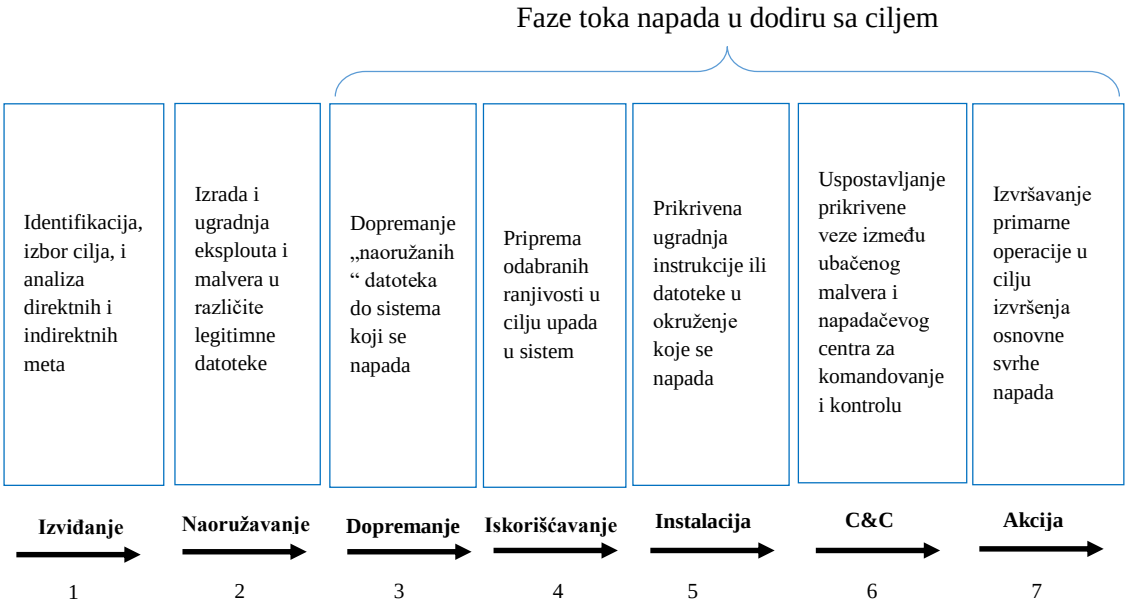
Na primer, pojedine etape mogu se paralelno odvijati. Neposredno izvršenje napada se realizuje u dve finalne etape (komandovanja i kontrole i izvršenja instrukcije napada). U pogledu primene međunarodnog prava, tek ta poslednja etapa napada odgovara

[558] Hutchins, Cloppert, and Amin, "Intelligence-driven computer network," 113.

[559] Ibid.

[560] U originalu ove metode se nazivaju: *Reconnaissance, Weaponization, Delivery, Exploitation, Instalation, Command and Control, and Actions on Objectives*.

neposrednoj primeni oružane sile u sukobu u fizičkom okruženju, na primer, gađanju vatrenim oružjem. Bez te poslednje etape napada, po međunarodnom pravu, sajber napad bi se mogao smatrati samo špijunskom aktivnošću, koja ne podleže pravilima Međunarodnog prava oružanih sukoba.



Slika 18. Model "kill chain" sajber napada kompanije *Lockheed-Martin*, 2011

7.4.2. PrEP model sajber napada

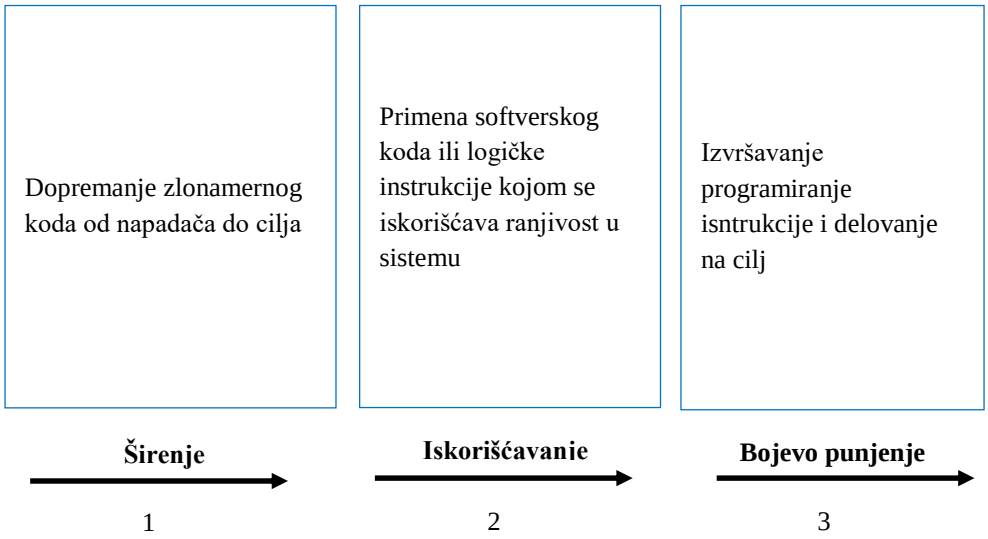
Istraživač Her[561] sa Univerziteta Džordž Vašington je 2014. godine predložio konceptualni model sajber napada koji je redukovan u odnosu na model „cyber kill chain" na svega tri faze. Ovaj model ne služi za organizovanje sajber napada već za njegovo razumevanje. Model je zasnovan na primeni malvera[562], kao softverskog oružja, i ranjivosti, kao centralne mete napada u okviru ciljanog sistema. Po ovom modelu, ključne faze napada su:

- širenje (eng. *propagation*), kojim se doprema malver do cilja;
- iskorišćavanje (eng. *exploit*), kojim se omogućava upad malvera u sistem; i

[561] Trey Herr, "PrEP: A Framework for Malware and Cyber Weapons," Proceedings of the International Conference On Information Warfare & Security, 2014: 84-91.

[562] Zlonamerni softver.

- „bojevo punjenje“ (eng. *payload*), kojim se izvršava programirana radnja nad ciljem od strane ubačenog malvera.



Slika 19. Model “PrEP” sajber napada, 2014[563].

Navedeni model napada je zasnovan na primeni malvera, koji ostvaruje funkciju oružja, dok je ključna izvršna radnja napadača etapa iskorišćavanja, tokom koje napadač aktivno upada u napadnuti sistem (ali ne vrši dejstvo na njega tokom ove faze). I ova radnja se ostvaruje primenom pisanog izvršnog programskog koda, takozvanog eksploita. Ključni uslov za primenu napada po PrEP modelu napada je poznavanje ranjivosti napadnutog sistema od strane napadača, koji na osnovu te informacije programiraju napadački softver, izvršnu datoteku. Ranjivosti sistema ne moraju nužno biti softverske, već mogu postojati u bilo kom području od značaja za informacionu bezbednost napadnutog sistema.

[563] Trey Herr, "PrEP: A Framework for Malware and Cyber Weapons."

Tabela 6. Uporedne faze sajber napada i analogija sa tradicionalnim vojnim operacijama[564]

Vrsta faze sajber napada	*Opis*	*Analogija sa drugim ofanzivnim aktivnostima*	*Analogija sa opštim fazama vojnih operacija*
1. Izviđanje	Identifikacija, selekcija cilja i analiza direktnih i indirektnih meta	Obaveštajno prikupljanje podataka i analiza, planiranje operacije	Pripremna faza
2. Naoružavanje	Ugradnja eksploita i malvera u legitimne klijentske datoteke (programske skripte, marke, *office* i pdf dokumente, slike, video ili zvučne datoteke itd.)	Proizvodnja naoružanja, ugradnja na borbeno sredstvo i opremanje borbenih sistema	Pripremna faza
3. Dopremanje	Dopremanje "naoružane" datoteke do ciljanog sistema, najčešće uz pomoć legitimnog servisa ili procesa (elektronskom porukom, veb-stranicom ili USB portabl uređajem)	Specijalne operacije obaveštajne operacije, teroristička aktivnosti, infiltracija, pripremna borbena dejstva	Faza izvođenja operacija
4. Iskorišćavanje	Priprema ciljane ranjivosti u napadnutom sistemu radi omogućavanja neovlašćenog upada u sistemske procese, resurse ili servise	Specijalne i tajne operacije, terorističke ili informacione aktivnosti	Faza izvođenja operacija
5. Instalacija	Prikriveno ubacivanje u okruženje ciljanog sistema	Specijalne i tajne operacije, terorističke ili informacione aktivnosti	Faza izvođenja operacija
6. Komandovanje i kontrola	Uspostavljanje prikrivene veze između ubačene datoteke ili procesa sa napadačevim centrom za komandovanje i kontrolu	Specijalne i tajne operacije, terorističke ili informacione aktivnosti	Faza izvođenja operacija; Faza iskorišćenja operacija
7. Akcija na cilj	Izvršenje osnovnog cilja napada	Vojne, terorističke ili obaveštajne operacije	Faza izvođenja operacija; Faza iskorišćenja operacija; Faza stabilizacije operacija

7.5. Ljudi, tehnologije i procesi kao cilj sajber napada

Zahvaljujući brojnim nedostacima, neki vid napada u sajber prostoru se uvek može ostvariti dugim i upornim traženjem načina za neovlašćeni pristup sistemu. To se može učiniti primenom pojedinačnih elemenata ili njihovom kombinacijom na fizičkom (preko ljudi, elektromagnetnih talasa, energije, hardvera, i u fizičkom prostoru), logičkom (putem logičkih instrukcija i podataka) i na kognitivnom nivou (u svesti, volji, znanju, razumevanju ljudi i inteligentnih sistema). U kontekstu informacione bezbednosti to podrazumeva uključivanje u obzir tri ključna područja bezbednosti: ljudi, procesa i tehnologija.

Konceptualni okvir organizaciono-bezbednosnog trojstva „ljudi, procesi i tehnologije" je nastao početkom šezdesetih godina kao rezultat istraživanja u oblasti organizacionih nauka, posebno organizacione strategije, strukture i menadžmenta znanja, u uslovima pojave novih automatizovanih tehnologija.[565] Po inicijalnom konceptu, koji su razvili Lavit[566] i Čandler[567], unutrašnje sile organizacije, inherentnu tehnologiju, strategiju, procese, ljude i strukturu organizacija pokreću dve najvažnije sile u životu svakog organizacionog sistema: spoljno socioekonomsko okruženje i tehnologija.[568] Iz tog koncepta je izgrađen novi model socioekonomskog sistema, po kome svaka organizacija funkcioniše kao dinamički sistem četiri ključne promenljive: ljudi, tehnologije, strukture i zadataka.[569] Po Lavitovom modelu, promene u jednom elementu impliciraju organizacione promene koje ostvaruju efekte na jedan ili više drugih elemenata. Struktura

[565] Harold J. Leavitt, and James G. March, *Applied Organizational Change in Industry: Structural, Technological and Humanistic Approaches* (Pittsburgh: Carnegie Institute of Technology, Graduate School of Industrial Administration, 1962).

[566] Harold J. Leavitt, „Applied Organizational Change in Industry," in *Handbook of Organizations*, ed. James G. March (Chicago: Rand McNally, 1965).

[567] Alfred, D. Chandler Jr., *Strategy and Structre: Chapters n the History of American Industrial Enterprise* (Cambridge, MA: MIT Press, 1962).

[568] John F. Rockart, and Michael S. Scott Morton, "Implications of Changes in Information Technology for Corporate Strategy," *Interfaces* 14 (January-February 1984): 84–95. http://dspace.mit.edu/bitstream/handle/1721.1/2040/swp-1408-09891521-cisr-098.pdf?sequence=1 (preuzeto 18. avgusta 2015).

[569] Harold J. Leavitt, „Applied Organization Change in Industry: Structural, Technical, and Human Approaches," in *New Perspectives in Organizational Research,* eds.Cooper S, Harold J. Leavitt and Shelly K., 55-71 (Chicester, UK: John Wiley and Sons, 1964).

i zadaci organizacije se jednostavnije mogu predstaviti najmanjim zajedničkim imeniteljem koji zadržava svojstvo oba elementa – organizacionim procesima.[570]

Sajber prostor je okruženje nastalo funkcionisanjem informaciono-komunikacionih tehnologija čiji su ključni sadržaji podaci, pri čemu ključni procesi potiču od manipulacije ljudi i sistema sa tim podacima. Pokretanje sajber napada predstavlja upotrebu IKT u cilju zlonamerne manipulacije sa podacima u sajber prostoru. U ovom prostoru je sve - **izvori pretnji** (napadači), **sredstva napada** (oružje/sistemi) i **primarni ciljevi napada** (sistemi i podaci korisnika). Same ranjivosti sistema se mogu nalaziti u sajber prostoru i van njega. Priroda ovih elemenata je složena i višeslojna, kao što je to i sam sajber prostor. Ona zavisi od mnoštva faktora koji se mogu svrstati u skup ljudi, procesa i tehnologije.

Sajber napadi se mogu shvatiti kao specifične aktivnosti vezane za primenu informacione bezbednosti u sajber prostoru, koja se tiče podataka i informacija i informacionih sistema (softverskih i hardverskih), koji predstavljaju tehnologiju. Od značaja za primenjenu informacionu bezbednost su i ljudi koji upotrebljavaju tehnologiju, kao i procesi koji nastaju u interakciji unutar sistema, i između sistema i ljudi. Ljudi i sistemi su istovremeno i izvor pretnji i ciljevi u sukobima u sajber prostoru.

Što tehnologija ostvaruje veći uticaj na život i aktivnosti ljudi, to je veći njen uticaj i na vođenje sukoba između ljudi. Računarstvo i informaciono-komunikacione tehnologije menjaju način na koji ljudi žive i rade, i konačno, menjaju i same ljude. Na taj način utiču i na sukobe: menjajući sredstva kojim se vode sukobi, aktere sukoba i metode vođenja sukoba. Savremene tehnologije, imaju ključni uticaj na prirodu, trajanje i ishod sukoba.

Sajber prostor je složena veštačka tvorevina čiju strukturu, sadržaj i formu neprekidno menjaju njegovi korisnici svojim aktivnostima, znanjem i umećem, kao i mnogobrojni automatizovani tehnički sistemi (softverski i hardverski) sopstvenim funkcionisanjem. Sajber prostor ima dinamičnu i rastuću strukturu. Međutim, sajber prostor nije „živ“, već je veštačka tvorevina ljudi i tehničkih sistema, pa se razvija u skladu sa voljom ljudi i unapred definisanim procesima, a ne po prirodnim zakonima. Njegovu dinamiku

[570] Laurie Mcleod and Bill Doolin, „Information Systems Development as Situated Socio-technical Change: A Process Approach,“ *European Journal of Information Systems* 21, no. 2 (2012): 176-191. http://search.proquest.com.nduezproxy.idm.oclc.org/docview/926222149?accountid=12686 (preuzeto 18. avgusta 2015).

ostvaruju procesi razmene podataka između sistema (servisima, protokolima), što se odvija na automatizovan način. U nekim slučajevima identitet izvora tih procesa može ostati anoniman.

Ljudi su direktni kreatori sajber prostora, stvarajući i utičući na njegovu strukturu, sadržaj i procese. Oni to mogu realizovati i indirektno, preko tehničkih sistema, koje su stvorili i napravili da to čine po njihovom naumu. Simboli te organizovane aktivnosti, čiji je cilj ostvarivanje nekakvih zadatka ili koristi, su servisi.[571] Servise izvršava softver, izvođenjem procesa i upotrebom podataka. Dakle, sajber prostor je skup sistema koji se konstantno ili povremeno povezuju ili međusobno komuniciraju razmenom podataka na organizovan način.

[571] Razlikovanje procesa i servisa se može posmatrati u organizacionom i tehnološkom pogledu. U organizacionom pogledu, procese i servise može da omogućava ili pruža isti sistem (provajder). Razlika između procesa i servisa se prvenstveno odnosi na potrebu onoga ko od njih zavisi ili ih koristi (korisnik). Servisi se odnose na očekivani doprinos korisniku, dok su procesi skupovi aktivnosti koje provajder izvršava u cilju postizanja tog doprinosa. U tom smislu, po Strategiji servisa, *Information Technology Infrastructure Library* (ITIL), „servisi su sredstva kojim se doprema vrednost klijentima omogućavanjem onih ishoda koje klijenti žele da ostvare bez prihvatanja specifičnih troškova i rizika“ (str. 13), dok su poslovni procesi struktuirani skupovi aktivnosti, dizajnirani u cilju ostvarivanja specifičnih rezultata, „ograničeni ciljevima, politikama i ograničenjima“ (str. 37). IT servis je servis koji pruža davalac IT usluga, koji se „sastoji od kombinacije tehnologije, ljudi i procesa“ (str. 13). „Proces je struktuirani skup aktivnosti koji je dizajniran da ostvari specifični cilj. Proces uzima jednu ili više definisanih ulaznih vrednosti i pretvara ih u definisane izlazne vrednosti“ (str. 20). Proces na taj način omogućava transformaciju sistema ka cilju, pri čemu koriste povratne informacije za samojačanje i samokorektivnu akciju, funkciju kao zatvoreni sistem.

Information Technology Infrastructure Library (ITIL), *ITIL Version 3 Service Strategy* (Norwich, UK: The Stationery Office, 2011), ftp://83.229.216.22/ITIL/ITIL%20Version%203%20%282011%29/01%20-%20ITIL%20V3%202011%20Service%20Strategy%20SS.pdf, 13, 20 i 37;

Kai Holthausk, *Processess and Services: White Box Versus Black Box*, Third Sky, http://www.thirdsky.com/downloads/ProcessesandServicesDifference.pdf, (preuzeto 20. decembra 2015);

U pogledu funkcionisanja računarskih sistema sa specifičnim procesorskim arhitekturama (na primer *Windows* operativni sistemi), razlikuju se aplikacije, procesi i servisi. Aplikacije su programi koji izvršavaju neku radnju i preko kojih se vrši interakcija korisnika sa računarskih operativnim sistemom. Svaka aplikacija se sastoji od jednog ili više procesa, odnosno izvršnih programa. Procesi kao takvi su posebni nivoi (radnje) određene aktivnosti koja se izvršava od strane aplikacije.

Servisi su specifični, osnovni procesi (ali i aplikacije) operativnog sistema, koji se izvršavaju u pozadini za potrebe funkcionisanja (više) aplikacija koje obavljaju svoju aktivnost u okviru jednog operativnog sistema i koji najčešće ne vrše interakciju sa korisnikom preko interfejsom operativnog sistema. Jedan proces može koristiti više servisa operativnog sistema. U nekim slučajevima i procesi mogu kao pozadinski procesi bez postojanja grafičkog interfejsa prema korisniku, ali tada nisu instalirani u sistemu kao servisi. U drugim slučajevima, aplikacije mogu direktno zavisiti od rada samostalnih servisa koji omogućava operativni sistem, koji nisu deo njihovih procesa. http://www.reviversoft.com/blog/2013/08/processes-and-services-in-windows/

Ljudi, procesi i tehnologija su ujedno i ključni elementi narušavanja informacione bezbednosti. Oni postoje, manifestuju se i organizovani su kroz logičko, fizičko i informaciono područje. Centralni deo sajber prostora su podaci i matematičko-logička pravila i instrukcije (softver), koji se kroz obradu signala i značenje povezuju sa fizičkim i informacionim okruženjem i ljudima. U pogledu međunarodnog prava, moguće je regulisati ljude i njihove postupke u sajber prostoru, ali je teško u praksi efektivno regulisati podatke i matematičko-logičke odnose. Sajber prostor je složeni sistem, koji je proizvod računarskih nauka i inženjerskog rada. Iako je sajber prostor po svojoj početnoj konceptualnoj prirodi označavao „virtuelno – ono što nema materijalnu prirodu“, njegova veza sa fizičkim je višeslojna.

Tabela 7. Osnovni elementi sajber prostora.

<table>
<tr><td rowspan="4">Sajber prostor</td><td>Svojstvo</td><td colspan="2">Element</td><td colspan="2">Vrednost</td><td>Oblik</td></tr>
<tr><td>Struktura</td><td>Informacione tehnologije, Ljudi</td><td>Sistemi</td><td colspan="2">Softver, Hardver, OSI slojevi mreže</td><td rowspan="3">Lokalni vs. Udaljeni Centralizovani vs. Distribuirani</td></tr>
<tr><td>Funkcija</td><td>Konekcija, Mreže Komunikacija,</td><td>Procesi Servisi</td><td>Umreženi, Neumreženi</td><td>Stalna, Povremena</td></tr>
<tr><td>Sadržaj</td><td colspan="2">Podaci, Informacije</td><td colspan="2">Diskretni, Kontinualni</td></tr>
</table>

Informaciono-komunikacione tehnologije imaju dualnu prirodu u pogledu karaktera primenjene tehnologije, koja se može svrstati u dve ključne kategorije:

- **softver** (logičku prirodu) i
- **hardver** (materijalno-fizičku prirodu).

Obe kategorije sistema koriste **ljudi** i drugi **sistemi** za manipulaciju informacijama u sajber prostoru. Sajber prostor ne može postojati bez materijalnog sveta i ljudi. Zajednička veza (u oba smera) i ujedno granica između sajber i fizičkog područja jeste fizička infrastruktura sajber prostora, sačinjena od elemenata koji postoje u fizičkom svetu.

Sajber prostor predstavlja kompleksnu mešavinu, čiji je ključni faktor kohezije softver. Softver omogućava procese i servise koji potiču od direktne interakcije između

informacionih sistema[572], odnosno od posredne interakcije između ljudi i sistema. Imajući to u vidu, postavlja se pitanje, kako je moguć bitan uticaj sajber prostora na nacionalnu bezbednost i odbranu država koji je omogućen samo funkcionisanjem softvera, odnosno značenjem podataka i primenom matematičko-logičkih pravila i instrukcija?

Koncept savremenog borbenog prostora predstavlja područje svih vojnih aktivnosti na kopnu, moru, vazduhu i u svemiru (fizičkom okruženju) i u informacionom području. Sajber prostor treba posmatrati kao presek svih tih područja iz konteksta proizvoda primene informaciono-komunikacionih tehnologija.[573]. Razlog za to ne leži isključivo u moći softvera i matematičkih pravila, već pre u sistemskoj povezanosti različitih područja realnosti od značaja za nacionalnu bezbednost i odbranu kroz uzajamno i međuzavisno delovanje ključnih faktora: ljudi, procesa i tehnologije.

[572] Hardverskih i/ili softverskih

[573] Rossouw von Solms and Johan van Niekerk. "From Information Security to Cyber Security." *Computers and Security* 38, (October 2013): 97-102.

8. SAJBER ORUŽJE

Za razumevanje fenomena sajber sukoba, sajber rata i sajber napada neophodno je prethodno definisati, u smislu međunarodnog prava i tehnologije izrade oružja, pojam „sajber oružje“ i njegove karakteristike, odnosno da li se, i po čemu, razlikuje od oružja u tradicionalnim sukobima.

8.1. Opšte značenje oružja

Čovek oduvek koristi oružja. Tieme[574] navodi da najstariji arheološki identifikovan alat za lov napravljen od organskog materijala[575], drveno koplje nađeno u Nemačkoj, datira iz perioda od pre 400.000 godina. Najstarije otkriveno kameno oruđe koje su koristili primati je napravljeno pre 2,5 miliona godina u Africi[576]. Pretpostavke o upotrebi raznih priručnih alatki i kamenja za bacanje na plen ili drugu stranu se odnose na period od pre 6 miliona godina[577]. Konačno, u sukobima čak i delovi tela mogu biti upotrebljeni kao oružje (npr. rogovi, kopita, ruke, noge) i koristiti kao nekakvo sredstvo za primenu i pojačavanje dejstva sile. Upotreba oružja nije rezervisana samo za ljude. Gudal[578], kao i Pruec i Bertolani[579] navode da šimpanze za lov koriste primitivne alate koje modifikuju i prilagođavaju cilju. Bilo da je reč o ljudima ili životinjama, ova sredstva se koriste aktivno, i sa namerom da onesposobe, ozlede, ili ubiju živo biće, ili da onesposobe, oštete ili unište predmet ili sistem. Složenost i efektivnost tih sredstava zavisi od inteligencije živih bića, njihovog iskustva, odnosno stečenog znanja.

---

[574] Hartmut Thieme, "Lower Palaeolithic Hunting Spears from Germany," *Nature* 385, no. 6619 (1997): 807-810.

[575] Što znači da nije upotrebljen slučajno ili u instiktivno dohvatanjem čvrstog predmeta, već da je svesno i sistematično upotrebljeno i obrađeno sa ciljem da postane instrumen za nasilje (ubijanje ili lov). U tom pogledu, ovakvo oružje se može smatrati primenom tehnologije.

[576] Sileshi Semaw, Paul Renne, John WK Harris, Craig S. Feibel, Raymond L. Bernor, N. Fesseha, and Kenneth Mowbray. "2.5-million-year-old Stone Tools from Gona, Ethiopia," *Nature* 385 (1997): 333-336.

[577] Frank W. Marlowe, "Hunter-gatherers and Human Evolution," *Evolutionary Anthropology: Issues, News, and Reviews* 14, no. 2 (2005): 54-67.

[578] Jane Goodall, "Tool-using and Aimed Throwing in a Community of Free-living Chimpanzees," *Nature* 201 (1964): 1264.

[579] Jill D. Pruetz and Paco Bertolani. "Savanna Chimpanzees, Pan Troglodytes Verus, Hunt with Tools." *Current Biology* 17, no. 5 (2007): 412-417.

Svaka ljudska kultura koristi bar jedan pojam koji označava oružje, koji često ima široko značenje. Po *Oksfordskom rečniku* pojam „oružje“ (eng. *weapon*) obuhvata „instrument bilo koje vrste, upotrebljen u ratovanju ili u borbi radi napada i savladavanja neprijatelja“[580]. Ova definicija ističe postojanje cilja pri primeni oružja u svrhu savladavanja protivnika, što, u suštini, predstavlja vođenje sukoba. Međutim, nije svako oružje sredstvo kojim se vodi sukob ili rat. Po ovom rečniku pojam oružje ima i drugo značenje, kao „sredstvo kojim se ostvaruje prednost ili se neko brani u sukobu ili takmičenju“[581]. *Meriam-Vebster* rečnik, oružje definiše kao „nešto što se koristi za borbu ili napad na nekoga ili za vlastitu odbranu kada neko napada“, odnosno „nešto (poput veštine, ideje ili alata) što je upotrebljeno da se pobedi u takmičenju ili da se nešto postigne“[582]. U *Rečniku srpskohrvatskoga jezika Matice Srpske* termin „oružje“ obuhvata bilo koje oruđe (sredstvo) za napad ili odbranu, uključujući sopstveni deo tela i opreme ili neki eksterni instrument, čija osnovna svrha ne mora biti povezana sa aktom napadanja i sa ciljem da se ozledi ili ubije protivnik, odnosno da se uništi ili onesposobi objekat napada[583].

Ove definicije, koje su opšteg značenja, tretiraju oružje kao nešto, sredstvo, instrument, kojim se izvršava napad, ili koje se u funkcionalnom pogledu koristi da se ostvari neki cilj vezan za sukob ili borbu sa drugom stranom. Taj cilj je povezan sa efektima dejstva oružja, odnosno povređivanjem, ubijanjem, oštećivanjem, uništenjem ili onesposobljavanjem osoba, živih bića, tehničkih sistema ili objekata (retrospektivno), pri čemu je dovoljno da ostvari bar neka od sposobnosti napadača, odnosno bar neki od efekata na cilj.

---

[580] *Oxford English Dictionary*, s.v. „weapon“, http://www.oed.com.nduezproxy.idm.oclc.org/view/Entry/226597?rskey=Hbtkn3&result=1&isAdvanced=false#eid, (preuzeto 10. januara 2016).

[581] *Oxford Dictionaries Online*, s.v. „weapon“, http://www.oxforddictionaries.com/definition/american_english/weapon (preuzeto 22. decembra 2015).

[582] *Merriam-Webster Dictionary*, s.v. „weapon“, http://www.merriam-webster.com/dictionary/weapon (preuzeto 22. decembra 2015).

[583] Oružje je oruđe za napad i odbranu, ubojno sredstvo; Oruđe je predmet podešen za vršenje nekog rada, naprava, alat(ka). *Rečnik srpskohrvatskoga književnog jezika, Drugo fototipsko izdanje*, 1990., knjiga prva A-E, (Novi Sad, Zagreb, 1967), 193.

8.2. Definicije sajber oružja u međunarodnoj zajednici

U međunarodnoj zajednici ne postoji mnogo definicija pojma „sajber oružje“. Pri tome, države i međunarodne organizacije svoje definicije ne zasnivaju na istim principima i kriterijumima. Tako, na primer, *Organizacija za ekonomsku saradnju i razvoj* (OEBS) definiše sajber oružje na sledeći način:

> „Sajber oružje obuhvata: neautorizovan pristup sistemima („haking“), viruse, crve, trojance, napade uskraćivanjem servisa[584], distribuirane napade uskraćivanjem servisa, rutkite i upotrebu socijalnog inženjeringa. Rezultati napada mogu uključivati: narušavanje poverljivosti/krađu tajni, krađu identiteta, narušavanje veb-prezentacija, ucenu, preuzimanje sistema ili blokiranje servisa. Sajber oružje se upotrebljava individualno, u kombinaciji i simultano sa konvencionalnim „kinetičkim“ oružjima, kao multiplikator njihove moći. Pouzdano se može predvideti da će sajber oružje uskoro postati sveprisutno“[585].

Ovo određenje obuhvata nabrajanje (određenih) vrsta sredstava i tehnika sajber napada i njihovih ciljeva, zbog čega se ne može smatrati potpunom. Nabrajanje postojećih vrsta zlonamernih sistema, metoda i tehnika napada ne može pružiti dobar osnov za definisanje pojma ili kategorije sajber oružja. Konačno, tehnologija sajber napada se brzo menja i njen razvoj dovodi do pojave novih sistema i tehnika, kao i do različite kombinacije postojećih. Opšti karakter pojma se ne može uspešno definisati prostim nabrajanjem njegovih pojavnih elemenata, jer takav postupak ne opisuje njegovu prirodu. Definicija, međutim, navodi mogućnost kombinacije upotrebe informacionih sistema i tradicionalnih sredstava napada i predviđa budući razvoj sajber oružja u skladu sa razvojem tehnologija.

Tokom prethodne decenije u okviru tela i organa UN, posebno u okviru nadležnosti Generalne skupštine, **Kancelarije za razoružanje** (eng. *UN Office for Disarmament Affairs* - UNODA) i rada **Grupe vladinih eksperata** (eng. *Group of Governmental*

[584] Denial-of-service (DoS) – vrsta računarskog napada pri kome se mrežni i računarski resursi (procesorsko vreme, procesorska snaga, mrežni protok, dostupnost servisa) čine nedostupni autorizovanim korisnicima (sistemima, procesima, servisima, licima). Poseban oblik ovih napada su distribuirani DoS napadi (eng. *Distributed Denial of Service Attack* – DdoS), pri kojima napad istovremeno izvršava mnoštvo napadača različitim kanalima napada.

[585] Peter Sommer and Ian Brown, „Reducing Systemic Cybersecurity Risk“, *OECD/IFP Project on Future Global Shocks* (2011), http://www.oecd.org/governance/risk/46889922.pdf, 6.

Experts - GGE), u periodu od 1999. godine, pojedine države su u okviru vlastitih predloga za rezolucije nudile i definicije pojma „sajber oružje“.

Tako, u predlogu Rusije za usvajanje rezolucije Generalne skupštine UN koja se odnosi na informacionu bezbednost u međunarodnim odnosima ne pominje se termin „sajber oružje“, već „informaciono oružje“, ali u smislu sličnom opštem značenju sajber oružja. Po ruskom predlogu, informaciono oružje su: „Sredstva i metode upotrebljene sa ciljem nanošenja štete **informacionim resursima, procesima i sistemima** drugih država; upotreba informacija sa ciljem narušavanja državne odbrane, administrativnih, političkih, društvenih, ekonomskih i drugih vitalnih sistema, kao i masovna manipulacija državne populacije sa ciljem destabilizacije društva i države“[586]. Iako navedena definicija u skladu sa političkim opredeljenjem ove zemlje, spaja različite koncepte sukoba u sajber prostoru i sukoba u informacionom prostoru u jedan zajednički, ona pruža važne stavove: sajber oružje čine podjednako sredstva i metode (koje nemaju materijalnu prirodu), a ciljevi na koje navedeno oružje dejstvuje su informacioni resursi, procesi i sistemi.

Stav Rusije o prirodi informacionog oružja na sledećem zasedanju Generalne skupštine je delimično izmenjen: „Načini i sredstva upotrebljeni sa ciljem oštećivanja državnih informacionih resursa, procesa i sistema, vršenjem neprijateljskog uticaja, primenom informacija, na odbrambene, administrativne, političke, društvene, ekonomske i druge vitalne sisteme države, kao i masovna psihološka manipulacija populacije u cilju destabilizacije društva i države“[587]. Evolucija navedene definicije je pokazala da se ona gotovo u potpunosti odnosi na sukobe u informacionom području, a ne na sukobe u sajber prostoru i da se stoga više tiče neoružanih oblika agresije između država, a manje sajber ratovanja.

Jedanaest godina kasnije, u *Konceptu aktivnosti Oružanih snaga Rusije u Informacionom prostoru*, koji je izradilo Ministarstvo odbrane, ponuđena je znato opštija definicija informacionog oružja. Po toj definiciji informaciono oružje čine: „Informacione

[586] Russia, Submission to the United Nations General Assembly Resolution G.A. Res. 54/213, U.N. Doc. A/RES/54/213 (August, 10, 1999), https://disarmament-library.un.org/UNODA/Library.nsf/f4c497d5f90e302d85257631005152d2/fae7e8060174f22c8525764e0051ce60/$FILE/A-54-213.pdf, 10.

[587] Russia, Submission to the United Nations General Assembly Resolution G.A. Res 55/140, U.N. Doc A/RES/55/140, (July 10, 2000), http://www.un.org/documents/ga/docs/55/a55140.pdf, 3-4.

tehnologije, sredstva i metode upotrebljeni u svrhu informacionog ratovanja“[588]. Iako se čini suviše opšta, navedena definicija izgleda i kao najpreciznija u pogledu (informacionih) sukoba, pošto dopušta da svako adekvatno sredstvo pogodno za informacioni napad bude ujedno i oružje. Pri tome treba imati u vidu rusko političko opredeljenje da u prvi plan ističe informacione, a ne sajber sukobe i ratovanje.

U Kubi preovlađuje slično mišljenju ruskom, po kome se sajber i informacioni napad smatraju jedinstvenim skupom aktivnosti: „Informacioni i komunikacioni sistemi mogu postati oružje kada su dizajnirani ili upotrebljeni da izazovu oštećenje državne infrastrukture. Na primer, napadanje nacionalnih mreža upotrebom softvera iz inostranstva ili iz izvora unutar države, ali promovisanog ili osmišljenog u inostranstvu; radio-televizijsko emitovanje sa namerom narušavanja društvenog reda i institucionalnog okvira koji proističe iz ustava druge države kojoj su navedeni signali upućeni; aktivnosti sa ciljem ometanja, narušavanja ili paralisanja radio-emiterskih servisa drugih država itd“ [589]. Iako se navedena definicija sa primerima više odnosi na upotrebu elektronskih medija u svrhu neoružanih sukoba, značajno je naglašavanje da sistemi mogu biti oružje ukoliko su namenjeni ili ukoliko su upotrebljeni za napad, iako nisu inicijalno dizajnirani za izvođenje napada.

Filipinska definicija informacionog oružja je vrlo opšta: „Informacioni resursi koji su strategijski razvijeni ili kreirani u cilju informacionog ratovanja ili za izazivanje štete, konfuzije ili nedostataka, ili bilo kog drugog oblika zlonamernog cilja“[590].

[588] Министерство обороны Российской Федерации (Минобороны России), *Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве* (2011), http://ens.mil.ru/science/publications/more.htm?id=10845074@cmsArticle (preuzeto 18. mart 2015).

[589] Cuba, Submission to the United Nations General Assembly Resolution G.A. Res 58/373, U.N. Doc A/RES/58/373 (September 17, 2003), https://disarmament-library.un.org/UNODA/Library.nsf/c793d171848bac2b85256d7500700384/b69c21ea9dcbb95785256dc10058b4c9/$FILE/sg58.373.pdf, 5.

[590] Philippines, Submission to the United Nations General Assembly Resolution G.A. Res 56/164, U.N. Doc A/RES/56/164 (July 3, 2001), http://www.un.org/documents/ga/docs/56/a56164.pdf, 4.

Po predlogu Španije, informaciono oružje se smatra upotrebom Interneta kao oružja, to jest, kao sredstva upućivanja napada protiv informacionih sistema kritične infrastrukture ili same infrastrukture Interneta“ [591].

Konačno, jedna od najtačnijih i najobuhvatnijih definicija sajber oružja je rezultat zajedničkog rada zapadnih i ruskih eksperata u oblasti informacione bezbednosti u okviru projekta *EastWest* Instituta, po kojoj je sajber oružje: „Softver, firmver ili hardver koji je dizajniran ili primenjen da izazove štetu kroz sajber prostor“[592].

Navedene definicije su prilično raznolike i suštinski se razlikuju, pri čemu treba imati u vidu i da su predložene u različitim vremenskim periodima.

8.3. Uticaj karaktera savremenih sukoba na shvatanje pojma „sajber oružje“

Sukobi u sajber prostoru se sprovode izvođenjem sajber napada. Njihovo primarno sredstvo (oružje) i ciljevi su informacioni sistemi i procesi. Primena informaciono-komunikacionih tehnologija u savremenim društvima je opšta i sveobuhvatna. Njihov značaj za funkcionisanje ljudi, sistema i procesa je veliki i znatan. Informacioni sistemi se široko i intenzivno koriste i u vojnim i u civilnim organizacijama. U društvu se informaciono-komunikacione tehnologije koriste za sve savremene funkcije (trgovinu, funkcionisanje finansijskog i bankarskog sistema, javnu upravu, medije i informisanje, izborni proces, privredu i druge), uključujući i one od kritične važnosti za bezbednost i odbranu. Upravljanje svim savremenim sistemima kritične nacionalne infrastrukture je zasnovano na IKT. Vojne organizacije koriste informacione i telekomunikacione sisteme kao osnovu procesa komandovanja, podrške i izvođenja vojnih operacija. Dakle, sajber oružje i sajber napad su koncepti koje je potrebno analizirati zajedno, pošto je njihova priroda povezana na nivou istih tehnologija, i u okviru istog procesa vođenja sukoba u sajber prostoru.

Praktičan način da se razume priroda sajber sukoba i ratovanja je primena analogije sa

[591] Spain, Submission to the United Nations General Assembly Resolution G.A. Res 64/129, U.N. Doc A/RES/64/129/Add.1 (January 28, 2010), http://www.unhcr.org/4b8fd5889.html, 10.

[592] James B. Godwin III, Andrey Kulpin, Karl Frederick Rauscher and Valery Yaschenko, eds., *Russia-U.S. Bilateral on Cybersecurity: Critical Terminology Foundations 2* (New York, NY: The EastWest Institute, 2014), 56.

sukobima i ratovanjem u fizičkom okruženju. Svako sredstvo koje učesnici sukoba koriste da izvrše destruktivno dejstvo na cilj dejstva je oružje. Cilj primene oružja je onesposobljavanje funkcije cilja, povređivanje ili uništavanje, odnosno degradiranje njegovih svojstva ili sposobnosti. Posledice destruktivnog dejstva na cilj mogu imati privremen ili trajni karakter. Dakle, **oružje** *je instrument kojim se primenjuje sila nad ciljem dejstva radi destruktivnog ili onesposobljavajućeg efekta*.

Po Intokiji i Muru[593] oružje predstavlja instrument ili sredstvo za vođenje borbe, pri čemu nije bitno da li je ta borba ofanzivna ili defanzivna. Ovakvo shvatanje se bazira na primeni oružja u toku **procesa** borbe. Oni smatraju da se primena Međunarodnog prava oružanih sukoba treba direktno povezati sa nasilnom upotrebom naoružanja. Ovakvo shvatanje se zasniva na činjenici da su ljudi oduvek u sukobima koristili ubojitu, ali i neubojitu manifestaciju sile. Priroda savremenih sukoba više nije takva da se dve sukobljene strane u ograničenom vremenu i na ograničenom prostoru, oružano suprotstavljaju jedna drugoj do konačne pobede. Savremeni sukobi se vode u kontinuitetu, primenom mnogobrojnih, oružanih i neoružanih aktivnosti. I vojno najmoćnije države pre primene oružane sile dugotrajno i temeljno neoružano onesposobljavaju protivnika i utiču na okruženje. Tek nakon političkih, diplomatskih, medijskih, informacionih, ekonomskih, pravnih, specijalnih i prikrivenih aktivnosti vrše dejstvo oružanom silom, a i tada to čine u ograničenom vremenu i precizno. U savremenim sukobima se teži povećanoj efikasnosti, pa su oni stoga asimetrični, hibridni, nelinearni, informacioni ili sveobuhvatni, sa ciljem da efektnije, efikasnije, brže, lakše i ekonomičnije dovedu do pobede u sukobu. Zbog toga se koncept ratovanja između država sve više transformiše u koncept sukoba, koji latentno i u kontinuitetu traje.

Sve velike vojne sile su razvile ili prihvatile neki specifičan koncept sukoba, koji je zasnovan na određenim osnovama. Na primer, SAD su od kraja Hladnog rata razvile koncept dejstva na centar gravitacije protivnika, primenom mrežnocentričnog i

[593] Gregory F. Intoccia and Joe Wesley Moore, „Communications Technology, Warfare, and the Law: Is the Network a Weapon System," *Houston Journal of International Law*, 28 (2006): 467-473.

nelinearnog ratovanja, koji zahteva široku i intenzivnu primenu umrežavanja i informacionih tehnologija i organizaciju vlastite strukture kao "sistema sistema"[594].

Koncept neograničenog ratovanja kineskih oficira Liangu i Ksiangšuiu[595], pominje veći broj specifičnih oblika međunarodnih sukoba, kao i mogućih metoda njihove kombinacije. Po njima, države vode trgovačke i finansijske ratove; mogu davati podršku terorističkim organizacijama da napadaju njihove protivnike[596]; preduzimaju tehnološki zasnovane postupke da utiču na prirodno okruženje i resurse, poput kontrole toka reka i vremenskih prilika, pa čak pokretanja ploča na Zemljinoj kori ili stvaranja ozonskih rupa u atmosferi; kulturnim ratovima utiču na civilizacijske vrednosti nacije[597]; ratuju trgovinom narkoticima; vode medijsko ratovanje; primenjuju tehnološko ratovanje; ratuju pristupom i vrednošću prirodnih resursa[598]; mogu voditi trgovinsko ratovanje kojim se narušava funkcionisanje nacionalnog tržišta; primenjuju mrežno ratovanje uz primenu informacionih sistema[599]; ratuju primenom međunarodnog prava[600], pa čak i manipulacijom ekonomskom pomoći, kojim se određena država dovodi u podređen i zavistan položaj u odnosu na donatora[601]. Metode sukoba između nacija se mogu kombinovati na nadnacionalnom nivou; na naddomenskom nivou, primenom

[594] Arthur K. Cebrowski, and John J. Garstka. "Network-centric warfare: Its origin and future," *US Naval Institute Proceedings*, 124, no. 1 (1998): 28-35.

[595] Qiao Liang and Wang Xiangsui, *Unrestricted Warfare* (Beijing: PLA Literature and Arts Publishing House, 1999).

[596] Kao što, na primer, SAD godinama optuživali Libiju, Iran, Irak, Avganistan da čine, ili Venecuela i Kuba to činile u odnosu prema SAD.

[597] U tom pogledu poznat je slučaj naglog povećanja broja satelitskih televizijskih stanica u državama u kojima žive pripadnici arapske nacije na Bliskom istoku, preko kojih su emitovani sadržaji neprihvatljivog sadržaja za moral arapske nacije, poput pornografije.

[598] Nagli pad cena nafte na svetskom tržištu uvek može biti posledica međunarodnih tržišnih odnosa, ali i posledica sračunate političke odluke. Na primer, naglo smanjenje cena nafte sa oko 120 na manje od 30 dolara po barelu moguće je izvesti i veštačkim putem, političko-ekonomskim špekulacijama i tajnim diplomatskim dogovorom članica organizacije proizvođača nafte, s ciljem da se ekonomski naudi trećoj strani, čiji je budžet velikim delom zasnovan na projektovanoj većoj ceni nafte. Posledice u konačnom ishodu mogu biti slične oružanoj akciji. Kao posledica ekonomskog gubitka prihoda može doći do ekonomske krize koja vodi ka političkim promenama vlasti (što se na primer desilo Venecueli i preti Rusiji).

[599] Koje je od tada preraslo u sajber ratovanje.

[600] Kada se, na primer, neka država u međunarodnoj zajednici posredno označi zločinačkom, jer se naizgled legitimnim sudskim odlukama naruši ravnoteža u odnosu na broj i težinu počinjenih dela u odnosu na druge učesnike sukoba, iz čega proističu buduće političke i ekonomske posledice po tu državu.

[601] Liang and Xiangsui, *Unrestricted warfare*.

istovremenog dejstva u više područja; primenom više sredstava, sukoba, na različitim nivoima sukoba po intenzitetu i operativnom značaju[602].

Drugi autori smatraju da je nezavisno od nastojanja država, sam uticaj tehnologije na ljudsko društvo doveo do promene načina vođenja sukoba, nazivajući ga "Sukobom četvrte generacije"[603]. Virilio i Tofler[604] se pridružuju ovoj oceni značaja tehnologije za prirodu sukoba, naglašavajući da vojnu pobedu u savremenim sukobima ostvaruju oni protivnici koji su u stanju da duže, jače i dalje utiču na suparnika, odnosno oni koji ostvare veću brzinu vojnog delovanja[605, 606].

Osnovna karakteristika savremenih ratova je, po ruskom ministru odbrane Gerasimovu[607], kao i po više zapadnih autora[608, 609], optimizacija efekata dejstva na protivnika koja nastaje usklađivanjem različitih oblika, sadržaja, intenziteta i redosleda primene vojnih i nevojnih dejstava na protivnika, kao i asimetričnost sukoba[610].

Međutim, kako navodi Ečevarija[611], bilo bi pogrešno smatrati da se navedene forme sukoba pojavljuju tek u savremenom dobu i da su nastale isključivo pod uticajem savremenih tehnologija, poput informaciono-komunikacionih. Optimizacija sinergijskog efekta zajedničke primene različitih formi sukoba, maksimizacija efekata njihovog

---

602 Liang and Xiangsui, *Unrestricted warfare*.

603 William S. Lind, Keith Nightengale, John F. Schmitt, Jospeh W. Sutton, Garry I. Wilson, "The Changing Face of War: Into the Fourth Generation", *Marine Corps Gazzette*, 73, no. 10 (1989): 22-26, https://www.mca-marines.org/files/The%20Changing%20Face%20of%20War%20-%20Into%20the%20Fourth%20Generation.pdf (preuzeto 18. oktobra 2015).

604 Alvin Toffler and Heidi Toffler, *War and anti-war: Survival at the dawn of 21st century* (New York, NY: Warner Books, 1995), 30.

605 Paul Virillio, *Speed and Politics* (New York, NY: Semiotext(e), 1977 [2006]).

606 Paul Virillio, *Information Bomb* (London, UK: Sage, 2000).

607 Valerii Gerasimov, "Cennost' Nauki v Predvidenii [The Value of Science in Foresight]" *Voyenno-Promyshlennyy Kuryer*, February 27, 2013, http://www.vpk-news.ru/articles/14632 (preuzeto 12 novembra 2015).

608 Peter Pomerantsev, "How Putin is Reinventing Warfare," *Foreign Policy*, May 5, 2014, http://foreignpolicy.com/2014/05/05/how-putin-is-reinventing-warfare/ (preuzeto 12 novembra 2015).

609 Russel W. Glenn, „Thoughts on "Hybrid" Conflict," *Small Wars Journal*, http://smallwarsjournal.com/blog/journal/docs-temp/188-glenn.pdf (preuzeto 10. oktobra 2015).

610 David L. Buffaloe "Defining Asymmetric Warfare" *The Land Warfare Papers, Institute of Land Warfare* 58 (2006): 1-34. https://www.ausa.org/SiteCollectionDocuments/ILW%20Web-ExclusivePubs/Land%20Warfare%20Papers/LWP_58.pdf (preuzeto 12 novembra 2015).

611 Antulio J. Echevarria II, „Fourth-Generation War and Other Myths", *Strategic Studies Institute* (November 2005): 9-14.

dejstva na protivnika u odnosu na uloženi napor u primeni sile, i primena različitih vrsta dejstva u cilju nasilnog nametanja volje protivniku je oduvek postojalo tokom duge istorije civilizacije. Pojedina carstva, na primer Vizantijsko, su tradicionalno vekovima primenjivala metode i tehnike koje se danas nazivaju informaciono ratovanje[612], dok se trgovinsko i ekonomsko ratovanje primenjivalo još u antičko doba[613]. Sukobi su deo ljudske prirode, a društva su ih oduvek vodila u skladu sa svojim iskustvom, veštinama, znanjima i raspoloživim resursima. Tako ih i danas vode u skladu sa novim tehnologijama i društvenim odnosima.

Korišćenju nevojnih i specifičnih instrumenata primene sile nad protivnikom, kakve su ekonomske sankcije, manipulacija proizvodnjom nafte ili zloupotreba međunarodnog prava ne može se dodeliti status oružja. Međutim, sa primenom napada u sajber prostoru treba biti pažljiv. Priroda ove vrste sukoba je drugačija. U kontekstu utvrđivanja prirode sajber ratovanja i analize međunarodnog regulisanja njegove primene, neophodno je utvrditi šta je sajber oružje u smislu instrumenta kojim se ostvaruje negativno dejstvo i šta predstavlja primena sile nad protivnikom u sajber prostoru.

8.4. Mogućnost napada na informacione sisteme

Sajber ratovanje podrazumeva vođenje sukoba između nacija u sajber prostoru (primenom IKT). Priroda sajber ratovanja primarno zavisi od primene informaciono-komunikacionih tehnologija i zato se mora pre svega objasniti analizom sa tehnološkog aspekta, a tek zatim i iz pravnog društvenog, vojnog ili ekonomskog.

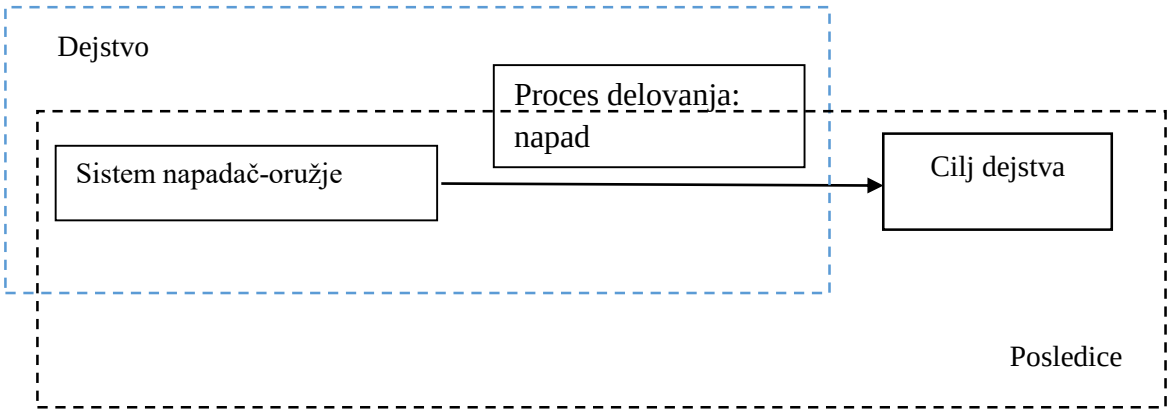
Primenom tradicionalnog oružja, ostvaruju se direktni efekti dejstva u fizičkom okruženju. U zavisnosti od prirode oružja, **dejstvo** može biti **hemijsko**, **biološko** ili **fizičko** (mehaničko, toplotno, talasno, elektromagnetno, radiološko ili kombinovano)[614]. Rezultat dejstva po relaciji može biti direktan ili indirektan, a po učinku onesposobljavajući, ubojni ili razorni uticaj na ljude, sisteme, objekte, okolinu ili procese.

[612] John Arquilla and Douglas A. Borer, eds., *Information strategy and warfare: A guide to theory and practice*, (London, UK: Routledge, 2007), 3.

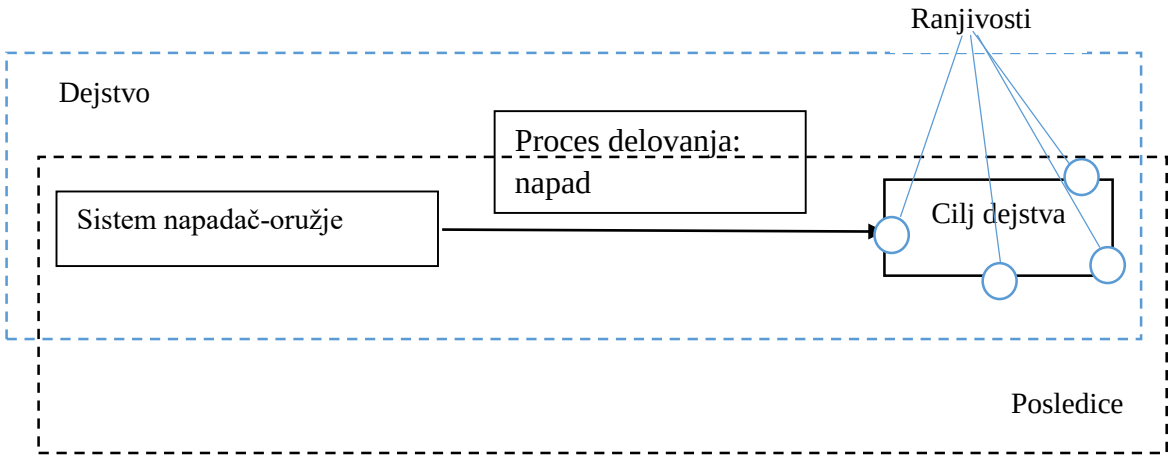
[613] Gary Clyde Hufbauer, Jeffrey J. Schott, and Kimberly Ann Elliott, *Economic sanctions reconsidered: History and current policy Vol. 1* (Washington, DC, Institute for International Economics, 1990), 4.

[614] Dragan Mladenović, „International Legal Regulation of Cyber Conflict: Problems and a Proposed Solution“ (Capstone paper, National Defnse University, Information Resources Management College, 2015), 16.

Pri tome oružje uvek manifestuje silu na cilj u skladu sa svojim kapacitetom, a ne prirodom cilja. Moć dejstva sajber napada na cilj nije apsolutna, kao u slučaju primene tradicionalnog naoružanja[615], već je relativna u odnosu na skup ranjivosti[616] napadnutog sistema.



a) Fizičko okruženje



b) Sajber prostor

Slika 20.Grafički prikaz različitog uticaja dejstva na cilj u odnosu na njegovu prirodu tokom fizičkog i sajber napada.

[615] Pod tradicionalnim naoružanjem u ovom radu smatra se svako naoružanje (konvencionalno ili nuklearno) izvan skupa metoda, tehnika i sistema za preduzimanje sajber napada

[616] Skup svih ranjivosti nekog sistema u informacionoj bezbednosti predstavlja takozvanu „površinu napada“.

Relativnost moći sajber napada se može predstaviti apstraktnom logičkom predstavom. Tokom oružane borbe na sukobljenim stranama su naoružane organizovane borbene jedinice. Dejstvom oružja na cilj uvek se oslobađa ista količinu destruktivne energije bez obzira na vrstu cilja i zaštitu koju cilj poseduje. Na primer, moć dejstva tenka zavisi od dometa i preciznosti topa, kao i od eksplozivne moći granate. Što cilj ima veću zaštitu, efekti dejstva oružja na njega će biti manji, ali sila kojom oružje deluje je ista. Tokom oružane borbe više pojedinačnih učesnika na sukobljenim stranama kumulativno se sabiraju pojedinačna dejstva mnoštva pojedinaca, oružja i oruđa, organizovanih u naoružane jedinice. Više bojeva sačinjava bitke, a one operacije, koje čine rat. U ratu, u seriji sukcesivnih i naizmeničnih borbenih dejstava suprotstavljenih strana u sukobu, pobeđuje ona strana koja ima veće resurse za vođenje naoružanja, bolje vlada veštinom vođenja sukoba i nalazi se u povoljnijoj situaciji u borbenom okruženju. Situacija sajber ratovanja nije takva. Učesnici u sukobima nisu naoružani, niti moraju biti organizovani u borbene jedinice. Dovoljno je da imaju cilj i interes da deluju na protivničke sisteme, da raspolažu sa informacijama o ranjivostima informacionih sistema protivnika i znanje kako da otkriju i iskoriste te ranjivosti u cilju neovlašćenog upada u protivničke informacione sisteme i naknadnog dejstva. Sajber napad zavisi od postojanja ranjivosti u ciljanom sistemu, od sposobnosti da je napadač iskoristi za neovlašćeni i prikriveni upad u sistem i znanja da se kreira skup instrukcija kojim će se ostvariti dejstvo na protivnički sistem. Ukoliko nema ranjivosti ili informacija o njoj, i ukoliko napadač ne raspolaže sa neophodnim znanjem kako da iskoristi otkrivenu ranjivost, napad se ne može izvesti. U tom pogledu, oružje u tradicionalnom fizičkom sukobu se može uporediti sa posedovanjem informacija, znanjem i veštinom da se ono iskoristi. Iako se za sajber napade često koristi pripremljeni softver (malver) suština sajber napada nije u malveru kao proizvodu, već u specifičnoj organizaciji, znanju i veštini da se ostvari napad. Svaki sajber napad je, dakle, proces koji se sastoji od pronalaženja i iskorišćenja ranjivosti u napadnutom sistemu i ostvarivanja željenih efekata na cilj.

Nasuprot tradicionalnom oružju, direktno dejstvo sajber napada se uvek manifestuje u logičkom području, na informacije i informacione sisteme (softver, hardver i procese). Indirektno dejstvo se može ostvariti na ljude, sisteme i procese u bilo kom području

manifestacije sajber prostora (fizičkom, logičkom ili saznajnom)[617]. Logički nivo je centralni sloj sajber prostora koga čine podaci, sistemi, relacije i procesi, predstavljene logičkim instrukcijama, odnosno softverom. Zbog toga je neophodno utvrditi kako se ostvaruje napad na softver.

8.5. Ranjivosti kao ključni faktor sajber napada

Ranjivosti su nedostaci, mane, greške ili neusklađenosti koje omogućavaju sajber napad. One otvaraju prostor narušavanju informacione bezbednosti i ključni su faktori koji omogućavaju agentima pretnje da pokreću sajber napade. Njih ne čine samo softverske greške u logičkom okruženju sajber prostora, već svi mogući interni, eksterni i funkcionalni faktori tokom upotrebe sistema na bilo kom nivou sajber prostora (logičkom, fizičkom i kognitivnom).[618]

Nisu sve aktivnosti ugrožavanja informacione bezbednosti ujedno sajber napadi, niti su sve ranjivosti informacione prirode. Treba razlikovati ranjivosti od samog procesa sajber napada, pošto se sajber napadi odnose samo na one agresivne aktivnosti koje se pokreću upotrebom informacionih sistema[619] i čiji su primarni ciljevi informacioni sistemi[620].

Ranjivosti mogu biti tehničke, društvene, organizacione, pravne, ekonomske i druge prirode (Tabela 8). Osnov za pokretanje napada može biti ranjivost u jednom području ili kombinacija ranjivosti različite prirode i porekla. Skup svih ranjivosti napad čine takozvanu površinu napada (eng. *attack surface*).

Upotreba informacionih tehnologija se širi, pri čemu tehnologije postaju sve složenije, što povećava ukupan broj ranjivosti. Samim tim se povećava i broj i ozbiljnost mogućih sajber napada. Pojavom novih tehnologija i nedostataka u njima dešava se evolucija sajber napada. Novi koncepti poput manipulacije velikim količinama podataka, kvantnog računarstva, opšte umreženosti, distribuirane proizvodnje sredstava omogućene

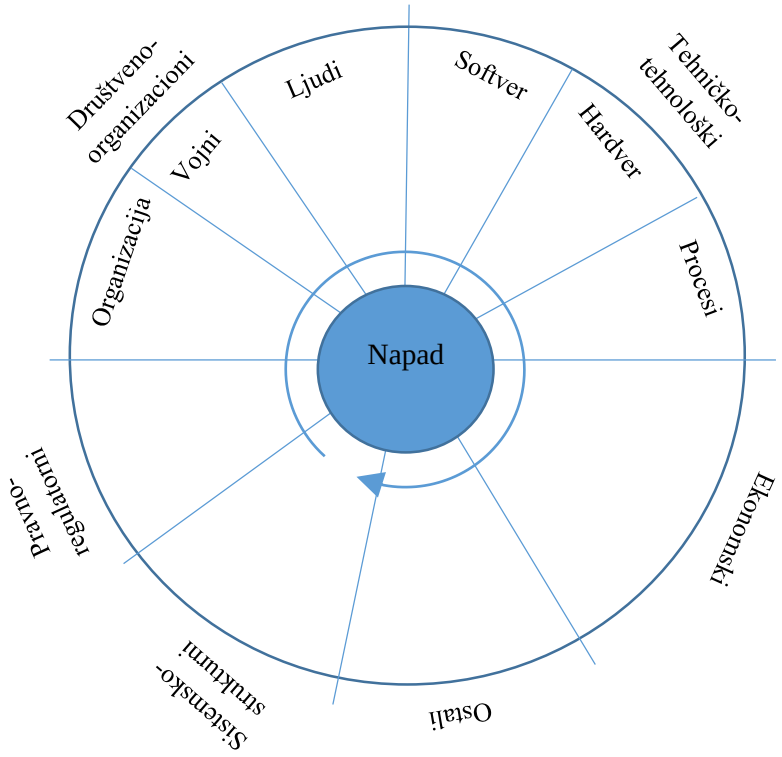
[617] Dragan Mladenović, „International Legal Regulation," 16.

[618] Mladenović, *Međunarodni aspekt sajber ratovanja*, 60.

[619] Irving Lachow, "Cyber Terrorism: Menace or Myth?" in *Cyberpower and National Security*, eds., Franklin D. Kramer, Stuart H. Starr and Larry Wentz, 437-464 (Washington DC: Potomac Books, 2009), 5.

[620] Oona A. Hathaway et al., "The Law of Cyber-Attack," *California Law Review* 100, no. 4 (2012): 817-885, 823.

informacionim tehnologijama, robotike i veštačke inteligencije, donose nove oblike sajber napada i nove mogućnosti sajber napadača. Ipak, svi oni se nalaze u osnovi informacione bezbednosti, pa se sajber ratovanje može nazvati i primenom informacione bezbednosti u svrhu vođenja sukoba.



Slika 21. Moguća područja porekla ranjivosti informacionih sistema.

Sajber napadi se odvijaju u sajber prostoru, pri čemu su ključni element koji ih omogućavaju i ključna mesto napada ranjivosti u logičkom sloju sajber prostora - softveru.

Tabela 8. Mogući izvori nedostataka koji mogu postati ranjivosti pogodne za pokretanje sajber napada.

Tehnički	Društveno-organizacioni	Sistemsko-strukturalni	Pravno-regulatorni	Ekonomski
Softverski	Individualni (svest, znanje, odgovornost, podložnost uticaju i greškama, namera…)	Struktura sistema	Nadležnost/ Jurisdikcija	Resursi
Hardverski	Društveni (kultura, sistem, interesi, političke odluke…)	Hijerarhija/arhitektura (na primer, arhitektura Interneta)	Sadržaj i relevantnost pravila i propisa	Poslovna orjentacija
Procesni	Vojni (strategija, operatika, taktika, vojna veština, izbor sredstava i metode borbe, izbor ciljeva…)	Odnosi/relacije između elemenata i podsistema	Međunarodni sporazumi	
Orjentisani na podatke (oblik zapisa, dostupnost podataka, integritet)…		Način funkcionisanja protokola, servisa i sistema (BGP, DNS, …)	Mogućnost detekcije napada	
Orjentisani na bezbednost (kontrola pristupa, primena kriptografije…)			Mogućnost identifikacije i atribucije napadača, Utvrđivanje odgovornosti države	

8.6. Softver kao izvor ranjivosti

Svi savremeni tehnički sistemi su rastuće zavisni od funkcionisanja informaciono-komunikacionih tehnologija. Ove tehnologije se konstantno ugrađuju u sve tehničke sisteme sa ciljem da im se unapredi funkcija, dograde nove funkcionalnosti ili produži životni ciklus upotrebe. Paralelno sa tim trendom, raste složenost ugrađene tehnologije i sposobnost umrežavanja sa drugim sistemima i okruženjem.

Softver predstavlja integralni deo svakog informacionog sistema. To je centralni deo logičkog sloja sajber prostora i povezuje taj sloj sa fizičkim slojem (sistemima/hardverom, procesima i ljudima) i kognitivnim slojem (značenjem i razumevanjem informacija, znanjem i kreativnim mišljenjem od strane ljudi i inteligentnih sistema). Ključne karakteristike softvera u skladu sa ISO/IEC 9126 standardom[621] su: funkcionalnost, pouzdanost, upotrebljivost, efikasnost, lakoća održavanja, portabilnost (Tabela 9). Po navedenom standardu, bezbednost softvera je direktno svojstvo (podkarakteristika) njegove funkcionalnosti i preko nje utiče na ukupni kvalitet softvera. To znači da napadači zloupotrebom grešaka i nedostataka u softveru i njegovoj implementaciji, funkcionisanju i interakciji utiču na bezbednost softvera (pri čemu greške postaju ranjivosti) i tako direktno utiču na funkcionalnost softvera. Bezbednost softvera se sastoji od bezbednosti aplikacije i bezbednosti podataka. Prva se ostvaruje mehanizmima prevencije slučajnog ili namernog neovlašćenog pristupa sistemskoj funkcionalnosti, koji omogućava sam sistem ili treća strana. Druga se ostvaruje mehanizmima pristupa podacima pohranjenim, poslatim ili primljenim od strane sistema[622].

---

[621] *ISO/IEC 9126-1:2001, Software engineering -- Product quality -- Part 1: Quality model.*

Napomena: Ovaj standard više nije važeći, jer je povučen i zamenjen je standardom ISO/IEC 25010:2011, Systems and software engineering -- Systems and software Quality Requirements and Evaluation (SQuaRE) -- System and software quality models. Međutim, i citirani i poslednji, kao i drugi odgovarajući ISO/IEC strandardi koji se bave kvalitetom softvera su preuzeli identične karakteristike i podkarakteristike kvlaiteta softvera, pa je navedeni standard citiran kao prethodnik koji uvodi pomenuti sistem.

[622] Ibid.

Tabela 9. Karakteristike i podkarakteristike softvera po ISO/IEC 9126-1 standardu[623, 624]

KARAKTERISTIKE I PODKARAKTERISTIKE ISO/IEC 9126-1:2001	
Karakteristike	***Podkarakteristike***
Funkcionalnost	Pogodnost, tačnost, interoperabilnost, bezbednost, usklađenost (funkcionalnosti)
Pouzdanost	Zrelost, podnošenje kvarova, mogućnost popravke, usklađenost (pouzdanosti)
Upotrebljivost	Razumljivost, pogodnost za učenje, operabilnost, privlačnost, usklađenost (upotrebljivosti)
Efikasnost	Upravljanje vremenom, korišćenje resursa, usklađenost (efikasnosti)
Lakoća održavanja	Mogućnost analiziranja, mogućnost promene, stabilnost, mogućnost testiranja, usklađenost (održavanja)
Portabilnost	Prilagodljivost, mogućnost instaliranja, mogućnost zamene, koegzistencija, usklađenost (portabilnosti)

Iz ovog standarda je razvijen standard ISO/IEC 25010[625], po kome, svojstvo bezbednosti je jedna od osnovnih karakteristika kvaliteta sistema i softvera kao proizvoda (Tabela 10). Bezbednost predstavlja "nivo do koga proizvod ili sistem štiti informacije i podatke tako da osobe ili drugi proizvodi ili sistemi imaju nivo pristupa podacima koji odgovara vrsti i nivou njihovih ovlašćenja" i sastoji se od poverljivosti, integriteta, nepovredivosti, odgovornosti i autentičnosti.[626]

[623] *ISO/IEC 9126-1:2001, Software engineering -- Product quality -- Part 1: Quality model*

[624] Ho-Won Jung, Seung-Gweon Kim and Chang-Shin Chung. "Measuring Software Product Quality: A Survey of ISO/IEC 9126." *IEEE Software* 5 (2004): 88-92.

[625] *ISO/IEC 25010:2011, Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models*

[626] Ibid. Tačka 4.2.6. Napomena, po standardu se bezbednost odnosi na podatke u sistemu, sačuvane od strane sistema STAO https://www.iso.org/obp/ui/#iso:std:iso-iec:25010:ed-1:v1:en

Tabela 10. Karakteristike i podkarakteristike softvera po ISO/IEC 2520 standardu[627]

KARAKTERISTIKE I PODKARAKTERISTIKE ISO/IEC 25010-1:2001	
Karakteristike	***Podkarakteristike***
Funkcionalna podobnost	Funkcionalna potpunost, funkcionalna tačnost, funkcionalna podesnost
Efikasnost učinka	Upravljanje vremenom, korišćenje resursa, kapacitet
Kompatibilnost	Koegzistencija, interoperabilnost
Upotrebljivost	Podesnost, prepoznatljivost, mogućnost učenja, operabilnost, zaštita od korisničkih grešaka, estetika korisničkog interfejsa, pristupačnost
Pouzdanost	Zrelost, dostupnost, tolerancija na kvarove, mogućnost popravke
Bezbednost	Poverljivost, integritet, neporecivost, autentičnost, odgovornost
Mogućnost održavanja	Modularnost, ponovna iskoristljivost, mogućnost analize, mogućnost modifikacije, mogućnost testiranja
Portabilnost	Adaptabilnost, mogućnost instaliranja, mogućnost zamene

Dakle, bezbednost softvera je mera kontrole pristupa (odnosno dostupnosti) podacima od značaja za izvršenje njegove funkcije. Karakteristike kvaliteta softvera mogu biti merene interno (načelno merenjem statičkih mera), eksterno (tipično merenjem ponašanja/funkcionisanja softvera kada se on izvršava) ili u situaciji stvarne ili simulirane upotrebe (u realnim okolnostima). To znači da ukupni kvalitet softvera, kao i njegove pojedinačne karakteristike i podkarakteristike, uključujući i bezbednost, zavise od internih i eksternih faktora, odnosno od specifičnog konteksta upotrebe[628].

[627] *ISO/IEC 25010:2011, Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models, 4.2 Product quality model*, Slika 4, Tabela 4.

[628] *BS ISO/IEC 25010:2011, Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models,* http://janus.uclan.ac.uk/pagray/BS-ISO-IEC%2025010%202011%20quality%20requirements%20models.pdf

8.6.1. Posledice delovanja nedostataka u softveru na funkcionisanje tehničkih sistema

Posledice rastuće zavisnosti savremenih sistema od IKT nisu samo pozitivne, već i negativne. Negativni aspekti se ogledaju u nesavršenostima arhitekture informacionih sistema, načina funkcionisanja i međusobne interakcije. Zbog prirodnih ograničenja ljudi, koje dovode do grešaka prilikom programiranja, nemoguće je programirati softver bez grešaka u sadržaju instrukcija, odnosno softver savršene funkcionalnosti. Mogućnost preduzimanja sajber napada na te sisteme upravo zavisi od broja i dostupnosti tih grešaka. Ukoliko ih mogu iskoristiti napadači (faktori pretnje), te greške predstavljaju ranjivosti. Ranjivosti su univerzalne u svim informacionim sistemima, bez obzira da li služe za vojne ili civilne svrhe, i bez obzira na značaj tih sistema.

Studija kompanije *Qualis* o istraživanju softverskih ranjivosti na veb-zavisnim aplikacijama je utvrdila da se ranjivosti aktuelno podložne iskorišćenju od strane napadača nalaze u proseku 48 dana na internim sistemima; da se najčešće vrste ranjivosti koje su bezbednosno otkrivene i ažurirane u prethodnim verzijama softvera, u kratkom roku ponovo pojavljuju sa novim softverom; da postoje određene ranjivosti čiji je životni ciklus neograničen; da postoje kritične ranjivosti koje uzrokuju većinu površine napada sistema; da ciklus od nastanka do otkrivanja ranjivosti u sistemu od strane napadača traje kraće nego ciklus otkrivanja i ažuriranje od strane korisnika, i da se gotovo svi napadi koji potiču od sistema za automatsku analizu i otkrivanje ranjivosti dogodi u prvih 15 dana postojanja ranjivosti.[629]

Kavusoglu, Kavusoglu i Žang[630] su na teoretskom modelu dokazali da čak i kada se na jednom računarskom sistemu nalazi instaliran jedan softverski program koji sadrži softversku ranjivost, ne postoji način da se optimalno usklade ciklusi objavljivanja i ažuriranja softvera između proizvođača i korisnika koji se rukovode različitim poslovno-organizacionim motivima. Navedeno pokazuje da politika otkrivanja i ažuriranja

[629] Qualys, *The Laws of Vulnerabilities: Six Axioms for Understanding Risk* (2006), https://www.qualys.com/docs/Laws-Report.pdf (preuzeto 8. jula 2015).

[630] Huseyin Cavusoglu, Hasan Cavusoglu, and Jun Zhang.,"Economics of Security Patch Management" in Workshop on the Economics of Information Security - WEIS (Robinson College, University of Cambridge, England, 2006).

softverskih ranjivosti nikada ne može biti dovoljno uspešna da bi sprečila sajber napade koji iskorišćavaju postojanje softverskih ranjivosti u informacionim sistemima.[631]

Greške u softveru se ne mogu izbeći čak ni kada se za pomoć u programiranju koriste automatizovani sistemi i dodatne mere za ograničavanje broja grešaka, pošto izrada softvera primarno zavisi od ljudi, a njihov rad je podložan prirodnim ograničenjima. Navedene karakteristike koje omogućavaju postojanje ranjivosti i omogućavaju napade Mekgrav[632] naziva „trojstvom nevolja“. Softver postaje sve kompleksniji,[633] kompatibilan je sa softverom starije i novije generacije i lako se umrežava. Čak i kada softver originalno nije namenjen za umrežavanje sa drugim informacionim sistemima, osobina kompatibilnosti mu omogućava da bude umrežen zahvaljujući softveru novije generacije.

Međutim, ključni faktor za brojnost grešaka u softveru nije kompleksnost njegovih logičkih instrukcija, iako i ona povećava verovatnoću nastajanja grešaka, već veličina softvera merena brojem kodnih linija. Što je veći broj kodnih linja softvera, veća je verovatnoća pojave greške, čak i u kodnim linijama sa jednostavnim logičkim instrukcijama. Da bi se na velikim softverskim projektima umanjila ova uzročna veza, timovi programera koriste standarde čijom primenom se ograničava broj grešaka u softveru.[634] Međutim, takve metode mogu da održavaju broj grešaka u odnosu na broj kodnih linija u granicama konstantnih, ali ne sprečavaju njihovu pojavu i kasniji uticaj na bezbednost. Pored složenosti softvera, dodatni uzroci koji su izvori softverskih nedostataka, koji postaju ranjivosti podložne napadima su nadogradljivost softvera i konektivnost. Ove osobine su inherentne informaciono-komunikacionim tehnologijama, jer se one kreiraju sa bi bile kompatibilne i samim tim funkcionalne.

Stručnjaci nisu saglasni u vezi toga koliki je prosek pojave grešaka u softveru. To nije ni moguće upoređivati, jer je softver različit po nameni i kvalitetu, a vremenom se i

[631] Anup K. Ghosh, Chuck Howell, and James A. Whittaker, "Building Software Securely from the Ground up." *IEEE software* 19, no. 1 (2002): 14.

[632] Gary McGraw, *Software security: Building Security In*. Vol. 1. (Boston, MA: Addison-Wesley Professional, 2006), 6.

[633] Steve D. Suh and Iulian Neamtiu, "Studying Software Evolution for Taming Software Complexity," In *21st Australian Software Engineering Conference (ASWEC)* (IEEE, 2010), 3-12.

[634] Bo Einarsson, ed., *Accuracy and Reliability in Scientific Computing*. Vol. 18 (Philadelphia, PA: SIAM, 2005).

unapređuju same tehnike pisanja softvera, i menjaju se programski jezici u kome se piše softver. Po MekKonelu[635] industrijski prosek pojave softverskih grešaka na 1000 kodnih linija[636] je 2004. godine bio između 1 i 25. Međutim, u ovaj prosek je ušao samo prijavljeni i otkriveni broj grešaka, koji se očekivano umanjuje, jer niko ne želi sebe da prikaže kao autora nekvalitetnog softvera, niti napadači prijavljuju otkrivene greške. U realnosti, broj grešaka je veći. Po istom autoru, prijavljeni broj softverskih grešaka u proizvodima kompanije Majkrosoft u periodu devedesetih godina 20. veka je bio između 10 i 20[637]. To se poklapa sa nalazom studije Karnegi Melon univerziteta iz 2004. godine, po kojoj se procenjeni prosečni broj grešaka u komercijalnom softveru se kreće između 20 do 30 na svakih 1000 kodnih linija softvera.[638]

Šanon[639] to potvrđuje i ističe da su jedine institucije u kojima se softver stvara primenom krajnje rigoroznih metoda i retko sadrži greške institucije poput *Nacionalne aeronautičke i svemirske administracije* (NASA), u kojoj se softver stvara sa ciljem da pokreće sisteme koji moraju stabilno da rade decenijama, bez ikakve greške, milionima kilometara daleko od Zemlje.[640] Međutim, svaka primena dodatne metode na osiguravanju kvaliteta programiranja značajno usporava i samim tim poskupljuje projekat, jer povećava broj radnih časova angažovanja programera i kontrolora softvera. Kupman navodi da se cena industrijskog softvera 2010. godine kretala od 15 do 40 dolara po kodnoj liniji, u

[635] Steve McConnell, *Code Complete* (Upper Saddle River, NJ: Pearson Education, 2004), 521.

[636] Kodna linija je mera količine izvornog koda koja se sastoji od broja linija teksta tog koda (fizičkih linija ili logičkih iskaza) i služi kao približna mera očekivanog napora programera do završetka projekta, održavanja softvera ili produktivnosti procesa njegove izrade. U pitanju nije egzaktna kvantitativna mera, pošto jedna kodna linija nije standardna veličina koja zahteva isti napor programera. U slučaju različitog softvera, ne obuhvata isti obim logičkih iskaza ili procesa, niti je ista za svaku vrstu programskog jezika. Pored toga, na primer, jedna fizička linija teksta može obuhvatati dve logičke linije i jedan komentar. S druge strane ista logička celina napisana u različitim programskim jezicima obuhvata različit broj kodnih linija, pri čemu je „mašinskim" jezicima, čija je sintaksa pogodna za procesiranje od strane računara, za isti logički iskaz potreban veći broj kodnih linija od takozvanih „viših" programskih jezika, čiji su kodni izrazi lakši za razumevanje ljudima. Zbog toga se broj kodnih linija uglavnom povezuje sa naporom i produktivnošću programera da programira neki softver, poput broja radnih časova programiranja, koji podrazumeva količinu kodnog teksta prosečne težine koji prosečan programer isprogramira za jedan radni čas.

[637] Steve McConnell, *Code Complete* (Upper Saddle River, NJ: Pearson Education, 2004), 521.

[638] Carnegie Mellon University's CyLab Sustainable Computing Consortium, in Michelle Delio, „Linux: Fewer Bugs Than Rivals," *Wired*, December 14, 2004, http://archive.wired.com/software/coolapps/news/2004/12/66022 (preuzeto 24. januar 2016).

[639] Eng. Greg Shannon, vodeći naučnik na Carnegie Mellon University's Software Engineering Institute

[640] Greg Shannon in David Talbot, „Why We're So Vulnerable," *MIT Technology Review*, January 25, 2016, https://www.technologyreview.com/s/545621/why-were-so-vulnerable/ (preuzeto 28. januara 2016).

zavisnosti do kvaliteta, bezbednosti i pouzdanosti, a da je do 2015 godine porasla za dodatnih 20%.[641]

Primenom posebnih tehnika na optimizaciji rada i proveri grešaka obučenih timova pri izradi softvera moguće je smanjiti broj grešaka na ispod jedne greške na 1000 kodnih linija.[642] U pojedinim visoko rizičnim projektima, poput softvera za kosmičke rakete, u praksi je čak postignuto potpuno eliminisanje grešaka na 500.000 kodnih linija, ali uz primenu raznih formalnih metoda razvoja softvera, naizmenično kontrolisanje softvera i metoda statističkog testiranja.[643] Međutim, svaka primena dodatne metode na osiguravanju kvaliteta programiranja značajno usporava i samim tim poskupljuje projekat, jer značajno povećava broj radnih časova angažovanja programera i kontrolora softvera.

Dakle, softver sadrži greške. U skladu sa složenošću savremenog softvera, identifikovani su različiti tipovi grešaka. Oni su različito definisani različitim standardima. Takođe, sama stručna praksa izrade softvera je vremenom dovela do razlikovanja različitih vrsta softverskih grešaka i njihovih posledica. Ova terminološka podela nije univerzalna u tehnologiji, jer ne postoji jedinstveni standard za kvalitet softvera u svetu, kao ni jedan svetski jezik u kome je svaki termin jednoznačno određen.[644] Uprkos preklapanju značenja termina i neujednačenih terminologija, u stručnoj praksi načelno se razlikuju sledeće četiri vrste nedostataka: greška opšteg karaktera, koja se najčešće naziva buba (eng. *bug*), nedostatak ili mana (eng. *flaw*), otkaz (*failure*) i kvar (eng. *fault*).

Po rečniku termina američke *Alijanse za rešenja iz oblasti telekomunikacionih industrija* (ATIS), termini buba, nedostatak (mana), otkaz i kvar imaju sledeće značenje:

- **buba** (eng. *bug*) ima najšire značenje i jednostavno označava grešku ili kvar;[645]

[641] Phil Koopman, „Embedded Software Costs $15-$40 per Line of Code,“ http://betterembsw.blogspot.rs/2010/10/embedded-software-costs-15-40-per-line.html (preuzeto 24. marta 2016).

[642] Steve McConnell, *Code Complete.*

[643] Ibid.

[644] Gotovo svi originalni termini u oblasti informacionih tehnologija su nastali na engleskom govornom području.

[645] *ATIS Telecom Glossary*, s.v. „bug,“ http://www.atis.org/glossary/definition.aspx?id=5964, (preuzeto 15. decembra 2015). Navedeni rečnik je predloženi stručni rečnik u oblasti telekomunikacija koji obuhvata i zamenjuje prethodni rečnik *Telecom Glossary 2000*. TK1.523-2001, koji je u stručnom

- **nedostatak/mana** (eng. *flaw*) označava "grešku u dodeljivanju, nedodeljivanju ili nadzoru koja omogućava zaobilaženje ili onemogućivanje zaštitnih mehanizama" [646];
- **otkaz** (eng. *failure*) znači "privremeni ili stalni prekid sposobnosti nekog entiteta da izvodi zahtevanu funkciju"[647];
- **kvar** (eng. *fault*) označava "1. slučajno stanje koje uzrokuje nemogućnost izvršavanja zahtevane funkcije od strane funkcionalne jedinice; 2. nedostatak koji uzrokuje reprodukujuću[648] ili katastrofalnu neispravnost; 3. u energetskim sistemima, slučajan kratak spoj ili delimični kratak spoj između provodnika pod naponom ili između provodnika pod naponom i uzemljenja"[649].

Po ISO standardu, kvar (*fault*) predstavlja "abnormalno stanje ili defekt komponente, opreme ili podsistema koji može dovesti do otkaza"[650].

Greške u softveru dovode do nepredvidivih ili predvidivih otkaza. Uticaj softverskih grešaka nije isti u svim vrstama sistema. Na primer, u veb-okruženju, softverska greška se uočava brzo, dovodi do smanjene funkcionalnost nekog dela veb-prezentacije, koja se u slučaju nefunkcionalnosti vrlo brzo može zameniti sadržajem iz rezervne kopije podataka i brzo popraviti angažovanjem operativnih timova programera koji se bave održavanjem veb aplikacije ili prezentacije. Međutim, postoje mnoga visoko rizična okruženja u kojima greška u softveru može trenutno dovesti do narušavanja funkcionalnosti sistema, njegovog otkaza, uništenja i potencijalno smrtnih posledica po posadu i ljude u okolini, ili čak dovesti do ozbiljnih posledica po funkcionisanje nacionalne infrastrukture i ugrožavanja nacionalne bezbednosti.

---

pogledu zamenio federalni rečnik definisan standardom 1037C, Federal Standard 1037C, Telecommunications: Glossary of Telecommunication Terms.

[646] *ATIS Telecom Glossary*, s.v. „flaw" http://www.atis.org/glossary/definition.aspx?id=8016, (preuzeto 15. decembra 2015).

[647] *ATIS Telecom Glossary*, s.v. „failure", http://www.atis.org/glossary/definition.aspx?id=7888, (preuzeto 15. decembra 2015).

[648] Reprodukujuća neispravnost podrazumeva da se dosledno nastaje (ponavlja se) pod istim okolnostima.

[649] *ATIS Telecom Glossary*, s.v. „fault", http://www.atis.org/glossary/definition.aspx?id=7926 (preuzeto 15. decembra 2015).

[650] ISO/CD 10303-226

Zbog načina funkcionisanja sistema, okruženja u kome se sistem nalazi u toku operativne upotrebe, značaja funkcije sistema, i visoke rizičnosti po bezbednost, greška u softveru se ne može detektovati niti otkloniti trenutno u toku operativne upotrebe. Detekcija greške u takvim sistemima je obično povezana sa otkazom funkcije samog sistema u toku operativne upotrebe, što u odnosu na operativno okruženje može značiti njegovo uništenje (na primer, vojni sistemi, vazduhoplovi, kosmičke letelice i sateliti, podvodni sistemi, nuklearni sistemi, sistemi kritične infrastrukture, medicinski uređaji i drugi).

Ukoliko je sajber napad izveden zloupotrebom nedostatka koji je implementiran u informacioni sistem, detekcija samog napada je veliki problem. Da bi se napad mogao identifikovati (regulisati), prvo je potrebno da žrtva bude svesna njegovog postojanja. U slučaju uništenja sistema, ili jednostavno u slučaju pojave otkaza sistema u toku rada, teško je utvrditi da li se radi o slučajnoj grešci ili namernom napadu. Posebno je to teško utvrditi u realnom vremenu i kratkom vremenskom periodu. Detekcija greške koja dovodi do narušene funkcionalnosti, upotrebljivosti, bezbednosti ili bilo koje druge kritične karakteristike kritičnih sistema je direktno povezana sa značajnim negativnim posledicama po ljude, sisteme, servise i organizacije. Zbog toga, u cilju sprečavanja pojave grešaka, programiranju softvera za sisteme visokog rizika traje godinama, pa i decenijama, i vrlo je skupo, jer se softver podvrgava dugačkim periodima testiranja u raznim situacijama, dok je za neka druga okruženja, poput veb prezentacija i aplikacija ono značajno brže i samim tim jeftinije.

Na primer, 1996. godine je pri lansiranju kosmičke rakete Evropske svemirske agencije, *Arijana 5*, sa kosmodroma u Francuskoj Gvajani, u 40-oj sekundi leta došlo je do eksplozije i uništenja rakete. Raketa je nosila u svemir satelit vredan oko 500 miliona dolara[651]. Do eksplozije je došlo zbog male, ali kritične sistemske softverske greške pri procesorskoj obradi informacija dobijenih od senzora, a u vezi matematičko-logičke konverzije vrednosti različitih brojčanih zapisa vrednosti parametara leta pri radu sa realnim brojevima[652]. Softver rakete je napisan u namenskom programskoj jeziku ADA,

[651] Ariane 501 Inquiry Board Report, *ARIANE 5, Flight 501 Failure*, Paris (19 July 1996), http://esamultimedia.esa.int/docs/esa-x-1819eng.pdf (preuzeto 15. decembra 2015).

[652] Gérard Le Lann, "An analysis of the Ariane 5 flight 501 failure-a system engineering perspective," in *Engineering of Computer-Based Systems, 1997. Proceedings., International Conference and Workshop*, 339-346 (IEEE, 1997),

koji služi za programiranje softvera vrhunske pouzdanosti i široko se koristi za vazduhoplovne, vojne, kosmičke i slične kritične sisteme. Pri programiranju su poštovane procedure koje utiču na smanjenje broja grešaka i povećavaju pouzdanost i bezbednost sistema. Iako je raketa imala ugrađene paralelne sisteme za merenje i izračunavanje parametara koji utiču na trajektoriju i brzinu leta pri lansiranju, značaj te, prilično banalne logičko-matematičke greške[653, 654] je bio ključan za ukupan rad sistema i zaobišao je sve druge ugrađene kontrole bezbednosti sistema.

Za funkciju rakete je bila značajnija činjenica da se softverska greška ipak potkrala programerima u toku programiranja i okolnost da je ona samo u specifičnim uslovima (pri određenom opsegu brojčanih vrednosti parametara leta) mogla dovesti do otkaza sistema koji je imao veći značaj po funkcionisanje sistema nego sve bezbednosne mere ugrađene u sistem. Greška je postojala u programu od njegovog nastanka, ali se nikada nije manifestovala izvan specifične situacije pod dejstvom okruženja i spoljnih faktora. Na specifične okolnosti koje su dovele do manifestacije otkaza niko u tom trenutku nije mogao da utiče. One se čak nisu ni morale manifestovati u toku konkretnog leta. Greška je dovela do eksplozije rakete i njenog potpunog uništenja i uništenja korisnog tovara (satelita).

Posledica je da su iznova procenjeni postojeći standardi u programiranju koji se odnose na specifičnu grešku i da su oni unapređeni, kako do nje ne bi ponovo došlo[655]. Međutim, softver postaje sve zastupljeniji, obimniji i složeniji, a proces programiranja od strane

---

http://www.niwotridge.com/Resources/Ariane5Resources/78890339.pdf (preuzeto 15. decembra 2015).

653 Računarski procesori su u stanju da obrade isključivo celobrojne vrednosti. Za rad sa realnim brojevima koriste se metode kojima se realnim brojevima dodeljuje simboličan zapis u 1, 8, 16, 32 ili 64-bitnom formatu, a konverzija se vrši po standardu *IEEE 754 – Floating Point Standard*. U navedenom zapisu pozicija decimalnog zareza nije fiksna, već je pokretna (eng. *floating point*). Ukoliko se dese minimalne tehničke greške u aproksimaciji brojnih vrednosti može se dobiti krajnje netačan rezultat obrade podataka.

Dragan Mladenović, „Sajber ratovanje: Neslućene mogućnosti novih tehnologija“ *Magazin Odbrana*, broj 191 (1. septembar 2013), Specijalni prilog broj 93, http://www.odbrana.mod.gov.rs/specijalni%20prilog/93/Specijalni%20prilog%2093%20-%20Sajber%20ratovanje.pdf (preuzeto 10. decembra 2015).

654 David Goldberg, „What Every Computer Scientist Should Know About Floating-Point Arithmetic,“ *ACM Computing Surveys*, 23, No. 1 (1991): 5-48. http://perso.ens-lyon.fr/jean-michel.muller/goldberg.pdf (preuzeto 20. oktobra 2015).

655 Institute of Electrical and Electronics Engineers, *754-2008 - IEEE Standard for Floating-Point Arithmetic* (29 August 2008), http://ieeexplore.ieee.org/servlet/opac?punumber=4610933 (preuzeto 10. decembra 2015).

ljudi nije moguće osloboditi od nastanka nenamernih grešaka[656]. Štaviše, njihov broj se povećava proporcionalno složenosti i obimu softvera.

Greške u softveru i računarskom, senzorskom i mrežnom hardveru mogu dovesti do katastrofalnih otkaza u radu i onemogućiti izvršenje borbenog zadatka. Kada te greške otkriju napadači, one postaju ranjivosti u smislu informacione bezbednosti. Ranjivosti u softveru, hardveru i procedurama mogu omogućiti sajber napade na te borbene sisteme, u realnom vremenu ili odložene.

Vojni sistemi se koriste u ekstremnim uslovima i zahtevaju visoku pouzdanost i efikasnost, pa se uobičajeno razvijaju na osnovu posebne projektne specifikacije i postavljenih uslova i zato skuplje koštaju. Primer aviona F-35 ilustruje potrebu da se zbog rastuće potrebe za softverom u vojnom okruženju sve češće koriste komercijalne tehnologije civilne namene[657] za izradu vojnih sistema. Međutim, to znači da često, vojni sistemi dele iste nedostatke i slabosti kao i komercijalni proizvodi, iako se od njih zahtevaju ekstremni uslovi rada i visoka pouzdanost.

Na primer, programski jezik C++ u kome je napisan veliki deo softvera aviona F-35 je jedan od najraširenijih u svetu.[658] Napadači mogu izvršiti statističku analizu sklonosti tog programskog jezika da sadrži specifične vrste grešaka i pokušati da zloupotrebe informacije o tome u procesu traženja ranjivosti i kreiranja napada u specifičnim situacijama. Proces traženja ranjivosti i mogućnosti upada u neki sistem je težak i spor, posebno u slučaju informacionih sistema koji su fizički izolovani od dostupnih mreža[659]. Timovi iz državnih agencija koji izvode ofanzivne operacije u sajber prostoru imaju značajno veće resurse od pojedinaca u svakom pogledu, raspolažu informacijama o

[656] Greške, mane i nedostaci mogu biti i namerni.

[657] *Commercial-off-the-shelf* (COTS) tehnologije iz komercijalne civilne primene.

[658] U programskom jeziku C++ je, na primer, programirana većina softvera za telefone, kao i većina softverskih proizvoda softverske kompanije *Microsoft*. Sve verzije operativnog sistema *Windows*, internet pretraživači, *MS Office* softverski paket i druge proizvode *Microsoft* je programirao primenom programskih jezika Visual C++ i C++.

Bjarne Stroustrup, „C++ Applications,“ http://www.stroustrup.com/applications.html, (preuzeto 23. marta 2016).

[659] Radi se o sistemima koji su fizički izolovani od drugih sistema (eng. *air gap*).

većem broju ranjivosti nultog dana[660], poseduju mogućnost da prave modele ciljeva, raspolažu sa većim brojem eksperata i mogu izvršiti detaljnu analizu cilja[661, 662, 663]. Pored svega, takve timove, koji u praksi i realizuju sajber napade na državnom nivou, po sopstvenoj tvrdnji karakteriše i najveća posvećenost tom zadatku, disciplina i upornost, pa im informacije ovakvog tipa mogu biti od pomoći da budu efikasniji. Direktor najpoznatije jedinice za izvođenje ofanzivnih operacija u sajber prostoru, Rob Džojs, je na hakerskoj konferenciji *USENIX Enigma* 2016. godine izjavio: "Mi ulažemo mnogo vremena u…poznavanje (informacionih mreže) bolje od ljudi koji su ih dizajnirali i ljudi koji ih održavaju. Vi poznajete tehnologije koje nameravate da upotrebite u toj mreži. Mi poznajemo tehnologije koje su trenutno u upotrebi u toj mreži… U pogledu bilo koje velike mreže, reći ću vam da je upornost i fokusiranje to što će vam omogućiti da uđete u nju, bez upotrebe informacija o ranjivostima nultog dana"[664].

Upoređivanje prirode i kvaliteta programskih jezika u pogledu njihove pogodnosti za izradu specifične vrste softvera je teško i nepouzdano[665, 666]. Programski jezik je alat pomoću koga se stvara neki proizvod, a kvalitet i funkcionalnost proizvoda se teško može meriti upoređivanjem različitih alata. Drugi faktori, poput znanja i umeća programera i okruženja u kome softver funkcioniše, direktnije i u većem obimu utiču na bezbednost softvera nego izbor programskog jezika. Pored toga, informaciona bezbednost

---

660 Eng. *Zero-day (0-day) vulnerabilites*, ranjivosti u informacionim sistemima (uglavnom softverskim) koje nisu poznate proizvođaču niti javno (poznate su 0 dana, odatle im dolazi i naziv), pa stoga za njih nije napravljeno ni bezbednosno ažuriranje (popravka) sistema.

661 Bill Nelson, Rodney Choi, Michael Iacobucci, Mark Mitchell, and Greg Gagnon. "Cyberterror prospects and implications." (1999), http://calhoun.nps.edu/bitstream/handle/10945/27344/Cyberterror%20Prospects%20and%20Implications.pdf?sequence=1, 15.

662 Joseph F. Gustin, *Cyber Terrorism: A Guide for Facility Managers,* (Lilburn, GA: The Fairmont Press, Inc., 2003).

663 Irving Lachow, "Cyber Terrorism: Menace or Myth?" in *Cyberpower and National Security*, eds., Franklin D. Kramer, Stuart H. Starr and Larry Wentz, 437-464 (Washington DC: Potomac Books, 2009).

664 Rob Joyce, „USENIX Enigma 2016 - NSA TAO Chief on Disrupting Nation State Hackers", *USENIX Enigma Conference*, https://www.youtube.com/watch?v=bDJb8WOJYdA, (preuzeto 06. marta 2016). Rob Džojs je direktor jedinice Tailored Access Operations, iz NSA, najpoznatije jedinice za izvođenje sajber operacija u svetu.

665 „The Advantage of ADA 95," *AdaIC*, http://archive.adaic.com/intro/ada-vs-c/ada-vs-c.html, (preuzeto 22. marta 2016).

666 Guenter Dotzel, „Oberon-2 and Modula-2 Technical Publication", *The ModulaTor*, 10 and 11 (November and December 1992), http://www.modulaware.com/mdlt28.htm, (preuzeto 22. marta 2016).

savremenih, složenih informacionih sistema je proces koji se stalno procenjuje, menja i usavršava, a ne jedinstveni proizvod. Pri programiranju se moraju razmotriti i mnogi obziri vezani za bezbednost, poput namene i funkcionalnosti softvera, njegovog radnog okruženja, arhitekture softverskog proizvoda, zahteva korisnika i odnosa bezbednosnih principa i mera u odnosu na funkcionalnost.

Međutim, opšta podložnost softverskih proizvoda određenoj vrsti nedostataka i napada potiče iz okolnosti da se svaki programski jezik kreira za neku specifičnu svrhu i potrebu (inače bi bio korišćen neki od postojećih jezika). Pri kreiranju, programski jezik se u samom dizajnu prilagođava toj potrebi i specifičnim okolnostima rada. Zbog specifične sintakse i pravila koja važe za svaki jezik, programeri mogu biti skloniji da češće prave greške određene vrste pri programiranju softvera u određenom jeziku. Navedena okolnost čini programske jezike statistički manje ili više podložnim određenim klasama i vrstama grešaka i ranjivosti. [667] Te vrste grešaka i verovatnoća njihovog pojavljivanja u softverskim proizvodima u odnosu na vrstu jezika se mogu utvrditi ispitivanjima kvaliteta i bezbednosti softvera određene kategorije slične funkcionalnosti[668, 669]. Takođe, može se utvrditi i statistička "sklonost" softvera pisanog u određenim jezicima da sadrži ranjivosti pogodne za izvođenje napada određene klase[670]. Na primer, po izveštaju kompanije *Veracode*, najveći rizik od bezbednosnog incidenta u softveru pisanom u programskom jeziku C++ se nalazi u upravljanju softverskim greškama, kao i u metodi napada "*Buffer overflow*".[671] Vojni sistemi su predviđeni da rade u izolovanim (eng. *air gapped*) okruženjima zbog zahtevane bezbednosti, zbog čega se moraju zaštititi od svake vrste injektovanja zlonamernog softverskog koda ili instrukcija u sopstvene sisteme. Postoji sumnja da su ovakve metode korišćene u prošlosti za prevazilaženje bezbednosnih mehanizama zaštite sistema pozicioniranja i upravljanja bespilotnim letelicama nad

[667] Veracode, „State of Software Security," (Fall 2015): 8.

[668] WhiteHat Security, „2014 Website Security Statistics Report," http://info.whitehatsec.com/rs/whitehatsecurity/images/statsreport2014-20140410.pdf (preuzeto 22. marta 2016).

[669] Bertrand Meyer, „Those Who Say Code Does not Matter, and Those Who Say Languages Do not Matter," *BLOG@CACM*, entry posted April 15, 2014, http://cacm.acm.org/blogs/blog-cacm/173827-those-who-say-code-does-not-matter/fulltext (preuzeto 22. marta 2016).

[670] Veracode, „State of Software Security," 5.

[671] Ibid, 7.

Iranom[672]. Tom prilikom je upotrebljena tehnika ometanja radio veze letelice (eng. *radio jamming*), u kombinaciji sa napadom koji za cilj ima "zbunjivanje" geolokacijskog sistema letelice po pitanju odabira legitimnog izvora signala (eng. *spoofing attack technique*)[673], sa ciljem da se preuzme upravljanje letelicom[674] primenom injektovanja instrukcija ili softvera (*software/instruction injection*). Na primer, po ranije pomenutom izveštaju, verovatnoća injektovanja malicioznog softvera i instrukcija u originalni programski kod je najveća kod aplikacija programiranih primenom jezika PHP ili *Classic* ASP (koji se načelno koriste za veb-orjentisano okruženje).[675] Navedene i druge tehnike se uspešno mogu kombinovati, a njihova upotreba je olakšana time što su navedene metode napada poznate, dobro dokumentovane, a čak postoje i vojni sistemi kao proizvodi koji koriste te metode napada ili neke njihove faze.[676]

Dakle, softver složenih sistema koji su potencijalna meta napada spada u izuzetno kompleksne tehničke sisteme koji rade automatski. Priroda procesa kreiranja tog softvera dovodi do toga da se u softveru nalaze brojne greške, koje se povećavaju kako obim i kompleksnost softvera rastu. Sposobnost i potreba umrežavanja informacionih sistema takođe konstantno se povećavaju. Softver može biti uzrok nastanka različitih incidentnih situacija čija ozbiljnost zavisi od okruženja i uslova upotrebe. To dovodi do situacije u kojoj i minimalne greške i nedostaci u informacionim sistemima mogu biti osnov za pokretanje napada sa ozbiljnim posledicama. Na primer, 2015. godine izraelski istraživač softverskih grešaka[677] je otkrio postojanje ranjivosti u svim vrstama operativnih sistema kompanije *Microsoft* (koji obuhvataju preko 90% svih desktop računarskih sistema u

[672] Dragan Mladenović i Danko Jovanović, „Open Source UAV in MANET Combat Environment," *5th International Scientific Conference on Defensive Technologies, OTEH 2012*, Belgrade, September 2012.

[673] Hengqing, W., Huang, P., Dyer, J., Archinal, A., Fagan, J., "Countermeasures for GPS signal spoofing" in *Proceedings of the 18th International Technical Meeting of the Satellite Division of The Institute of Navigation* (*ION GNSS 2005*), Long Beach, 2005, pp. 1285-1290.

[674] Jon S. Warner and Roger G. Johnston, „GPS Spoofing Countermeasures," *Homeland Security Journal* (December 12, 2003).

[675] Veracode, „State of Software Security," 6-7.

[676] Warner and Johnston, „GPS Spoofing Countermeasures."

[677] Udi Javo (eng. Udi Yavo), bivši pripadnik *National Electronic Warfare Research & Simulation Center of Rafael Advanced Defense System* i suosnivač kompanije *enSilo* koja se bavi sajber bezbednošću. https://www.crunchbase.com/person/udi-yavo#/entity

svetu)[678], koja je omogućivala napadačima da zaobiđu ugrađenu bezbednosnu zaštitu sistema praveći izmene od samo jednog jedinog bita[679, 680].

Softverske greške u vojnim borbenim sistemima nisu potencijalna mogućnost, već su realnost koja postoji već decenijama, tokom mira i u ratu. Na primer, po izveštaju Petera i Randela[681] iz 1968. godine koji je sačinjen za potrebe NATO, jedna jedina softverska greška je u tom periodu dovela do serije ozbiljnih avionskih nesreća. Lin[682] još 1985. godine navodi celu seriju incidenata sa katastrofalnim posledicama koji su nastali kao rezultat grešaka u softveru tehničkih sistema od kojih su mnogi korišćeni u svemirskoj tehnologiji ili borbenim vojnim sistemima. Po njemu, tokom Foklandskog rata, britanski razarač je pogođen argentinskom raketom francuske proizvodnje *Exocet*, jer je softver radarskog sistema za upozorenje bio programiran da raketu tog tipa tretira kao prijateljsku, jer je ona bila u naoružanju britanske vojske. [683] Na testovima novog sistema tipa *Aegis* za upravljanje vatrom na krstarici američke vojske utvrđeno je da čak 6 od 16 zadatih ciljeva nije bilo dejstvovano zbog naknadno utvrđene softverske greške koja je promakla u svim ranijim fazama testiranja softvera.[684] Daglas [685]navodi da tokom Prvog zalivskog rata 1991. godine u Iraku, antiraketni sistem Patriot američke vojske nije reagovao i blagovremeno oborio iračku raketu tipa *Skad*, zbog softverske greške, zbog

[678] NetMarketShare, „Desktop Operating System Market Share“, March 2016, https://www.netmarketshare.com/operating-system-market-share.aspx?qprid=10&qpcustomd=0, (preuzeto 28. marta 2016).

[679] Udi Yavo, „CVE-2015-0057: The 1-Bit that will Bring Windows Down,“ *Ensilo Blog*, entry posted February 15, 2015, http://blog.ensilo.com/one-bit-rule-compromising-windows-single-bit, (preuzeto 28. marta 2016).

[680] Microsoft, TechNet, „Microsoft Security Bulletin MS15-010 – Critical,“ February 10, 2015, https://technet.microsoft.com/library/security/MS15-010, (preuzeto 28. marta 2016).

[681] Peter Naur and Brian Randell, eds., *Software Engineering: Report of a Conference sponsored by the NATO Science Committee* (Garmisch, Germany, 7-11 Oct. 1968) (Brussels, Scientific Affairs Division, NATO, 1969), 121.

[682] Herbert Lin, "The Development of Software for Ballistic-missile Defense," *Scientific American*, 253, no. 6 (1985), 51-52.

[683] Ibid, 48.

[684] Ibid, 51.

[685] United States General Accounting Office (GAO), B-247094, The Honorable Howard Wolpe Chairman, Subcommittee on Investigations and Oversight Committee on Science, Space, and Technology House of Representatives, February 4, 1992, http://fas.org/spp/starwars/gao/im92026.htm (preuzeto 26. januara 2015).

čega je nastradalo 28 i ranjeno 98 vojnika. Nojman[686] navodi dugačku listi softverskih grešaka čije postojanje u civilnim i vojnim sistemima predstavlja ozbiljne rizike po informacionu bezbednost tehničkih i organizacionih sistema.

Osnova postojanja sajber oružja nije u sposobnosti izrade tehničkih sistema za ostvarivanje ubojnog, onesposobljavajućeg ili destruktivnog dejstva (kao u slučaju tradicionalnih sistema naoružanja za dejstvo u fizičkom okruženju), već u postojanju nedostataka i grešaka u sistemima (informacionim, softverskim, hardverskim). Čak i kada takvi tehnički sistemi postoje u vidu softvera (malvera), tehnika i metoda napada ili hardvera (materijalnih tehničkih sistema), čija je osnovna namena da ostvare neki vid primene sile ili agresije na ciljanu metu, funkcija tih sistema je uvek zasnovana na činjenici da se njihovo dejstvo na sistem uvek zasniva na postojanju njihove specifične ranjivosti. I obrnuto, sistem koji nema slabosti je otporan na sajber napade koji su zasnovani na iskorišćavanju tih slabosti. Zbog toga je verovatniji napadač u sajber prostoru onaj akter, koji poznaje slabosti nekog sistema, nego onaj akter koji ima neprijateljske namere, ali ne raspolaže sa informacijama o ranjivostima protivnika, kapacitetom da ih otkrije, prodre u sistem i ostvari dejstvo. Ova činjenica je od značaja za primenu i regulisanje sajber napada i sukoba.

8.6.2. Primer aviona F-35

Primera za narušavanje bezbednosti sistema greškama u softveru ima onoliko koliko postoji tehničkih sistema sa ugrađenim informacionim tehnologijama. Jedan od karakterističnih je višenamenski borbeni avion *Lockheed Martin F-35 Lightening II*[687], koji se već dve decenije nalazi u procesu razvoja. Njegova operativna upotreba je predviđena do 2070. godine[688], a razvoj mu je započet 1996. godine. Namenjen je da bude univerzalni borbeni avion koji će služiti vojnim potrebama svih vidova vojske SAD i savezničkih armija. Predviđeno je da bude opremljen većim brojem automatizovanih i

[686] Peter G. Neumann, *Illustrative Risks to the Public in the Use of Computer Systems and Related Technology* (Menlo Park, CA: SRI International, 2015), http://www.csl.sri.com/users/neumann/illustrative.html#8 (preuzeto 25. januara 2015).

[687] F-35 Lightening II, Lockheed Martin, https://www.f35.com/

[688] Lara Seligman, „F-35 Will Fly Until 2070 — Six Years Longer Than Planned“, *Defense News*, 25 March 2016, 15, http://www.defensenews.com/story/defense/air-space/2016/03/24/f-35-fly-until-2070-six-years-longer-than-planned/82224282/ (preuzeto 27. marta 2016).

sofisticiranih sistema. Procenjeni troškovi njegovog razvoja, proizvodnje, upotrebe i održavanja do kraja životnog ciklusa aviona su 2014. godine procenjeni na iznos veći od 1.000 milijardi dolara[689]. Završetak razvojne faze je više puta odlagan, iako su određene količine aviona već prodate stranim državama. Jedan od centralnih problema odlaganja je bio softver za upravljanje centralnog računarskog sistema aviona i više borbenih sistema[690, 691].

Avion F-35 je u pogledu primene IKT vremenom postao najsloženiji borbeni tehnički sistem namenjen za učešće u oružanim dejstvima koji je ikada napravljen. Iako je inicijalno bilo planirano da ukupna količina softvera u sistemima ove letelice bude 8 miliona kodnih linija, tokom dugog vremena razvoja i međusobnog usaglašavanja funkcionisanja posebnih sistema na letelici (modula) ta količina je vremenom povećana na čak 24 miliona kodnih linija[692]. Na izradi softvera za sisteme letelice već dve decenije istovremeno radi više stotina programera. Zahtevi u pogledu bezbednosti i funkcionalnosti, kao i sama veličina programskih blokova softvera su uticali na izbor programskih jezika. Na primer, za izradu softvera većine ranijih vazduhoplovnih, raketnih i satelitskih sistema na upotrebi u Ministarstvu odbrane SAD su, sukcesivno, korišćene verzije programskog jezika JOVIAL, ADA83 (kao osnovni programski jezik za softver borbenog aviona pete generacije F-22 *Raptor*) i ADA95. Namena programskih jezika JOVIAL i ADA je izrada softvera visoke pouzdanosti[693], bezbednosti i modularnosti, zbog čega ih je Ministarstvo odbrane SAD konstantno koristilo decenijama[694].

---

689 United States Government Accountability Office (GAO), *F-35 Joint Strike Fighter: Problems Completing Software Testing May Hinder Deliver of Expected Warfighting Capabilities*, GAO-14-322, March 2014, http://www.gao.gov/assets/670/661842.pdf (preuzeto 27. marta 2016).

690 Idrees Ali and Andrea Shalal, „F-35 Chief Cites 'Good, Bad and Ugly' About No. 1 U.S. Arms Program," *Reuters*, March 24, 2016, http://www.reuters.com/article/us-lockheed-f35-software-idUSKCN0WP26V, (preuzeto 27. marta 2016).

691 GAO, *F-35 Joint Strike Fighter*.

692 Michael J. Sullivan, Acquisition and Sourcing Management, *Joint Strike Fighter: Restrucuring Added Resources and Reduced Risk, but Concurrency is Still a Major Concern*, 20 March 2012, http://www.gao.gov/assets/590/589454.pdf, (preuzeo 19. oktobra 2014), 11.

693 AdaCore, „Safe and Secure Software - An invitation to Ada 2005", http://www.adacore.com/knowledge/technical-papers/safe-secure/ (preuzeto 18. januara 2016).

694 Michael J. Sullivan, *Joint Strike Fighter: Restrucuring Added Resources and Reduced Risk, but Concurrency is Still a Major Concern* (GAO-12-525T) (Washington, DC: U.S. Government Accountability Office, 2012), 11, http://www.gao.gov/assets/590/589454.pdf, (preuzeto 19. oktobra 2014).

Tabela 11. Višenamenski borbeni avion Lockheed Martin F-35 Lightening II[695, 696, 697]

Proizvođač: *Lockheed Martin*		
Naziv	***F-35***	***F-22***
Godina početka upotrebe	2016 (planirana)	1991
Dominantni programski jezik	C++, C	ADA
Broj kodnih linija softvera	24 miliona	1,7 miliona
Prosečna cena izrade u milionima dolara	90-130	146,2

Borbeni tehnički sistemi vremenom postaju složeniji i sposobniji za izvršenje vojnih operacija. Od novih verzija sistema se očekuju poboljšane performanse i nove funkcionalnosti. To iziskuje sve više softvera koji pokreću tehničke sisteme i njima upravljaju. U cilju poređenja, softver lovačkog borbenog aviona prethodne generacije, F-22 *Raptor*, koji je počeo da se proizvodi 1991. godine, ima ukupno 1,7 miliona kodnih linija, a oko 90% njegovog softvera je programirano u jeziku ADA[698]. Zbog ograničenog broja kvalitetno osposobljenih, pouzdanih i bezbednosno prihvatljivih programera za rad na poverljivim projektima moraju se praviti kompromisi pri izboru softvera. To je bio osnovni razlog što su na projektu aviona F-35 umesto tradicionalnih programskih jezika

[695] John Nimmo, a U.S. Air Force pilot navigates an F-35A Lightning II aircraft assigned to the 58th Fighter Squadron, 33rd Fighter Wing into position to refuel with a KC-135 Stratotanker assigned to the 336th Air Refueling, 2013, http://www.defenseimagery.mil/imageRetrieve.action?guid=bcfecb7f82c5cf53d10ff066ef2e4d985ff7ce35&t=2

[696] https://www.f35.com/

[697] Pace, *Lethal War Machine*, 58.

[698] Steve Pace, *America's Next Lethal War Machine* (New York, NY: McGraw-Hill, 1999), http://imagery.vnfawing.com/PDF-Archive/F-22-Raptor.pdf, 58.

izabrani programski jezici opšte namene (C++, C i Asemblerski programski jezik). Za izradu standarda pri programiranju u C++ jeziku angažovan je i sam autor tog jezika[699].

[699] Lockheed Martin Corporation, *Joint Strike Fighter Air Vehicle C++ Coding Standards For the System Development and Demonstration Program*, Document Number 2RDU00001 Rev C, December 2005, http://www.stroustrup.com/JSF-AV-rules.pdf.

9. SAJBER BEZBEDNOST

Po tvrdnji Šamira[700], savremenu informacionu bezbednosti karakterišu tri principa:

1. Potpuno bezbedni (informacioni) sistemi ne postoje, niti će ikada postojati u budućnosti.
2. Kriptografska zaštita je matematički dovoljno pouzdana da neće biti probijena, već će uvek biti zaobilažena.
3. Nastojanje da se otkrije svaka pojedinačna ranjivost u informacionim sistemima je uzaludno i nije racionalno s obzirom na potrebne resurse i ogroman broj ranjivosti.[701]

Po *Nacionalnom rečniku Informacionog obezbeđenja Ministarstva unutrašnje bezbednosti SAD,* rizik je „mera do koje je neki entitet ugrožen potencijalnim okolnostima ili događajem, i tipično je funkcija 1) neprijateljskog uticaja koji će se desiti ukoliko se te okolnosti ili događaj ostvare i 2) verovatnoće da se to desi“[702]. Ranjivost je „slabost u informacionom sistemu, sistemskim bezbednosnim procedurama, internim kontrolama ili njihovoj implementaciji, koji mogu biti iskorišćeni od strane izvora pretnje“[703]

Po istom izvoru, pretnja je „svaka okolnost ili događaj koji ima potencijal da neprijateljski utiče na organizacione operacije (uključujući misiju, funkcije, predstavu ili reputaciju), organizaciona sredstva, pojedince, druge organizacije ili naciju, preko nekog informacionog sistema u slučaju neovlašćenog pristupa, uništenja, objavljivanja, izmene informacija i/ili uskraćivanjem servisa“[704]. Zbog toga se govori o „agentu pretnje“ ili napadaču koji inicira pretnju. Tog napadača u oblasti informacione i sajber bezbednosti ne treba mešati sa napadačem u smislu primene Međunarodnog prava oružanih sukoba.

Konačno, protivmera je „akcija, uređaj, procedura ili tehnika koja se suprotstavlja pretnji, ranjivosti ili napadu, eliminisanjem ili prevencijom napada, minimiziranjem štete ukoliko

[700] Eng. *Adi Shamir*, jedan od najistaknutijih istraživača u oblasti kriptoanalize, jedan od autora *RSA,* najpoznatijeg algoritma za šifrovanje.

[701] Adi Shamir, „The Cryptographers' Panel,“ *RSA Conference 2015*, http://www.rsaconference.com/speakers/adi-shamir (preuzeto 29. Februara 2016).

[702] Committee on National Security Systems, *National Information Assurance (IA) Glossary, CNSS Instruction No. 4009,* 26 April 2010, 61.

[703] Ibid, 81.

[704] Ibid, 75.

se napad dogodi, ili otkrivanjem i izveštavanjem napada koji se dogodio tako da se mogu preduzeti korektivne akcije“[705]

Dakle, iz ugla informacione bezbednosti, napad je „događaj“ koji uzrokuje negativne posledice na napadnuti sistem. Korisnik napadnutog sistema ga može otkriti, sprečiti i umanjiti njegove posledice preduzimanjem protivmera. U funkcionalnom smislu, napad „sreće“ ranjivosti u ciljanom sistemu da bi ostvario negativni uticaj. Za informacionu bezbednost nije bitan karakter izvora pretnji u političkom ili vojnom smislu, već akcije da se taj događaj spreči, i ukoliko se desi, da se njegove posledice umanje. Za napadača nije bitno „univerzalno“ oružje napada, niti njegova količina, već da u protivničkom sistemu postoji ranjivost, da poseduje informacije o njima, kao i sposobnosti i veštine da iskoristi ranjivosti kako bi se infiltrirao u sistem i ostvario cilj napada.

U fizičkom okruženju oružje se može upotrebiti podjednako za napad kao i za odvraćanje. U sajber prostoru znanje o ranjivostima se može upotrebiti za izvođenje sajber napada ili njihovo sprečavanje. Odvraćanje napadača poznavanjem sopstvenih ranjivosti je nemoguće. S druge strane, poznavanje ranjivosti nije dovoljan uslov da će napad biti uspešan, već samo nužan uslov koji omogućava napad. Ukoliko branilac blagovremeno otkrije sopstvene ranjivosti, i preduzme potrebne protivmere, taj sajber napad ne može biti ostvaren. Zbog toga je sajber ratovanje zasnovano na postojanju ranjivosti, veštini njihovog iskorišćavanja, brzini otkrivanja i uklanjanja ranjivosti i tajnosti, odnosno prikrivanju aktivnosti u sajber prostoru.

U pogledu primene međunarodnog prava u slučaju sajber napada između država bitne su sledeće okolnosti:

- karakter napada (sredstva, metode, način izvršenja, kada i da li se napad desio),
- karakter napadača (identitet, ciljevi i namere napadača),
- posledice (po civile, borce, objekte, suverenitet i teritoriju napadnute zemlje) i
- da li napad izvede u odgovornosti neke države.

Na nesreću, ni jedan od navedenih faktora ne može biti poznat u slučaju napada u sajber prostoru (odnosno u području informacione bezbednosti), pošto se napadi, zbog svoje uspešnosti prikrivaju i anonimizuju, a napadači ne koriste „oružje“ čije dejstvo ostavlja

[705] *CNSS Instruction No. 4009*, 19.

jasne tragove u svetu, već prikriveno izvode napade, zbog čega je otkrivanje napada i napadača otežano.

U procesu izvođenja sajber napada postoje sledeći faktori:

- agenti pretnji (potencijalni napadači; nalaze se u sajber prostoru, ali mogu biti istovremeno i u fizičkom okruženju[706]);
- ranjivosti (odnose se na informacionu bezbednost; mogu biti interne ili eksterne, u sajber prostoru ili u fizičkom okruženju),
- ciljevi napada (vrednosti koje se ugrožavanju: sistemi, procesi, lica; primarni ciljevi su uvek u sajber prostoru, a sekundarni mogu biti u sajber prostoru ili u fizičkom okruženju);
- napadi su procesi koji se ostvaruju kroz sajber prostor.

U daljoj analizi sajber napada, važno je utvrditi kako se ostvaruje napad na logički sloj sajber prostora (na softver). Prilikom napada vrši se direktno i namerno narušavanje informacione bezbednosti napadnutih informacionih sistema. Međutim, informaciona bezbednost zavisi ne samo od napadača na sistem, već i od stanja samog sistema, odnosno od aktivnosti branilaca na upravljanju informacionom bezbednošću sistema i organizacija. Imajući navedeno u vidu, potrebno je sagledati vezu između informacione bezbednosti, ranjivosti i upravljanja rizikom.

Po Rajanu i Rajanu, rizik da će neki agent pretnje (napadač) iskoristiti ranjivost u ciljanom sistemu se može prikazati preko sledećeg konceptualnog algoritma[707]:

$$Rizik = \left(\frac{Pretnja \times Ranjivost}{Protivmere}\right) \times Uticaj \quad (1)^{708}$$

[706] Kao fizička lica, organizacije, tehnički sistemi koji napade preduzimaju na automatizovan način ili kao osobe koje poseduju virtuelni identitet (sajber-persone).

[707] Navedena jednačina nije matematički tačna i njenom primenom se ne mogu dobiti kvantitativno validni rezultati. Ona, po samim autorima, predstavlja konceptualni prikaz odnosa ključnih kategorija od značaja za upravljanje rizikom.

Jeff Lowder, „Why the "Risk = Threats x Vulnerabilities x Impact" Formula is Mathematical Nonsense," *BlogInfoSec*, entry posted August 23, 2010, http://www.bloginfosec.com/2010/08/23/why-the-risk-threats-x-vulnerabilities-x-impact-formula-is-mathematical-nonsense/ (preuzeto 28. februara 2016).

[708] Julie J.C.H. Ryan and Daniel J. Ryan, „Risk Management," course material for the Information Assurance and Critical Infrastructure Protection Course, National Defense University, Information Resources Management College, 1.

Navedena jednačina ima više verzija. Iako su te verzije u čestoj upotrebu u području upravljanja rizikom, ne treba ih shvatiti kao kvantitativnu matematičku formulu, već kao koncept koji govori o proporcionalnom odnosu elemenata od značaja za nastupanje rizika u području informacione bezbednosti. Američko Ministarstvo unutrašnje bezbednosti koncept rizika predstavlja na sledeći način, koji je saglasan prethodnom:

$$Rizik = f\ (Pretnja, Ranjivost, Posledice) \quad (2)$$[709]

Ova jednačina nije primenjiva za procenu rizika u slučaju prirodnih katastrofa, već samo u slučaju napada. Funkcija u njoj označava da postoji relacija između vrednosti pretnje, ranjivosti i posledica, ali se ne navodi kakva.

U obe jednačine, rizik da će se dogoditi neki događaj koji predstavlja narušavanje informacione bezbednosti je u funkciji od:

- pretnje (kvaliteta, namere i sposobnosti napadača),
- ranjivosti u samom sistemu (nedostataka, grešaka) i
- protivmera.

Pri tome, rizik i posledice incidenta (napada) su u međusobnom odnosu. Prethodna jednačina rizika može biti prikazana i u funkciji od potencijalnog uticaja mogućeg dejstva sajber napada (Uticaj), verovatnoće da se napad desi (V_{napada}) i verovatnoće da će napad biti uspešan ($_{Vuspešnosti}$):

$$Rizik = (Uticaj) \times (Vnapada) \times (Vuspešnosti) \quad (3)$$[710]

Na osnovu navedene (takođe ne kvantitativne, već konceptualne) jednačine, vidi se da je rizik od sajber napada po napadnuti sistem najveći kada je:

– potencijalni uticaj napada na metu najveći (na primer, prilikom oružane borbe, u slučaju sistema kritične infrastrukture, kada su ugroženi životi ljudi i značajni sistemi);

[709] United States Department of Homeland Security, *Risk Management Fundamentals*, April 2011, https://www.dhs.gov/xlibrary/assets/rma-risk-management-fundamentals.pdf, 20 (preuzeto 28. februara 2016).

[710] Vedat Coskun, Karem Ok, and Busra Ozdenizci, *Near Field Communication: From Theory to Practice* (Chicester, UK: John Wiley & Sons Ltd, 2010).

- u slučajevima visoke verovatnoće da će se napad desiti kao posledica postojanja brojnih ranjivosti koje u dužem vremenu nisu otklonjene, ili nisu ni poznate korisniku napadnutog sistema,
- u slučaju visoke verovatnoće od će specifični sajber napad biti efikasan (na primer interni ili eksterni DoS napadi velikog kapaciteta, upotreba nezaštićenih podataka u neprijateljskom okruženju (odsustvo elementarnih mera zaštite poput kontrole pristupa ili enkripcije i druge).

S obzirom da pretnje ne mogu biti direktno kontrolisane, rizici od sajber napada i njihovih posledica mogu biti kontrolisani (umanjeni) samo otklanjanjem ranjivosti i preduzimanjem dovoljnih i adekvatni mera zaštite od napada. Sve ranjivosti nikada ne mogu biti identifikovane ili otklonjene, pa stoga rizik od sajber napada uvek postoji, čega svi učesnici aktivnosti u sajber prostoru moraju biti svesni.

9.1. Razlika između informacione i sajber bezbednosti u kontekstu sajber napada

Prilikom razmatranja razlike između informacione i sajber bezbednosti u pogledu regulisanja sukoba u sajber prostoru, koji predstavljaju oružanu vojnu manifestaciju političkih odnosa, logično je da se prvo misli na političke razlike između ključnih aktera. U svetu postoje dve osnovne struje političke misli o razlici i međusobnom odnosu navedenih pojmova, zapadni i istočni. Stav američke vlade je tehnološki orjentisan i u centralno mesto stavlja „sajber prostor“ i „sajber bezbednost“, a ruski stav ima širi politički i društveni kontekst u kome se upotrebljavaju koncepti “informaciona bezbednost” i “informacioni prostor”.[711] Međutim, prirodu sajber napada je potrebno posmatrati nezavisno od stavova Zapada ili Istoka, jer su njihovi stavovi politički zasnovani, a priroda sajber sukoba je zasnovana na tehnološkim osnovama. Zbog toga je potrebno analizirati značenje pojmova “informaciona bezbednost” i “sajber bezbednost” u tehnološkom kontekstu, koji pružaju definicije u standardima, uputstvima i relevantnim rečnicima.

[711] Franz-Stefan Gady and Greg Austin, *Russia, The United States, And Cyber Diplomacy Opening the Doors*, (EastWest Institute, 2010), 5.

9.1.1. Informaciona bezbednost

Po ISO/IEC 2700 standardu, informaciona bezbednost je "očuvanje poverljivosti[712], integriteta[713] i dostupnosti[714] informacija"[715], uz napomenu da u navedenu definiciju mogu biti uključena i druga svojstva informacija, poput autentičnosti[716], odgovornosti, neporecivosti[717] i pouzdanosti. Dakle, navedeni standard tvrdi da je narušavanje informacione bezbednosti povreda jednog od navedenih svojstava informacije. S druge strane, američki zakon FISMA[718], kao i Nacionalni institut za standarde i tehnologiju (eng. *National Institute of Standards and Technology* – NIST)[719], tvrde da "termin 'informaciona bezbednost' znači zaštitu informacija i informacionih sistema od neautorizovanog pristupa, upotrebe, objavljivanja, narušavanja, izmene ili uništenja u cilju obezbeđivanja…integriteta… poverljivosti… i dostupnosti"[720].

Navedene definicije se ne razlikuju ni u čemu, osim u tome što američki zakon tvrdi da se informaciona bezbednost odnosi i na informacije i na informacione sisteme, dok ISO/IEC standard tvrdi da se odnosi samo na informacije. Iako ova razlika izgleda značajna, posebno u pogledu primene međunarodnog prava, ona u praksi primene u sajber prostoru u stvari i ne postoji. Poput Federalnog ministarstva unutrašnjih poslova Nemačke, koje tvrdi da je sajber prostor sistem informacionih tehnologija koje su

[712] Poverljivost je stanje informacije u kome ona nije dostupna ili otkrivena neautorizovanim pojedincima, entitetima ili procesima.

International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), ISO/IEC 27000:2016 (en) *Information technology — Security techniques — Information security management systems — Overview and vocabulary*, (u daljem tekstu ISO/IEC 2700: 2016) https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-4:v1:en (preuzeto 5. januara 2015).

[713] Integritet je stanje tačnosti i kompletnosti (ISO/IEC 2700:2016).

[714] Dostupnost informacija je stanje pristupačnosti i upotrebljivosti na zahtev autorizovanog entiteta (ISO/IEC 2700:2016).

[715] ISO/IEC 27000:2016, 2.33., information security, https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-4:v1:en.

[716] Autentičnost je stanje da je neki entitet to što tvrdi da jeste (ISO/IEC 2700:2016).

[717] Neporecivost je sposobnost dokazivanja da se desio događaj ili akcija, kao i izvora njihovog porekla (ISO/IEC 2700:2016).

[718] Federal Information Security Management Act of 2002 (FISMA), Pub. L. No. 107-347, Title III, 116 Stat. 2899, 2002.

[719] William C. Barker, *Guideline for Identifying an Information System as a National Security System, SP 800-59*, (National Institute of Standards and Technology – NIST, 2003), 15.

[720] FISMA, 44 U.S. Code § 3542 – Definitions.

povezane na nivou podataka,[721] i ISO/IEC standard to ničim ne negira. Sajber prostor je sačinjen od informacionih sistema, informacija i informacionog okruženja. Po ISO/IEC, informacioni sistem predstavlja: „aplikacije, servise, sredstva informacione tehnologije ili druge komponente za rukovanje informacijama“[722]. FISMA definiše informacioni sistem kao „diskretni skup informacionih resursa organizovan za prikupljanje, obradu, održavanje, upotrebu, razmenu, širenje ili razmeštanje informacija“[723]. Dakle u oba slučaja informacioni sistem ne može postojati bez informacija. Postojanje informacija je nužan i dovoljan uslov za postojanje ili ugrožavanje informacione bezbednosti. Informaciona bezbednost se odnosi na bezbednost informacija, a ukoliko govorimo o informacionim tehnologijama ili posledici njihovog postojanja i povezanosti, sajber prostoru, podrazumeva se postojanje informacionih sistema.

9.1.2. Sajber bezbednost

Sajber bezbednost je relativno nov termin, koji predstavlja evolutivnu fazu u razvoju ideje informacione bezbednosti i odnosi na informacionu bezbednost u sajber prostoru. U savremenom dobu informaciona i sajber bezbednost se često koriste u uzajamno zamenljivom smislu, iako između ova dva pojma postoji razlika.

Po ISO/IEC 27032:2012 standardu, sajber bezbednost je „očuvanje poverljivosti, integriteta i dostupnosti u sajber prostotu“ [724].

Po Međunarodnoj telekomunikacionoj uniji, sajber bezbednost (eng. *cybersecurity*) predstavlja: „skup alata, politika, bezbednosnih koncepata, bezbednosnih mera, uputstava, pristupa upravljanju rizikom, akcija, treninga, najboljih praksi, obezbeđenja i

[721] FR Germany, Federal Ministry of the Interior, *Cyber Security Strategy for Germany* (February 2011), 9, https://www.bsi.bund.de (preuzeto 6. januara 2016).

[722] ISO/IEC 27000:2016, 2.39. information system.

[723] FISMA.

[724] International Organization for Standardization, ISO/IEC Glossary of IT Security Terminology, ISO/IEC, 2013, http://www.jtc1sc27.din.de/cmd?level=tpl-bereich&menuid=64540&languageid=en&cmsareaid=64540

tehnologija koje mogu biti upotrebljene za zaštitu sajber okruženja i organizacionih i korisničkih resursa“[725, 726].

Po *EastWest* institutu, sajber bezbednost je: „svojstvo sajber prostora koje predstavlja sposobnost suprotstavljanja namernim i/ili nenamernim pretnjama, odgovora na njih i oporavka“.[727]

Po Instrukciji američkog Ministarstva odbrane 8500.01, sajber bezbednost je „prevencija od štete na, zaštita od, i obnova računara, elektronskih komunikacionih sistema, elektronskih komunikacionih servisa, žičanih komunikacija i elektronskih komunikacija, uključujući i informacije u njima, sa ciljem da se obezbedi dostupnost, integritet, autentičnost, poverljivost i neporecivost.[728]

Po *Konceptu strategije sajber bezbednosti Ruske Federacije*, sajber bezbednosti predstavlja skup uslova pod kojim su sve komponente sajber prostora zaštićene od maksimalnog broja pretnji i uticaja sa neželjenim posledicama“ [729].

Po Vladi Izraela, sajber bezbednost predstavlja „politike, bezbednosne aranžmane, aktivnosti, uputstva, protokole upravljanja rizikom i tehnološke alate namenjene za zaštitu sajber prostora i omogućavanje preduzimanja aktivnosti u njemu“[730]

Po Pavlaku, iz Instituta za bezbednosne studije Evropske Unije (eng. *EU Institute for Security Studies*), sajber bezbednost predstavlja „metode koje koriste ljudi, procese i tehnologije, da spreče, otkriju i povrate od štete poverljivost, integritet i dostupnost

[725] ITU, *Definition of Cybersecurity*, http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx (preuzeto 6. januara 2016).

[726] International Telecommunication Union, ITU-T X.1205 (04/2008), 2008, 3.2.5, Termite 6L - Terminology of Telecommunications - V.7, Updated 2014, http://www.itu.int/online/termite/index.html (preuzeto 6. januara 2016).

[727] Godwin, Kulpin, Rauscher and Yaschenko, eds., *Russia-U.S. Bilateral*, 33.

[728] United States of America, *Department of Defense Instruction, 8500.01* (March 14, 2014), 55.

[729] Совет Федерации, Федералыного Собрания Российской Федерации, *Концепция стратегии кибербезопасности Российской Федерации - Проект*, (10 января 2014), 2, http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf (preuzeto 5. januara 2016).

[730] Government of Israel, Resolution No. 3611: Advancing National Cyberspace Capabilities, 2011, 1 http://www.pmo.gov.il/English/PrimeMinistersOffice/DivisionsAndAuthorities/cyber/Documents/Advancing%20National%20Cyberspace%20Capabilities.pdf

informacija u sajber prostoru. Sajber bezbednost nastoji da zaštiti kritičnu infrastrukturu“.[731]

Po nezvaničnoj definiciji Ministarstva unutrašnje bezbednosti SAD, sajber bezbednost je „aktivnost ili proces, sposobnost ili spremnost, ili stanje u kome su informacioni i komunikacioni sistemi i informacije u njima zaštićeni od i/ili branjeni od štećenja neautorizovane upotrebe ili iskorišćavanja“[732].

Po *Rečniku za nacionalno informaciono obezbeđenje*, *Komiteta za nacionalne bezbednosne sisteme*[733], kao i po *Rečniku ključnih termina informacione bezbednosti* NIST instituta, sajber bezbednost je „sposobnost zaštite ili odbrane upotrebe sajber prostora od sajber napada“, [734].

Na osnovu navedenih definicija može se utvrditi da se u svim slučajevima sajber bezbednost odnosi na primenu, stanje ili sposobnost uspostavljanja informacione bezbednosti u sajber prostoru, koji nastaje umrežavanjem pojedinačnih informacionih sistema. To se, bez izuzetaka, potvrđuje u svim navedenim definicijama, a ističe se i posredno u nekim. Na primer, ruska definicija pominje da se sajber bezbednost odnosi na stanje zaštite od maksimalnog broja pretnji, a dosadašnja praksa informacione bezbednosti u svetu je pokazala da nije moguće zaštititi se od svih pretnji u području informacione bezbednosti. Ukoliko svaki računarski informacioni sistem ima sposobnost povezivanja sa drugim računarskim informacionim sistemima, to znači da se informaciona i sajber bezbednost poklapaju. Međutim, praksa pokazuje da takav zaključak nije u svakom slučaju važeći, iako je u praktičnom pogledu najčešći.

---

[731] Patryk Pawlak, ed., *Riding the Digital Wave: The Impact of Cyber Capacity Building on Human Development* (report), (Paris: Institute for Security Studies, 2014, http://www.iss.europa.eu/uploads/media/Report_21_Cyber.pdf, 73, (preuzeto 11. februara 2015).

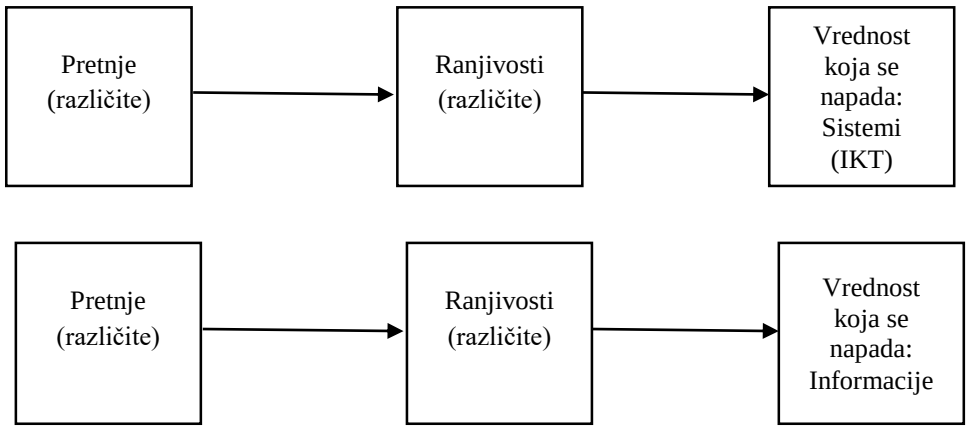
[732] United States of America, Department of Homeland Security, National Initiative for Cybersecurity Careers and Studies, “Explore Terms: A Glossary of Common Cybersecurity Terminology,” http://niccs.us-cert.gov/glossary

[733] United States of America, Committee on National Security Systems, National Information Assurance Glossary, 2010, 22, http://www.ncix.gov/publications/policy/docs/CNSSI_4009.pdf

[734] Richard Kissel, National Institute of Standards and Technology Glossary of Key Information Security Terms, U.S. Department of Commerce, 2013, 58, http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

Van Solms i Niekerk pružaju objašnjenje u čemu je razlika između informacione i sajber bezbednosti, uključujući i nekoliko drugih odgovarajućih vrsta bezbednosti.[735] Po njima, navedene pojmove ne treba posmatrati po analogiji kao uzajamno zamenjive, već suštinski različite, jer se odnose na različite sadržaje i područja. Dok se sajber bezbednost odnosi na sve elemente sajber prostora (koji uključuju sisteme, informacije i ljude), informaciona bezbednost se odnosi na bezbednost informacija, bez obzira na prirodu i okruženje informacija (digitalno, analogno ili neelektronsko). Na primer, u sajber bezbednosti ljudi su kreatori, akteri, napadači mete napada, dok je u informacionoj bezbednosti njihova uloga uža, i odnosi se na aktere od kojih zavisi bezbednost informacija. Navedeni oblici bezbednosti se odnose na relevantne sadržaje, tako se „informaciona bezbednost" odnosi na bezbednost informacija, a „sajber bezbednost" na bezbednost u sajber prostoru. Pri tome postoje i druge, slične, ali ne identične vrste bezbednosti, poput bezbednost informaciono-komunikacionih tehnologija (IKT) i bezbednosti informacionih tehnologija (IT), koje se odnose na bezbednost odgovarajućih tehnologija.

Po njihovom modelu, koji se sastoji od pretnji, ranjivosti i vrednosti koje se štite, IKT bezbednost predstavlja očuvanje bezbednosti u procesu u kome različite pretnje ugrožavaju različite ranjivosti koje postoje u IKT sistemima.



Slika 22. Model IKT i informacione bezbednosti po Van Solmsu i Niekerku.[736]

[735] Rossouw von Solms and Johan van Niekerk. "From Information Security to Cyber Security." *Computers and Security* 38, (October 2013): 97-102.

[736] Ibid, 99.

Po standardu ISO/IEC 13335-1:2004, IKT bezbednost predstavlja „sve aspekte u odnosu na definisanje, dostizanje, održavanje poverljivosti, integriteta, dostupnosti, neporecivosti, odgovornosti, autentičnosti i pouzdanosti informaciono-komunikacionih tehnologija“[737] Imajući u vidu navedenu definiciju, Van Solms i Niekerk[738] zaključuju da je IKT bezbednost podkomponenta informacione bezbednosti.

U sajber prostoru postoji više mogućih scenarija napada koji mogu, ali ne moraju da predstavljaju ugrožavanje informacione bezbednosti. Na primer, po Van Solmsu i Niekerku, pri informacionom psihološko-propagandnom delovanju u sajber prostoru nisu ugrožena svojstva dostupnosti, poverljivosti i integriteta informacija ili podataka u sajber prostoru, već je sama osoba predmet napada (na primer pri maltretiranju[739] na društvenim mrežama u sajber prostoru). Pri narušavanju autorskih prava na Internetu, razmenom digitalnih sadržaja ili krađom intelektualne svojine u sajber špijunaži, žrtava sajber napada (kriminala) ima više, pri čemu ponovo nije nužno narušena poverljivost, integritet i dostupnost informacija, već ekonomska i vlasnička prava nad tim informacijama.

Razlog za često preklapanje značenja ova dva područja je u tehnološkom trendu da se većina savremenih informacija nalazi u IKT okruženju. U teoriji postoji razlika između IKT i IT bezbednosti, s obzirom na tehnološku konvergenciju IKT i IT sistema. Da bi se ostvarila bezbednost informacija u IKT okruženju, neophodno je zaštiti tehnologije (tehničke sisteme koji su zasnovana na tim tehnologijama) koje su upotrebljene za čuvanje, obradu i transmisiju tih informacija.[740]

Po analogiji pristupa, razlikuje se i bezbednost podataka i informacija. Po Rečniku Ministarstva odbrane SAD, podatak je „skup vrednosti dodeljenih osnovnim i izvedenim

[737] *ISO/IEC 13335-1:2004, Information technology — Security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security*, 3.

[738] Von Solms and Van Niekerk. "Information Security to Cyber Security", 98.

[739] Eng. *cyber bullying*

[740] Center for Cyber and Information Security (CCIS), „Cyber Security Versus Information Security“, https://ccis.no/cyber-security-versus-information-security/, (preuzeto 22. maja 2014).

merama[741] i/ili indikatorima“[742], odnosno „1. osnovna jedinica informacija izgrađena na standardnoj strukturi koja ima jedinstveno značenje i razlikuje jedinice i vrednosti; 2. u elektronskom pohranjivanju podataka, kombinacija karaktera ili bajtova koji se odnose na odvojenu informaciju, poput imena, adrese ili godišta.“[743]

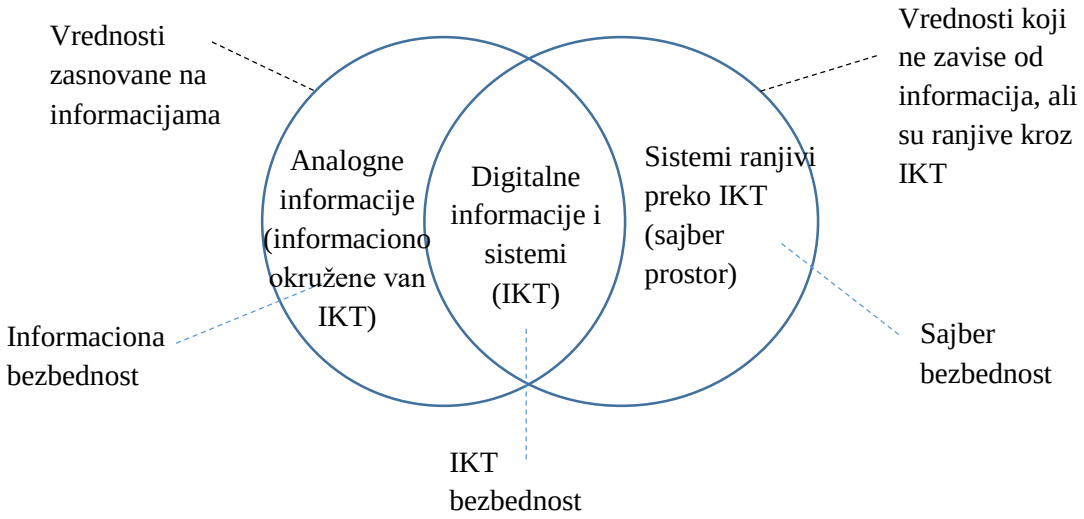
Dakle, podatak predstavlja vrednost nečega, dok informacija predstavlja podatak sa kognitivnim značenjem koji je moguće interpretirati u kontekstu (razumljivom za čoveka ili za inteligentni sistem). Zbog toga u praksi govorimo o informacionoj bezbednosti, a ne o bezbednosti podataka (iako i ona postoji) jer bezbednost podataka kojima niko ne zna značenje ne predstavlja opasnost po njihovog vlasnika. Na primer kriptografijom se informacije prevode u formu podataka, pri čemu samo vlasnik informacija zna ključ po kome je to učinjeno.

Po norveškom Centru za sajber i informacionu bezbednost, sve informacije u svetu se mogu podeliti na digitalne (zasnovane na IT) i nedigitalne (analogne). Pored toga, postoji i skup IKT sistema (softverski i hardverski), koji imaju ranjivosti koje ih čine podložnim narušavanju bezbednosti. Predmet bavljenja prvog skupa je informaciona bezbednost, a drugog sajber bezbednost. Skup IKT sistema se sastoji od informacija (koje postoje u tim sistemima) i samih tehničkih sistema (bez informacija). Informacije koje nisu digitalne prirode (analogne ili materijalno predstavljene) mogu takođe biti (posredno) podložne narušavanju bezbednosti kroz IKT uređaje. Centar predlaže podelu informacione, IKT (IT) i sajber bezbednosti po šemi prikazanoj na slici 23.

[741] Osnovna mera predstavlja atribut (stanje ili karakteristiku objekta koja se može kvalitativno ili kvantitativno razlikovati) nečega i metodu za njegovo kvantitativno predstavljanje. Izvedena mera predstavlja meru koja je funkcija dve ili više osnovnih mera. Mera predstavlja varijablu koja je dodeljena nekoj vrednosti merenja. Merenje je proces određivanja vrednosti nečega. Indikator predstavlja meru koja pruža procenu ili ocenu specifičnog atributa izvedenog iz analitičkog modela u odnosu na definisane potrebe za informacijama. ISO/IEC 27000:2016(en).

[742] ISO/IEC 2700:2016(en), 2.20. data.

[743] *Department of Defense Dictionary of Military and Associated Terms: Joint Publication 1-02,* Washington, DC: Joint Chiefs of Staff, 2010 (As Amended Through 15 January 2015), 59.



Slika 23. Odnos informacione i sajber bezbednosti.[744, 745]

Dakle, u bilo kom slučaju specifične bezbednosti, uvek postoji zaštita neke vrednosti od različitih pretnji koje iskorišćavaju određeni skup ranjivosti vezanih za tu vrednost ili sistem koji nosi vrednost. IKT bezbednost obuhvata zaštitu IKT sistema, informaciona bezbednost zaštitu informacija (u kontekstu koji je širi od skupa IKT sistema), dok sajber bezbednost obuhvata svaku vrednost koja može biti ugrožena delovanjem kroz ili u sajber prostoru (ljudi, sistema, informacija) i ima najširi mogući opseg značaja, od ličnog do nacionalnog. [746] Pri tome se treba imati u vidu da sajber prostor primarno sačinjavaju računarske informacione tehnologije. Takođe, sajber bezbednost predstavlja proširenje područja informacione bezbednosti (posmatrano iz konteksta sajber prostora), jer se pored informacija, i informacionih sistema, odnosi i na nemerljive i nematerijalne vrednosti i oblike ugrožavanja njihove bezbednosti (poput shvatanja, volje, ugleda, ekonomskih vrednosti i drugih). Takođe, po Van Solmsu i Niekerku, informacije u sajber prostoru, same po sebi, mogu predstavljati ranjivosti podložne napadu agenta pretnje.[747] Međutim, iz ugla oružanih sukoba među nacijama i međunarodnog prava koje ih reguliše, navedeni

[744] CCIS, „Cyber security versus information security.“

[745] Von Solms and Van Niekerk. "Information Security to Cyber Security."

[746] Ibid, 100.

[747] Ibid, 101.

oblici ugrožavanja u okviru sajber bezbednosti se moraju razlikovati od napada, agresije i oblika ispoljavanja sile u skladu sa odredbama međunarodnog prava. Zbog toga se kao zaključak može navesti da, niti je svaki sajber napad (u smislu ugrožavanja mete napada) ujedno i ugrožavanje informacione bezbednosti, niti je svako ugrožavanje informacione bezbednosti ujedno i sajber napad. Konačno, u smislu međunarodnog prava nema svaki sajber napad karakter oružanog napada ili oblika ispoljavanja agresije.

Na osnovu stavova Von Solmsa and Van Niekerka, CCIS, kao i analize prethodno navedenih definicija informacione, IKT i sajber bezbednosti, može se doneti sledeći zaključak. U sva tri slučaja postoje faktori pretnji, sistemi kojima je bezbednost potencijalno ugrožena i ranjivosti koje omogućavaju to ugrožavanje. Takođe, u svim slučajevima se radi o ugrožavanju svojstava informacione bezbednosti: integriteta, poverljivosti, dostupnosti, neporecivosti i autentičnosti. Ta svojstva se uvek odnose na informacije, ali i na informacione sisteme. Ono što se razlikuje između navedenih koncepata jeste **primarni** (ne osnovni ili konačni) **cilj**, odnosno **vrednost** koja se štiti od napadača i koju napadači primarno ugrožavaju, odnosno preovlađujući kontekst – okruženje u kome se ugrožavanje informacione bezbednosti. U informacionoj bezbednosti to su informacije u opštem kontekstu; u IKT bezbednosti to su IKT sistemi koji čuvaju, stvaraju i obrađuju informacije; u sajber bezbednosti to su informacije i sistemi u kontekstu i okruženju umreženog sajber prostora.

10. PRIMER SJEDINJENIH AMERIČKIH DRŽAVA

SAD su ključni inicijator, kreator i pokretač razvoja i informaciono-komunikacionih tehnologija u području bezbednosti i odbrane. Razvoj i primena informaciono-komunikacionih tehnologija u SAD su započele su još tokom Drugog svetskog rata, što je a nastavljeno tokom Hladnog rata. Od devedesetih godina 20. veka u SAD su nastali i koncepti informacionog i sajber ratovanja, usvojena je prva vojna doktrina operacija u sajber prostoru, sajber prostor je proglašen petim područjem ratovanja i izgrađeni su prvi nacionalni strategijski kapaciteti za izvođenje vojnih operacija u sajber prostoru, kao i odgovarajuće vojne komande za dejstva u sajber prostoru i jedinice po dubini.

Zbog svega navedenog, sa razlogom se može reći da su SAD savremeni predvodnik vojne primene sajber prostora u svetu, koji svojim aktivnostima diktira razvoj, primenu i regulisanje vojne upotrebe sajber prostora. Na primeru SAD se najlakše mogu videti dosadašnji trendovi razvoja kapaciteta za sajber ratovanje, konvergencija državnih i privatnih kapaciteta i interesa u tom pravcu, kao i veza između odbrane nacije spolja i uspostavljanja unutrašnje nacionalne bezbednosti. Referentna nacionalna institucija u pogledu definisanja sajber napada i sajber oružja na nacionalnom nivou je Ministarstvo odbrane SAD. Njegov godišnji budžet za potrebe sajber odbrane je veći od svih javno poznatih odgovarajućih budžeta drugih država na svetu.[748, 749]

Imajući navedeno u vidu, od praktične koristi može biti analiza specifičnog pristupa SAD u izgradnji i primeni kapaciteta za izvođenje vojnih aktivnosti u sajber prostoru.

[748] U.S. Office of Management and Budget, *Fiscal Year 2016, Budget, of the U.S. Government*, https://www.whitehouse.gov/sites/default/files/omb/budget/fy2016/assets/budget.pdf (preuzeto 1. marta 2016).

[749] Aliya Sternstein, „The Military's Cybersecurity Budget in 4 Charts", *Defense One*, March 16, 2015, http://www.defenseone.com/management/2015/03/militarys-cybersecurity-budget-4-charts/107679/ (preuzeto 20. decembra 2015).

10.1. Razvoj shvatanja sajber prostora i odbrambeno-bezbednosnih aktivnosti u sajber prostoru u SAD

U okviru Vlade SAD ne postoji jedna jedinstvena definicija sajber prostora, već ovaj koncept različito definišu dokumenti različitih vladinih agencija i organa. Nacionalna strategija operacija u sajber prostoru SAD definiše sajber prostor kao: „područje za koje je svojstvena upotreba elektronskih uređaja i elektromagnetnog spektra radi čuvanja, modifikovanja i razmene podataka putem umreženih sistema i odgovarajuće fizičke infrastrukture“[750]. Sajber prostor i aktivnosti u njemu su od rastućeg značaja za društvo, ekonomiju i bezbednosti i odbranu SAD, pa se stoga sve češće definiše na opštiji način, tako da zadovoljava širi krug učesnika i aktivnosti. Po mišljenju Kongresne istraživačke službe (eng. *Congressional Research Service*), sajber prostor je definisan u najširem mogućem smislu i predstavlja: “Sveukupnu međupovezanost ljudskih bića pomoću računara i telekomunikacionih sistema, bez obzira na njihov fizički položaj“[751].

Sa razvojem kapaciteta, vremenom se razvijalo shvatanje koncepta sajber napada. Po *Rečniku vojnih termina Ministarstva odbrane SAD* iz 1999. godine, računarski mrežni napad (eng. *Computer Network Attack* – CNA) je definisan kao: „operacija u cilju poremećaja, onesposobljavanja, degradacije ili uništavanja informacija koje se nalaze u računarima i računarskim mrežama ili samih računara i računarskih mreža“[752]. Ovakve operacije mogu biti deo specijalnih informacionih operacija koje imaju za opšti cilj uticaj na proces donošenja odluka protivnika.[753]

Dopunjeno izdanje ovog rečnika iz 2002. godine dodatno razlikuje računarske mrežne napade od elektronskih napada, ističući da elektronski napad (na primer, dejstvo usmerenom energijom ili emitovanjem ometajućeg elektromagnetnog zračenja) može onesposobiti računar, ali da nema karakter računarskog mrežnog napada.[754] Ova

[750] United States Department of Defense, Joint Chiefs of Staff, *National Military Strategy for Cyberspace Operations*, ix, http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-023.pdf (preuzeto 14. decembra 2013).

[751] Steven A. Hildreth, *Cyberwarfare* (CRS Report No. RL 30735) (Washington, DC: Congressional Research Service,2001), http://www.fas.org/irp/crs/RL30735.pdf, 1.

[752] *Department of Defense Dictionary of Military and Associated Terms: Joint Publication 1-02,* Washington, DC: Joint Chiefs of Staff, 1994 (as amended through 6 April 1999), 95.

[753] Ibid, 320.

[754] *Department of Defense Dictionary of Military and Associated Terms, Joint Publication 1-02,* Washington, DC: Joint Chiefs of Staff, 2001, (as amended through 14 August 2002), 93.

napomena je značajna, jer računarske mrežne napade (kasnije nazvane sajber napadima) označava logičkim dejstvima (izvršenje napada se ostvaruje tokom podataka), dok su elektronski napadi fizička dejstva (zasnivaju se na elektromagnetnom spektru, koji iako nema materijalnu, već fizičku prirodu, postoji u fizičkom okruženju).

U svrhu početnog definisanja određenih vojnih aktivnosti, pojam „sajber" se pojavio u doktrinarnim dokumentima Ministarstva odbrane SAD u izdanju Rečnika iz 2002. godine, u kome je definisan kao „konceptualno okruženje u kome digitalizovane informacije komuniciraju kroz računarske mreže"[755] U periodu od narednih 11 godina, sve do objavljivanja *Združene publikacije 3-12 (R) – Operacije u sajber prostoru*[756], definicije sajber napada, operacije u sajber prostoru i drugih odgovarajućih aktivnosti su značajno evoluirale i dodatno precizirane. Po pomenutom vojnom dokumentu, koji predstavlja prvi sveobuhvatni doktrinarni dokument namenjen isključivo za vojna dejstva u sajber prostoru, operacije u sajber prostoru predstavljaju: „primenu sposobnosti u sajber prostoru čija je primarna svrha ostvarivanje ciljeva u sajber prostoru i kroz sajber prostor"[757]. Ti ciljevi se mogu prepoznati kroz funkcije koje su dodeljene Sajber komandi[758], delu Strateške komande Ministarstva odbrane SAD[759]. Po Doktrini združenih operacija Ministarstva odbrane SAD, Sajber komanda razvija sposobnost da vodi sveobuhvatne vojne operacije u sajber prostoru kojima se omogućava sloboda vojnog dejstva SAD (u sajber prostoru) i omogućavaju (vojne) aktivnosti u svim drugim okruženjima (na kopnu, moru, u vazduhu i svemiru), uz istovremeno onemogućavanje

[755] *Joint Publication 1-02*, 116.

[756] *Cyberspace Operations: Joint Publication 3-12*, Washington, DC: U.S. Joint Chiefs of Staff, 2013, http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf.

[757] *Joint Operations, Joint Publication 3-0*, Washington, DC: U.S. Joint Chiefs of Staff, 2011, IV-3.

[758] *United States Cyber Command* (USCYBERCOM).

[759] *United States Strategic Command* (USSTRATCOM) – je jedna od devet objedinjenih borbenih (operativnih) komandi Ministarstva odbrane SAD, čije područje aktivnosti su operacije u svemiru; informacione operacije; raketna odbrana; globalno komandovanje i rukovođenje; obaveštajne i izviđačke aktivnosti; elektronski nadzor; nuklearno strategijsko odvraćanje i borba protiv oružja za masovno uništenje. Strateška komanda je jedna od tri objedinjene komande američkog Ministarstva odbrane koje su organizovane na funkcionalnoj osnovi (ostalih šest su regionalno-geografskog karaktera), sa osnovnom misijom da: odvraća napade na američke vitalne interese; obezbedi slobodu akcije u svemiru i sajber prostoru; ostvaruje integrisane kinetičke i nekinetičke vojne efekte (dejstva napada) kao podršku operacijama združenih vojnih komandi; sinhronizuje borbu protiv oružja za masovno uništenje na geografskom regionalnom nivou i da obezbedi integrisani obaveštajni rad, izviđanje i elektronski nadzor. Jedna od ključnih funkcionalnih komandi Strateške komande je Sajber komanda, čiji je komandat ujedno i direktor Nacionalne bezbednosne agencije (*National Security Agency* – NSA), vodeće organizacione celine u svetu, koja razvija i sprovodi sposobnosti za izvođenje operacija u sajber prostoru, uključujući i sajber napade.

odgovarajućih protivničkih aktivnosti.[760] Za analizu značaja sajber ratovanja je važno primetiti činjenicu da je vodeća vojna sila sveta, istoj vojnoj komandi[761] dodelila nadležnosti za komandovanje nuklearnim snagama, i izvođenje vojnih operacija u sajber prostoru i informacionih operacija.

Navedena definicija operacije u sajber prostoru je konceptualno jasna, jer obuhvata većinu aktivnosti napada primenom informaciono-komunikacionih tehnologija, ali nije precizna u vojno-doktrinarnom pogledu. U doktrini operacija Ministarstva odbrane SAD razlikuju se sajber i informacione operacije. Informacione operacije predstavljaju „integrisanu primenu informaciono-zasnovanih sposobnosti, koje se kroz vojne operacije primenjuju zajedno sa svim drugim vrstama operacija u cilju uticaja, ometanja, narušavanja ili uzurpiranja procesa donošenja odluka trenutnih i potencijalnih protivnika, istovremeno štiteći vlastiti proces donošenja odluka".[762] Informacione operacije se dakle, odnose na informaciono i kognitivno područje u kome se donose odluke. One predstavljaju primenu aktivnosti u psihološko-medijsko-propagandnom području (takozvanoj informacionoj sferi) koje se preduzimaju podjednako i u fizičkom i u sajber okruženju. Dakle, prvenstveno se odnose na delatnost koja se tiče informacionih aktivnosti. S druge strane, sajber operacije se odnose na okruženje, jer predstavljaju primenu sposobnosti koje se odnose na sajber prostor (i primenu informaciono-komunikacionih tehnologija) sa ciljem da se ostvare efekti koji podržavaju sve vrste vojnih operacija koje se izvode u fizičkom ili sajber okruženju.

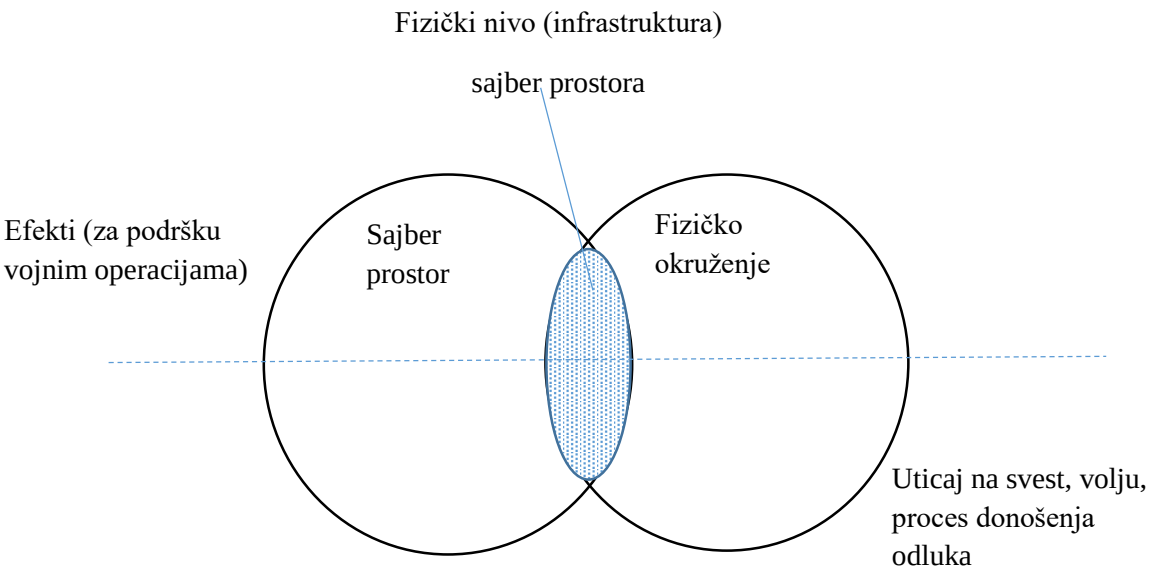
Ovakav stav predstavlja jasnu evoluciju u odnosu na raniji, delimično nejasan stav iz prve decenije 21. veka, po kome su operacije u sajber prostoru (sajber operacije) samo jedna od aktivnosti u okviru informacionih operacija. U početku razvoja vojnih doktrina koje se odnose na informacije, sajber aktivnosti su shvatane kao deo informacionih aktivnosti, dok se u savremenom dobu one u potpunosti razdvajaju, i zasnivaju se na različitim polaznim osnovama. Sa razvojem informaciono-komunikacionih tehnologija, sajber prostor je evoluirao od podskupa informacionog područja do potpuno samostalnog područja koje istovremeno ima osnovu i ostvaruje efekte na tri različita konceptualna

[760] Joint Publication 3-0, Washington, III-10.

[761] *United States Strategic Command* (USSTRATCOM).

[762] *Information Operations, Joint Publication 3-13,* (Washington, DC: U.S. Joint Chiefs of Staff, 2014), GL-3, http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf

nivoa: fizičkom, logičkom i informaciono-saznajnom. Istovremeno, informacione operacije su zadržale pređašnje značenje.



Slika 24. Razlika između sajber operacija i informacionih operacija po doktrini Ministarstva odbrane SAD.[763]

U skladu sa opštom doktrinom vojnih operacija, ispoljavanje sposobnosti u sajber prostoru se sastoji u preduzimaju ofanzivnih i defanzivnih operacija, kao i više različitih vrsta operacija koje se odnose na borbenu podršku i borbeno obezbeđenje u vezi primene i funkcionisanja jedinstvene informacione mreže Ministarstva odbrane SAD.[764]

Sposobnosti za izvođenje efekata u sajber prostoru se menjaju u skladu sa razvijem tehnologije, koja predstavlja ključni faktor u evoluciji sajber ratovanja. To se dešava velikom brzinom, u skladu sa brzinom razvoja tehnologije i razvojem sposobnosti za ostvarivanje raznih efekata. Po navedenoj Doktrini operacija u sajber prostoru, Ministarstvo odbrane SAD razlikuje ofanzivne, defanzivne i operacije obezbeđenja i podrške jedinstvene informacione mreže. U smislu Međunarodnog prava oružanih sukoba, od primarnog značaja su one operacije u sajber prostoru u kojima se ispoljava

[763] *Joint Publication 3-12*, I-5.
[764] Ibid, II-1 – II-6.

sila, vrši agresija, ili ostvaruje napad. Ofanzivne operacije u sajber prostoru su nedvosmisleno vojne operacije u kojima se manifestuje vojna moć primenom sile u sajber prostoru i kroz sajber prostor.[765] Sila se može primeniti u različitim okolnostima, za napad, odbranu ili odvraćanje. Odbrambene operacije u sajber prostoru imaju za cilj odbranu sposobnosti, informacija, sistema, mreža i kapaciteta u sopstvenom i savezničkom sajber prostoru,[766] koja se ostvaruje kroz aktivne i pasivne operacije.

Po Doktrini sajber operacija Ministarstva odbrane SAD, pored **operacija** u sajber prostoru, koje su klasifikovane po nameri i svrsi (cilju), karakter primene sile imaju i takozvana vojna **dejstva** (akcije) u sajber prostoru (eng. *cyberspace actions*), koja su klasifikovana u odnosu na efekte koje izazivaju (kao posledica primene odgovarajućih sposobnosti).[767] Ključno dejstvo koje predstavlja akt primene sile u sajber prostoru je napad u sajber prostoru. Napad u sajber prostoru je „dejstvo koje stvara različite direktne efekte **onemogućavanja** u sajber prostoru (degradaciju, poremećaj funkcionisanja ili uništenje) ili **manipulaciju** koja izaziva prikriveno onemogućavanje ili se manifestuje u fizičkom okruženju“[768] (Tabela 12).

Dakle, specifičnu ciljevi napada su:

a) onemogućavanje protivnika da raspolaže vlastitim resursima sprečavanjem pristupa, funkcionisanja ili dostupnosti, onda kada su mu potrebni u određenom trenutku i u određenoj meri;
b) manipulacija protivničkim informacijama, sistemima i mrežama ostvarena kontrolom ili izmenom u skladu sa ciljevima napadača.

Posledice koje sajber napad ostvaruje po mete su:

---

[765] *Joint Publication 3-12,* II-2.

[766] U navedenom pogledu, sajber prostor koji se brani se posmatra kao područje koje pripada nekome, koje je u nečijoj nadležnosti. U tom smislu, od značaja je fizička komponenta sajber prostora (u kojoj funkcionišu lica i nalaze se uređaji i informaciona infrastruktura), logička komponenta (koja se odnosi na komunikaciju i obradu informacija, procese i servise u sajber prostoru) i kognitivna komponenta (u kojoj se dešava proces saznavanja, shvatanja, donošenja odluka i svesti lica u nadležnosti sopstvenog društvenog sistema).

[767] U tom pogledu, akcije u sajber prostoru se u Doktrini sajber operacija MO SAD dele na:
a) odbranu u sajber prostoru;
b) obaveštajni rad, nadzor i izviđanje u sajber prostoru;
c) operativnu pripremu okruženja (bojišta) u sajber prostoru i
d) napad u sajber prostoru.

[768] *Joint Publication 3-12,* II-5.

- degradacija protivničkih resursa, čime se protivnik ograničava da pristupi nekom resursu ili njegovoj funkciji u punoj meri;
- onesposobljavanje, tokom koga se onemogućava pristup protivnika nekom resursu ili njegovom funkcionisanju u potpunosti, ali u ograničenom periodu vremena;
- uništavanje, čime se trajno, potpuno i nepovratno onemogućava protivniku da pristupi vlastitom resursu i
- kontrola ili izmena protivničkih informacija, informacionih sistema i mreža.

Tokom devedesetih godina 20. veka u strategiji odbrane SAD je pokrenuta ideja da su novi tehnološki i društveni koncepti, među kojima su i široka primena informaciono-komunikacionih tehnologija, omogućili da se tradicionalno jasna razlika između ratnih sukoba i mirnodopskih odnosa sasvim promeni[769, 770]. Ovu ideju je posebno predlagao rastući pokret pristalica neoliberalnih političkih rešenja u međunarodnim odnosima koji je bio dobro prihvaćen od strane svih predsedničkih administracija u SAD, a posebno onih iz Demokratske partije.[771]

U tom periodu, primena informaciono-komunikacionih tehnologija je postala privlačan izbor za široki krug donosilaca odluka, stratega i stručnjaka. One su se mogle istovremeno upotrebiti u cilju manifestacije „meke“ moći, privlačenjem drugih nacija političkim idejama SAD, kroz primenu diplomatije i širenje američke kulture u svetu, kao i u cilju ostvarivanja „tvrde“ moći, ostvarivanjem prvih destruktivnih vojnih operacija u sajber prostoru, odnosno intenzivnim razvojem špijunaže i nadzora svih građana u svetu.

[769] Dragan Mladenović, Danko Jovanović, Mirjana Drakulić, „Tehnološki, vojni i društveni preduslovi primene sajber ratovanja“, *Vojnotehnički glasnik*, 1 (2012), 70-98.

[770] John Arquilla and David Ronfeldt, eds., *In Athena's Camp, Preparing For Conflict in the Information Age* (Santa Monica, CA: Rand Corporation, 1997).

[771] U periodu Klintonove administracije, autor koncepta primene „meke“ i „pametne“ moći u međunarodnim odnosima, Džozef Naj, tada predsedavajući Nacionalnog obaveštajnog veća, i pomoćnik državnog sekretara odbrane za međunarodnu bezbednost je ostvarivao veliki uticaj na američku spoljnu politiku. Danijel Drezner je o njemu napisao u uticajnom časopisu Foreign Policy sledeće: „Svi putevi za shvatanja spoljne politike SAD idu preko Džozefa Naja“.

Daniel W, Drezner, „Get Smart; How to Cram for 2012,“ *Foreign Policy*, June 20, 2011, http://www.foreignpolicy.com/articles/2011/06/20/get_smart_how_to_cram_for_2012 (preuzeto 12. avgusta 2015.

Tabela 12. Karakteristike i svojstva operacija i dejstava u sajber prostoru.

Na osnovu podataka objavljenih u dokumentu: Cyberspace Operations: Joint Publication 3-12 (R), Department of Defense, (2013, February 5). Washington, DC: Joint Chiefs of Staff, II-2 – II-5.

Vrsta aktivnosti	Delovanje	Status	Aktivnost	Gde
Operacije u sajber prostoru (orjentisane na sopstvene mreže i sajber prostor)				
Ofanzive operacije u sajber prostoru	Sajber napad	Ima status primene sile	Aktivnosti u sajber prostoru	U sajber prostoru i kroz sajber prostor
Defanzivne operacije u sajber prostoru	Pasivna odbrana	Nema status primene sile	– Interne odbrambene mere – Vojni odgovor ka eksternim izvorima pretnji i napada (nedestruktivne protivmere i protivmere sa uticajem na agenta pretnje koje podležu pravilima angažovanja vojne sile)	Aktivnosti u sajber prostoru i fizičkom okruženju (na primer, odgovor kinetičkom silom na sajber napad ili preventivne fizičke mere zaštite)
	Aktivna odbrana, vojni odgovor	Može imati status primene sile		
Operacije vezane za jedinstvenu informacionu mrežu	Podrška, obezbeđenje	Nema status primene sile	Informaciono obezbeđenje stvaranje i očuvanje integriteta, poverljivosti, dostupnosti informacija i autentifikacije i neporecivosti korisnika i entiteta	U okviru sopstvene informacione mreže u sajber prostoru i u fizičkom okruženju
Bezbednost nevojnih informacionih mreža (od značaja za vojnu funkciju)	Podrška, obezbeđenje	Nema status primene sile	Informaciono obezbeđenje	U okviru nevojnih informacionih mreža
Rutinska upotreba sajber prostora				
Obaveštajne operacije				
Dejstva u sajber prostoru	Odbrana u sajber prostoru		Zaštita, otkrivanje i, utvrđivanje pretnji, protivdejstvo, sprečavanje,	
	Obaveštajne aktivnosti, elektronski nadzor i izviđanje u sajber prostoru	Nema status primene sile	Podrška i obezbeđenje	Neprijateljski i neutralni sajber prostor
	Operativna priprema vojnog okruženja	Nema status primene sile	Obezbeđenje	Neprijateljski i neutralni sajber prostor
	Napad u sajber prostoru	Ima status primene sile	Onemogućavanje (degradacija, poremećaj, ometanje pristupa cilju, sprečavanje funkcionisanja ili dostupnosti cilja) ili manipulacija kojom se kontrolišu ili izmenjuju protivničke informacije, informacioni sistemi i mreže (radi sprečavanja protivnika da koristi vlastite resurse)	

Ovaj trend je rezultirao intenzivnim razvojem institucionalnih, doktrinarnih i operativnih sposobnosti od strane američkog Ministarstva odbrane. Iako Vlada SAD nikada nije zvanično priznala i prihvatila autorizaciju izvođenja dugogodišnje operacije u sajber prostoru u kojoj su na sistematičan način korišćeni zlonamerni programi Staksnet (eng. *Stuxnet*), Flejm (eng. *Flame*), Dukju (eng. *Duqu*) i drugi, opšti stav svetske i američke javnosti je da su to učinile nadležne odbrambene agencije SAD u saradnji sa izraelskim agencijama.[772] Navedena operacija je imala strategijski karakter, jer su tokom nje na duži period onesposobljeni ključni sistemi za obogaćivanje uranijuma Irana, potrebni za razvoj strategijskih nuklearnih resursa[773]. U periodu nakon uspostavljanja Sajber komande 2009. godine, započeo je i intenzivan rast dodeljivanja budžetskih sredstava za razvoj kapaciteta za obaveštajni rad i obranu u sajber prostoru.[774]

10.2. Mešanje nadležnosti u oblastima odbrane i bezbednosti

Slučaj SAD predstavlja karakterističan primer kako su poslovi odbrane i nacionalne bezbednosti u sajber prostoru postali isprepletani i funkcionalno povezani. Odbranom nacije se bavi Ministarstvo odbrane[775], spoljnim obaveštajnim i tajnim operacijama specijalizovane agencije poput CIA[776], a poslovima unutrašnje bezbednosti i sprovođenja zakona veći broj agencija, među kojima težišno Ministarstvo unutrašnjih poslova[777] i Ministarstvo pravde[778]. Međutim, funkcionalne nadležnosti navedenih ministarstva i agencija su u praksi značajno pomešane i distribuirane, dok je praktična sposobnost za

[772] David E. Sanger, „Obama Order Sped Up Wave of Cyberattacks Against Iran," *The New York Times*, June 1, 2012, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r=0 (preuzeto 22. oktobra 2015).

[773] David Kushner, „The Real Story of Stuxnet," IEEE Spectrum, February 26, 2013, http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet (preuzeto 22. oktobra 2015).

[774] James Bamford, „NSA Snooping Eas Only the Beginning, Meet the Spy Chief Leading Us Into Cyberwar", *Wired*, June 12, 2013, http://www.wired.com/2013/06/general-keith-alexander-cyberwar/ (preuzeto 20. maja 2015).

[775] Eng. *Department of Defense*

[776] Eng. *Central Intelligence Agency*

[777] Eng. *Department of Homeland Security*

[778] Eng. *Department of Justice*

izvođenje operacija u sajber prostoru skoncentrisana u okviru Nacionalne obaveštajne agencije (NSA)[779].

Nakon završetka Hladnog rata, početkom devedesetih godina 20. veka, agencija NSA se našla u potpuno novom okruženju i stanju. NSA je decenijama imala jednog protivnika (SSSR), da bi zatim zona njenih operacija ušla u stanje unipolarnog, a zatim i multipolarnog sveta, u kome se odigravaju brojni unutrašnji građanski sukobi, i raste pretnja od umreženih terorističkih organizacija. Međutim, organizaciona struktura i ciljevi NSA nisu bili tome prilagođeni.[780] NSA je u dugom periodu od osnivanja funkcionisala kao tradicionalna vojna organizacija, s obzirom da je oduvek bila agencija u okviru Ministarstva odbrane SAD.[781] U tom stabilnom okruženju koje se tehnološki sporo razvijalo, razvijana je specifična ekspertiza poznavanja jednog protivnika kroz njegovu organizaciju, procedure, sisteme i jezik. Takvo organizaciono usmerenje je zahtevalo temeljnost, stabilnost, duboku stručnost u jednom širem predmetu bavljenja, reputaciju i pouzdanost.[782]

Tokom narednog perioda od dve decenije, vrednosti organizacione kulture NSA su se sukcesivno menjale u skladu sa okruženjem i zadacima i vremenom su se približile vrednostima karakteristične poslovne organizacije, čiji je osnovni cilj da ostvari svoj „biznis“ u potpunosti, na najbolji mogući način, u zadatim rokovima i na zakonit način.[783] Da bi se to postiglo, u organizacionoj kulturi agencije su počele da se ističu vrednosti poput znanja, saradnje sa drugim agencijama u okviru Vlade i u inostranstvu, kao i sa privatnim kompanijama i organizacijama, inventivnosti, učenja, otvorenosti i izgradnje

[779] Eng. *National Security Agency*

[780] National Security Agency, „NSA Culture, 1980s to the 21st Century-a SID Perspective,“ *Cryptologic Quarterly*, 30, no. 4 (Winter/Spring 2011): 79-85, http://www.nsa.gov/public_info/_files/cryptologic_quarterly/nsa_culture.pdf (preuzeto 11. oktobra 2015).

[781] Ibid.

[782] Ibid.

[783] NSA Office of Public Affairs, *NSA/CSS Strategy* (2011), http://www.nsa.gov/about/_files/nsacss_strategy.pdf (preuzeto 11. oktobra 2015).

ekspertskog potencijala zaposlenih i poslovne orjentacije ka budućnosti.[784, 785, 786] Iako vojna agencija sa potrebom izrazite vertikalne hijerarhijske organizacije, NSA se transformisala u sistem zasnovan na način karakterističan za poslovne sisteme: organizaciju sposobnu za brze i adekvatne promene koja rukovodi finansijskim i tehnološkim resursima na najbolji mogući način.[787] Ta transformacija je posebno dinamično izvršena za vreme dok je agencijom rukovodio Majkl Hajden. NSA se tokom navedenog perioda, a posebno nakon terorističkog napada na SAD 2001. godine, transformisala u dinamičan sistem koji funkcioniše u okviru šireg sistema i sposoban je za brzo, gotovo trenutno donošenje odluka i preduzimanje potrebne akcije.

Međutim, taj proces je u celokupan sistem odbrane doneo poslovnu organizaciju sa skoro neograničenim resursima, i uveo je u sistem nedržavne aktere u vidu mnoštva privatnih specijalizovanih organizacija. Ti resursi su bili adekvatni postavljenim ciljevima američke spoljne politike u sajber prostoru. Sajber prostor je proglašen petim područjem vojnih aktivnosti.[788, 789] Deklarisani su ciljevi da SAD imaju lidersku poziciju u svetu u pogledu odbrambeno-bezbednosnih aktivnosti u sajber prostoru, koju će ostvariti personal obučen po najvišim standardima i opremljen najboljim tehničkim resursima i omogućiti sposobnost da se ostvare vitalni američki interesi u svetu.[790] Tako visoko postavljene ciljeve u globalnim okvirima ne može ispuniti ni jedan organizacioni sistem samostalno, čak i veći od NSA. Zbog toga je NSA ušla u program međunarodne i nacionalne saradnje sa prijateljskim strukturama na nacionalnom i međunarodnom nivou.

---

[784] Dragan Mladenovic, „SAF Organizational Culture and Cyber Defense Development“, (final paper for the Organizational Culture for Strategic Leaders OCL 15-01 course, Information Resources Management College, NDU, August 17, 2014).

[785] National Security Service, *National Security Agency/Central Security Service Core Values, Clear Vision,* 2010, http://www.nsa.gov/about/_files/CoreValues.pdf (preuzeto 26. februara 2016).

[786] NSA Office of Public Affairs, *NSA/CSS Strategy* (2010), http://www.nsa.gov/about/_files/nsacss_strategy.pdf (preuzeto 11. oktobra 2015).

[787] Richard Lardner, „NSA Overhauls Corporate Structure in Effort to Improve Operations,“ *Inside the Air Force*, 11, no. 25 (2000), http://cryptome.org/nsa-redo.htm (preuzeto 10. avgusta 2015).

[788] U.S. Department of Defense, *Strategy for Operating in Cyberspace*, July 2011, http://www.defense.gov/news/d20110714cyber.pdf, (preuzeto 15. decembra 2015), 5.

[789] „War in the Fifth Domain*,“ The Economist*.

[790] U.S. Department of Defense, *Cyber Strategy*, April 2015, http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf, (preuzeto 15. decembra 2015), 13-15.

U međunarodnom okvirima to su bile strane obaveštajne agencije u okviru vojno-obaveštajno-političke zajednice "Pet očiju"[791].

U nacionalnim okvirima poslovno-bezbednosno saradnja je uspostavljena sa mnoštvom privrednih, industrijskih, istraživačkih i akademskih organizacija koje se bave naučnim istraživanjem, tehnološkim razvojem i odbrambeno-bezbednosnom primenom informaciono-komunikacionih tehnologija u oblasti sajber bezbednosti i odbrane. Ta saradnja je u okviru američke nacije postojala znatno ranije i na neke negativne aspekte te saradnje po američku naciju i demokratiju je ukazivao još 1961. godine tadašnji američki predsednik, general Dvajt Ajzenhauer. U svom poslednjem obraćanju naciji u svojstvu predsednika on je istakao da postoji realna opasnost od negativnog uticaja interesa vojno-industrijskog kompleksa po američku naciju i demokratske procese, koja može nastupiti u odsustvu balansa unutar i između nacionalnih programa: "U većima vlasti moramo se braniti protiv sticanja neprimerenog uticaja, zahtevanog ili nezahtevanog, od strane vojno-industrijskog kompleksa"[792]. U pogledu nacionalnih vojno-bezbednosnih aktivnosti u sajber prostoru, ta specifična civilno-vojna saradnja je došla do najvišeg nivoa ikada.

Nakon terorističkog napada na SAD 2001. godine, nastupio je periodu takozvanog „rata protiv terora", koji je kulminirao pokretanjem ratova u Avganistanu (2001), koji predstavljaju najduže učestvovanje SAD u međunarodnom ratu u njenoj istoriji,[793] i rata u Iraku (2003). Po završetku glavnih vojnih dejstava, veza američke vlade i privatnog vojno-industrijskog kompleksa nije umanjena po intenzitetu i obimu, već po predmetu i sadržaju saradnje. Fokus saradnje je velikim delom prešao iz stanja rata u stanje mira, i iz fizičkog okruženja u sajber prostor, podjednako na međunarodnom i nacionalnom nivou. Istraživački tim medijske kompanije Vašington Post je 2010. godine, u projektu Tajna Amerika (eng. *Top Secret America*) na dokumentovan način utvrdio angažovanje čak 165 velikih privatnih kompanija koje se na neki način bave aktivnostima u vezi sajber odbrane

[791] National Security Agency, „Ukusa Agreement."

[792] Dwight D. Eisenhower, *Farewell Address*, Eisenhower Presidential Library, Museum & Boyhood Home, https://www.eisenhower.archives.gov/research/online_documents/farewell_address.html (preuzeto 15. decembra 2015).

[793] Adam Taylor, „These are America's 9 Longest Foreign Wars," *The Washington Post*, May 29, 2014, https://www.washingtonpost.com/news/worldviews/wp/2014/05/29/these-are-americas-9-longest-foreign-wars/ (preuzeto 12. januara 2016).

ili bezbednosti, za potrebe mnoštva američkih državnih organa i institucija, posebno obaveštajno-bezbednosne zajednice, na čelu sa NSA iz Ministarstva odbrane.[794] Po izveštaju, na svim poslovima nacionalne bezbednosti, protivterorizma i obaveštajnih aktivnosti, na preko 10.000 lokacija unutar SAD je uspostavljena saradnja između 1271 vladine organizacije i ukupno 1931 privatne kompanije.[795] Tokom 2010. godine, u kojoj je izveštaj sačinjen, na troškove angažovanja privatnih kompanija u oblasti bezbednosti i odbrane Vlada SAD je utrošila čak 316 milijardi dolara, uključujući, na primer, 20% ukupnih troškova rata u Iraku[796]. Ovaj podatak najbolje govori o privatizaciji procesa ratovanja, odnosno o procesu ratovanja kao biznisu.

U skladu sa praksom angažovanja privatnih kompanija za obezbeđenje i specijalne zadatke, tokom ratova u Avganistanu i Iraku, ove kompanije nisu angažovane samo za podršku obaveštajno-bezbednosnim aktivnostima, već i za njihovu realizaciju na operativnom nivou. To znači za neposredno izvršavanje operacija u sajber prostoru, pri čemu su zaposlenima u privatnim kompanijama dodeljivani zadaci koje uobičajeno obavljaju pripadnici vojske. Uslovi za dobijanje bezbednosnih sertifikata pripadnika vojske i zaposlenih privatnih kompanija na poslovima za sistem odbrane su izjednačeni, uključujući i aktivnosti u sajber prostoru. Na primer, poznati insajder i uzbunjivač, Edvard Snouden, koji je iz centrale NSA na Havajima preuzeo ogromnu arhivu strogo poverljivih dokumenata, to nije učinio kao pripadnik NSA, već kao zaposleni privatne kompanije *Booz Alen Hamilton*.[797] Pre toga je od 2006. godine radio u agenciji CIA u Merilendu[798], odakle je 2009. godine prešao da radi u kompaniji *Dell* u Japanu za potrebe NSA,[799] da bi konačno prešao u kompaniju *Booz Alen Hamilton* 2013. godine na mesto

[794] Dana Priest and William M. Arkin, „Top Secret America," *The Washington Post*, 2010, http://projects.washingtonpost.com/top-secret-america/ (preuzeto 12. januara 2016).

[795] Ibid.

[796] Peter W. Singer, „The Regulation of New Warfare," *The Brookings Institution*, February 2010, http://www.brookings.edu/research/opinions/2010/02/27-defense-regulations-singer# (preuzeto 27. decembra 2013).

[797] James Bamford, „The Most Wanted Man in the World", *Wired*, August 22, 2014, http://www.wired.com/2014/08/edward-snowden/ (preuzeto 22. novembra 2015).

[798] Luke Harding, „How Edward Snowden Went from loyal NSA Contractor to Whistleblower", *The Guardian*, February 1, 2014, http://www.theguardian.com/world/2014/feb/01/edward-snowden-intelligence-leak-nsa-contractor-extract (preuzeto 22. novembra 2015).

[799] „Snowden Downloaded NSA Secrets While Working for Dell, Sources Say", *Reuters*, August 15, 2013, http://www.reuters.com/article/usa-security-snowden-dell-idUSL2N0GF11220130815 (preuzeto 22. novembra 2015).

administratora mreže u centru NSA na Havajima.[800] Kompanija *Booz Alen Hamilton* ostvaruje profit isključivo poslujući sa Vladom SAD na poslovima obaveštajno-bezbednosnih aktivnosti, posebno u sektoru informaciono-komunikacionih tehnologija.[801] Njen potpredsednik je viceadmiral u penziji Majkl MekKonel, bivši direktor agencije NSA i Nacionalne obaveštajne zajednice. U 2014. godini je kompanija *Booz Alen Hamilton* imala godišnji prihod od 5.48 milijardi dolara,[802] preko 22.000 zaposlenih i bila je u sastavu je velikog poslovnog sistema *Karlajl Grupa*[803], koji je još šire zastupljen u oblasti američke vojno-odbrambene industrije.

Da se pripadnici privatnih kompanija angažuju na ofanzivnim operacijama u sajber prostoru u inostranstvu u ime američke Vlade, najbolje ilustruje primer jednog oglasa za posao koji je američka privatna kompanija *Leonie* objavila 2013. godine.[804] U njemu se nudi posao na radnom mestu „Planer sajber operacija" u glavnom gradu Avganistana i traži se osoba koja ima: najmanje pet godina radnog iskustva u vođenju računarskih mrežnih operacija, od čega najmanje dve na operativnom planiranju i integraciji ofanzivnih sajber operacija; znanje na planiranju, preduzimanju (eng. *targeting*)[805, 806], sinhronizaciji i izvođenju sajber operacija; znanje o razvijanju strategije, planova i naređivanja akcija operacija u sajber prostoru; iskustva i znanja iz nadležnosti Centralne

[800] Booz Alen Hamilton, „Booz Allen Statement on Reports of Leaked Information", Press Release, June 11, 2013, http://www.boozallen.com/media-center/press-releases/2013/06/statement-reports-leaked-information-060913, (preuzeto 20. decembra 2015).

[801] Charles Riley, „Booz Alen Hamilton in Spotlight Over Leak", *CNN*, June 10, 2013, http://money.cnn.com/2013/06/10/news/booz-allen-hamilton-leak/index.html (preuzeto 20. novembra 2015).

[802] United States Securities and Exchange Commission, *Form 10-K, XNYS:BAH Booz Allen Hamilton Holding Corp Annual Report*, 2012, http://quote.morningstar.com/stock-filing/Annual-Report/2012/3/31/t.aspx?t=XNYS:BAH&ft=10-K&d=64ece737bbfff1deaf0c6b79fafe3153 (preuzeto 20. novembra 2015).

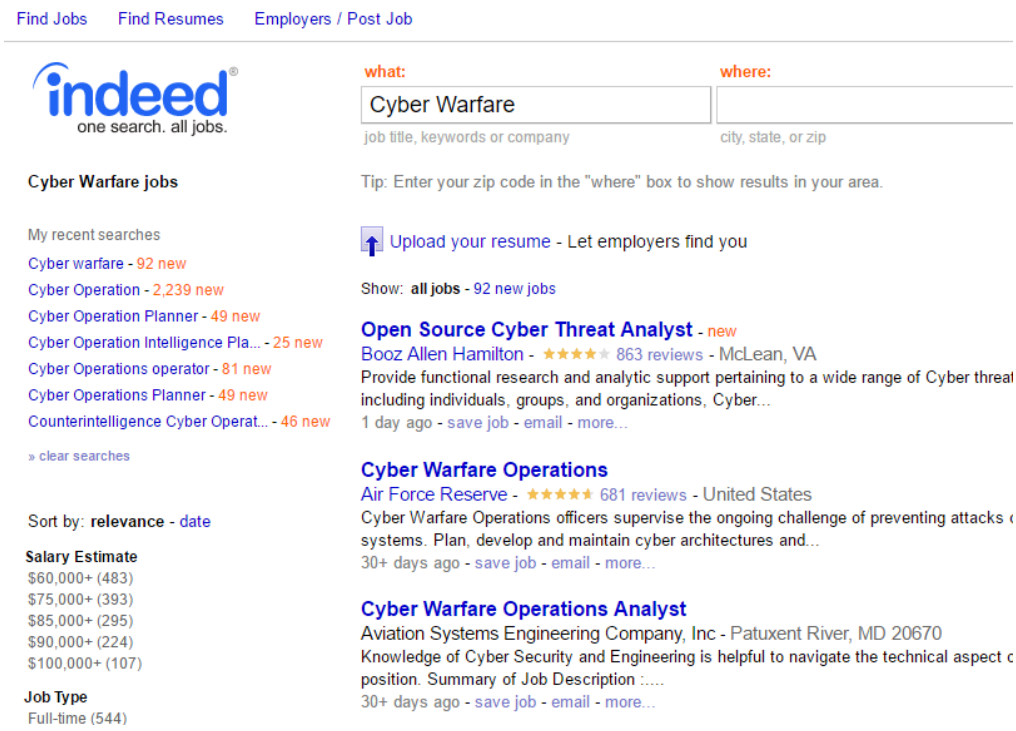
[803] The Carlyle Group, *Portfolio Company Highlights: Booz Alen Hamilton*, https://www.carlyle.com/our-business/portfolio-of-investments/booz-allen-hamilton-inc (preuzeto 20. novembra 2015).

[804] Dragan Mladenović, „Neslućene mogućnosti novih tehnologija," *Odbrana*, No. 191, Specijalni dodatak (septembar 2013), www.odbrana.mod.gov.rs/specijalniprilog/93/Specijalniprilog93-Sajberratovanje.pdf (preuzeto 12. decembar 2015), 46.

[805] U oglasu je navedeno: eng. *Knowledge of planning, **targeting**, synchronization and assessing Cyberspace Operation*, pri čemu glagol *tergeting* na engleskom jeziku označava neposredno preduzimanje napada, gađanje, nišanjenje, odnosno Biranje nečega kao objekta pažnje ili napada, usmeravanje nečega, *Oxford Dictionaries*, s.v. „target," http://www.oxforddictionaries.com/definition/english/target (preuzeto 20. januara 2016).

[806] Po rečniku Ministarstva odbrane SAD, *targeting* (ciljanje, gađanje) je proces odabiranja ciljeva (meta) i određivanja njihovog prioriteta i odgovarajućeg odgovora na njih, u odnosu na operativne zahteve i sposobnosti.

komande i Združenog štaba Vojske SAD, odnosno nadležne kancelarije Ministra odbrane; prethodno vojno iskustvo pokretanja sajber napada na strategijskom nivou, obavezno vojno iskustvo u naveden oblastima, kao i obaveznu službu u Iraku i/ili Avganistanu.[807]



Slika 25. Mnoštvo objavljenih oglasa privatnih kompanija za poslove u vezi područja sukoba u sajber prostoru u SAD na portalu Indeed.com.[808]

Međutim, u oglasu se dotično lice se zahteva posedovanje validnog američkog turističkog pasoša, što potvrđuje da će raditi u svojstvu civilnog lica.[809] Leoni je privatna kompanije iz Santa Monike u Kaliforniji, sa kojom je Ministarstvo odbrane SAD više puta sklapalo ugovore o angažovanju, posebno u Avganistanu, u oblasti sajber operacija, obaveštajne analize, psiholoških operacija, tehničke podrške obaveštajnim aktivnostima i operacijama

[807] Leonie, Cyber Operations Planner (closed), Bullhornreach, http://www.bullhornreach.com/job/793005_cyber-operations-planner-kabul-afghanistan (preuzeto 20.februara 2016).

[808] Indeed.com, http://www.indeed.com/jobs?q=Cyber+Warfare&l (preuzeto 28 aprila.2016).

[809] Ibid.

na terenu.[810] U 2014. godini je objavljen ugovor o angažovanju kompanije Leoni za potrebe američke vojske u Avganistanu do sredine 2019. godine.[811] Leoni je samo jedna, relativno manja, privatna kompanija koja u masi drugih redovno obavlja poslove u oblasti sajber odbrane za potrebe američke države.


Find Jobs > Kabul > Teri Scott

Cyber Operations Planner (closed)

Kabul, Afghanistan

Cyber Operations Planner

Leonie, an international, woman-owned, leading provider of execution management specialists, performance measurement experts and analysts to US Government organizations is seeking a qualified Cyberspace Operations (CO) Planner.

Job Description:

Provide expertise/conduct/support:

· Development of Cyberspace operations objectives
· Provide advice and assistance to key strategic operations synchronization team with Cyberspace Operations integrating processes, procedures and products into operational planning
· Knowledge and experience with Offensive Cyberspace Operations (OCO)
· Knowledge and experience with Cyberspace Operations enabling actions
· Knowledge and experience with the intelligence community and intelligence processes
· Knowledge and experience with synchronizing cyberspace operations efforts with militar deception (MILDEC), operations security (OPSEC), and military information support operations (MISO) in support of command objectives
· Provide support and subject matter expertise to maximize successful execution of theate and strategic Cyberspace Operations plans

Slika 26. Oglas kompanije Leoni i Kalifornije za radno mesto “Planer sajber operacija” u Kabulu, u kome se traži prethodno vojno iskustvo u ofanzivnim sajber operacijama.812

Po proceni autora projekta *Tajna Amerika*, čak 854.000 ljudi u SAD je imalo sertifikate za pristup i rukovanje informacijama i dokumentima američke Vlade nivoa „Strogo

[810] Leonie Industries, „Top Secret America,“ *The Washington Post*, http://projects.washingtonpost.com/top-secret-america/companies/leonie-industries/ (preuzeto 20. februara 2016).

[811] „Blog: Leonie Awarded Afghanistan Information Support Contract“, *Signal*, May 15, 2014, http://www.afcea.org/content/?q=leonie-awarded-afghanistan-information-support-contract (preuzeto 20. februra 2016).

[812] Leonie, Cyber Operations Planner (closed), Bullhornreach, http://www.bullhornreach.com/job/793005_cyber-operations-planner-kabul-afghanistan (preuzeto 20. februara 2016).

poverljivo (eng. *Top Secret*).[813] Lica koja se angažuju na zadacima u oblasti odbrane u nadležnosti Ministarstva odbrane SAD imaju u operativnom i zakonskom pogledu skoro ista prava i obaveze kao i pripadnici Ministarstva[814], ali i obaveze kao i vladini službenici ili vojnici. U pogledu odredbi Međunarodnog prava oružanih sukoba, na ove ljude prilikom izvođenja operacija u sajber prostoru se primenjuje Međunarodno pravo oružanih sukoba na aktivnosti koje su vezane za sukobe. Međutim, u skladu sa prethodno zaključenim međunarodnim bilateralnim pravnim sporazumima o uzajamnoj pravnoj pomoći (*Mutual Legal Assistance Treaty-MLAT*), kao i sporazumima o statusu pripadnika oružanih snaga u stranoj državi (*Status of Forces Agreements* - SOFA), Vlada SAD je stavila vlastiti suverenitet i nadležnost vlastitih sudova na prvo mesto.[815] Navedeni sporazumi definišu sudsku jurisdikciju u slučajevima kršenja zakona od strane pripadnika oružanih snaga i pridruženog vojnog osoblja koje radi za potrebe oružanih snaga u inostranstvu.

Područje primene operacija u sajber prostoru je u tom pogledu posebno specifično imajući u vidu probleme vezane za pravnu atribuciju sajber napada odnosno kategorisanja između akta oružane agresije i kriminala. Tamo gde nema jasne opšte (međunarodnopravne) regulative, kao što je područje sajber sukoba, bilateralni sporazumi pružaju jedini pravni osnov za ostvarivanje pravne nadležnosti i sprovođenje prava.[816] Međutim, u tom slučaju pravne akcije su najčešće unilateralne, i u skladu sa zakonima jedne strane. Na primer, ni jedna konvencija međunarodnog prava ne zabranjuje primenu špijunaže, ni u fizičkom okruženju, niti u sajber prostoru. S druge strane u svim nacionalnim zakonodavstvima aktivnosti špijunaže koje su umerene protiv državnih interesa se smatraju vrlo ozbiljnim krivičnim delom koje se najoštrije sankcioniše. U tom pogledu, primena nacionalnih zakona je vrlo selektivna. Takođe, sajber operacije koje su izvedene u vreme i u okviru

[813] Dana Priest and William M. Arkin, „A hidden world, growing beyond control", *The Washington Post*, July 19, 2010, http://projects.washingtonpost.com/top-secret-america/articles/a-hidden-world-growing-beyond-control/print/ (preuzeto 20. februara 2016).

[814] U skladu sa *Mutual Legal Assistance Treaty* (MLAT) bilateralnim sporazumima. *Department of Defense Dictionary of Military and Associated Terms: Joint Publication 1-02*, Washington, DC: Joint Chiefs of Staff, 2001 (as amended through 15 January 2015), 242.

[815] United States Department of State, Treaties in Force, *A List of Treaties and Other International Agreeements of the United States in Force on January 1, 2013*, http://www.state.gov/documents/organization/218912.pdf (preuzeto 21. februara 2016).

[816] United States Depeartment of Defense Office of General Counsel, *An Assessment of International Legal Issues in Information Operations*, 1999, 35, http://www.au.af.mil/au/awc/awcgate/dod-io-legal/dod-io-legal.pdf (preuzeto 8. jula 2015).

ratnih sukoba, kao deo nastojanja jedne strane da izvrši ofanzivnu operaciju (napad) prema drugoj strani, po pravilu se različito kvalifikuju. Za napadača one su zakonite i legalne (jer je doneta odluka o njihovom preduzimanju), a za napadnutog su nelegalne i predstavljaju akt agresije. Nadležnost prava samo jedne strane u tom slučaju ne može biti merodavna, niti pravična. Pored toga, nadležnost bilateralnih sporazuma u vreme sukoba bi verovatno bila ograničena ili suspendovana.

11. PRAVO, SUKOBI I RATOVANJE U SAJBER PROSTORU

Regulisanjem sukoba između država primarno se bavi Međunarodno pravo oružanih sukoba. Svaki sukob u opštem pogledu ima sledeće ključne elemente: učesnike i njihove motive, sredstva i metode ratovanja. Pošto motivi svih međunarodnih sukoba primarno zavise od političke volje, konačni cilj svakog učesnika sukoba je isti, bez obzira na okruženje u kojem se sukob odvija: potčiniti stanje i ponašanje protivnika svojoj volji[817]. Međutim, u pogledu vrste sredstava, učesnika i metoda kojim se sukobi vode, razlika između tradicionalnih i sajber sukoba je suštinska. Uzrok te razlike je primarno tehnološke prirode, dok su njene posledice primarno pravne i organizacione prirode.

U pogledu primene Međunarodnog prava oružanih sukoba, posledice specifičnosti prirode sajber sukoba je izuzetno otežano otkrivanje agresije, počinilaca i utvrđivanje okolnosti neophodnih za određivanje da li je agresija u nadležnosti Međunarodnog prava oružanih sukoba ili nekog drugog prava. Uzrok tome je priroda primenjenih tehnologija, okruženja i odnosa učesnika. Na primer, digitalne tehnologije omogućavaju neograničeno umnožavanje podataka; softver inherentno sadrži nedostatke koji mogu biti zloupotrebljeni za narušavanje bezbednosti sistema; ista sredstva i metode za izvođenje sajber napada koriste i pojedinci i države, u miru i u ratu. To nije karakteristično za primenu sile u fizičkom okruženju, u kome su organizacija, primena i manifestacija vojne sile uočljive zbog spektakularnih efekata dejstva vojnih sistema naoružanja, kao i zbog razvoja tehnologije za njihovo otkrivanje i praćenje.

Tradicionalno pravo oružanih sukoba je sistem koji ima za cilj da reguliše međunarodne oružane sukobe, obezbedi mir i umanji žrtve i razaranja do kojih dolazi tokom sukoba. Imajući u vidu činjenicu da oružani sukobi prate ljudski rod od njegovog nastanka i da se neprekidno razvijaju tehnologije i forme ratovanja, taj cilj je teško dostižan, a njegov

[817] Carl von Clausewitz, *On War*, trans. J.J. Graham (London, UK: Nicholas Trubner, 1873), Book I, Chapter 1, para 2, http://www.gutenberg.org/files/1946/1946-h/1946-h.htm#link2HCH0001 (preuzeto 22. avgusta 2015).

uspeh ne može biti apsolutan. Tradicionalno pravo se vremenom mora jako elastično interpretirati da bi moglo da obuhvati sve nove situacije koje donose nove tehnologije, a to zatim dovodi do neujednačene primene principa, normi i propisa. Sistem međunarodnog prava mora obezbediti mir i umanjiti posledice primene oružane sile i sukoba svuda u svetu, i u svakom trenutku na efikasan način, inače njegova svrha ne može biti ispunjena.

Međunarodno pravo je sistem koji teško i sporo nastaje, jer je za njegovu izgradnju potreban konsenzus međunarodne zajednice u kojoj su osnovni nosioci suvereniteta države, a ne međunarodni organi. Ključni sistemi Međunarodnog prava oružanih sukoba, Ženevske i Haške konvencije, nastajale su u dugom procesu usaglašavanja različitih stavova delova međunarodne zajednice decenijama. U tom, vremenski dugom periodu, dešavali su se brojni ratovi, uključujući i dva svetska. Tokom tog perioda, a i nakon usvajanja fundamentalnih međunarodnih dokumenata koje sporazumno regulišu oblast sukoba, tehnologija vođenja sukoba se konstantno menjala. Ti međunarodni sporazumi i konvencije ne važe apsolutno u potpunosti i za svaku državu. Njih su države usvajale sukcesivno i parcijalno u skladu sa vlastitim nacionalnim interesima i okruženjem. To je dovelo do niza novih situacija na koje se tradicionalno pravo ne može linearno primeniti. Najproblematičnija situacija do sada je primena sajber ratovanja i vođenje međunarodnih sukoba u sajber prostoru. U tom pogledu, u cilju efikasne primene Međunarodnog prava oružanih sukoba u regulaciji novih oblika sukoba, potrebna je nova interpretacija čiji legitimitet prepoznaju sve strane koje prihvataju postojeće norme i pravila međunarodnog prava. Pored toga, postoji više mogućnosti: (a) da Međunarodno pravo oružanih sukoba u nepromenjenom obliku reguliše nove odnose tradicionalnim pristupom, (b) da područje sajber ratovanja ostane neregulisano, (c) da se kreira novi sistem prava - Sajber pravo koje bi obuhvatilo i (međunarodne) aspekte sajber sukoba, odnosno sukoba, rata i napada u sajber prostoru ili d) da se na optimalan način iskombinuje primena različitih sistema međunarodnog prava u cilju maksimalnog učinka na regulisanje sajber sukoba.

Primenu tradicionalnog prava u novim okolnostima karakteriše veliki broj problema. Ključni su:

- nemogućnost utvrđivanja (napada, napadača, državne odgovornosti);
- mešanje vojnog i civilnog okruženja, ciljeva, infrastrukture;

- asimetričnost (zasnovanost na ranjivostima pre nego na apsolutnom kapacitetu oružja)
- umešanost nedržavnih subjekata u sve faze i oblike sukoba u sajber prostoru;
- problem nadležnosti državnog suvereniteta u sajber sukobima.

Imajući u vidu mogućnosti primene prava na sajber sukobe, u pravnom i političkom pogledu, bi bilo podesno i prihvatljivo rešenje može biti u Sajber pravu[818], [819] uz preuzimanje prihvatljivih i praktično primenljivih koncepata Međunarodnog prava oružanih sukoba, ali i drugih grana prava. Sukobi u sajber prostoru se odvijaju u stanju rata, ali još više u stanju mira, pa je stoga potrebna kombinacija primene raznih praktičnih koncepata i pristupa u regulisanju sukoba u sajber prostoru. U slučaju integracije i uključivanja različitih principa i sistema koji imaju drugačije izvore, u novo Sajber pravo, moguće je doći do novog pristupa, koji predstavlja povoljnije i efikasnije rešenje koje je praktično lakše ostvarivo, i prihvatljivije je za širi krug međunarodnih aktera. Njegovim uvođenjem se ne remete postojeći koncepti tradicionalnog prava, već se oni efikasno kombinuju u odgovarajući, konzistentan, i praktično primenljiv model[820]. Takav pristup zahteva novi kompleksni, multidisciplinarni i interdisciplinarni[821] pravni pristup koji respektuje sve specifičnosti sajber prostora i pojava u njemu. Na taj način, forma i sadržaj prava se prilagođavaju realnim problemima i fenomenima u sajber prostoru koje to pravo reguliše, pri čemu se izbegava potreba da se sporo promenljiv tradicionalni pravni sistem formalno prilagođava novim pojavama u realnom svetu. Takav pristup može biti od posebne koristi u oblastima u kojima se sreću dinamične promene odnosa i stanja, poput primene računarskih nauka i informaciono-komunikacionih tehnologija u sukobima u sajber prostoru. Ipak, razvoj bilo kog novog sistema međunarodnog prava takođe je spor, pošto je za njegov razvoj i usvajanje potrebno dugo i sporo usaglašavanje konsenzusom

818 Mirjana Drakulić, Ratimir Drakulić, „Evropska perspektiva regulisanja Internet usluga: izazov tradicionalnom evropskom pravu“, *Telekomuniakcije*, no. 6 (2010), http://www.telekomunikacije.rs/arhiva_brojeva/sesti_broj/prof_dr_mirjana_drakulic,_mr_ratimir_drakulic:_evropska_perspektiva_regulisanja_internet_usluga:_izazov_tradicionalnom_evropskom_pravu.344.html (preuzeto 15. avgusta 2015).

819 Mladenović, Međunarodni aspekt sajber ratovanja, 448.

820 Drakulic, Mirjana. "Osnovi kompjuterskog prava." Drustvo operacionih istrazivača Jugoslovije-DOPIS, Belgrade (1996).

821 Međunarodnog javnog prava, Međunarodnog ugovornog prava, Međunarodnog privatnog prava, Međunarodnog prava ljudskih prava, Krivičnog prava, Građanskog prava, Obligacionog prava, Prava intelektualne svojine, Međunarodnog prava oružanih sukoba, Saobraćajnog prava, Međunarodnog poslovnog prava i drugih.

između brojnog skupa zainteresovanih strana sa različitim interesima. Stoga se rešenje treba tražiti u postojećim oblastima prava, poput, na primer, međunarodnog javnog, odnosno međunarodnog ugovornog prava. Pravni instrument za ovo odavno postoji u vidu Bečke konvencije o ugovornom pravu[822]. U prilog ovom pristupu govore i najpoznatiji savremeni autoriteti u oblasti međunarodnog prava. Goldsmit i Posner navode brojne primere iz istorije interesno suprotstavljenih država u kojima su bilateralni sporazumi odigrali ključnu ulogu u saradnji, usklađivanju interesa, regulaciji i koordinaciji ponašanja između država, čak i u slučaju kada su takvi sporazumi povremeno kršeni[823].

Ključni obzir u tom pogledu je praktičnost prava. Praktičnost primene omogućava pravu visok stepen prihvatanja od strane osnovnih nosilaca suverene vlasti u međunarodnim odnosima – država. Pri tome su mogući različiti nivoi i koncepti ostvarivanja saradnje. Oni obuhvataju različite nivoe i pristupe: nacionalni, međunarodni, odnosno samoregulaciju. Pri tome su od ključne važnosti pristup izgradnji zajedničkog sistema na dogovoru i poklapanju interesa ključnih strana, već i nivo od koga se polazi. Za razliku od pokušaja samoregulacije na organizacionim nivoima nižim od državnog, samoregulacija međunarodnih odnosa ima malo šansi za uspeh. S druge strane, samoregulacija na nivou država ima realne izglede za uspeh, posebno ukoliko je moguć dogovor o komplementarnosti i neponištavanju zajedničkih interesa. Za uspeh takvog pristup, neophodno je pomeriti težište stručno težište pristupa sa isključivo pravnog na one oblasti čije zakonitosti i praksa imaju najveći potencijal za uspeh. U oblasti sukoba u sajber prostoru to je svakako tehnologija. Da bi međunarodno pravo bilo efikasno i primenljivo, nužno je da prethodno bude prihvatljivo što širem krugu država.

11.1. Sukob i ratovanje u sajber prostoru kao predmet međunarodnog prava

Kao i u slučaju informacione bezbednosti, sajber prostora, sajber oružja i sajber napada, u međunarodnoj i stručnoj zajednici se različito definišu sajber rat, sajber sukob i sajber ratovanje. Pri tome treba razlikovati vojno-tehnički pristup definisanju ratovanju, kao

[822] Vienna Convention on the Law of Treaties, May 23, 1969, 1155 U.N.T.S. 331, 8 I.L.M. 679.

[823] Jack L. Goldsmith and Eric A. Posner, *The Limits of International Law*, (New York, NY: Oxford University Press, 2005), 4.

procesu (oružanog) sukoba između zaraćenih strana od procesa ratovanja u pravnom pogledu.

U tom kontekstu, u opštem slučaju sukob i rat se razlikuju po: intenzitetu, angažovanju organizovanih vojnih snaga u vođenju aktivnosti oružanog sukoba i po sadržaju aktivnosti koje vode strane u sukobu. Pojmovi rat i ratovanje se međusobno odnose prema predmetu i sadržaju aktivnosti odnosno procesa.

Projekat *EastWest* instituta definiše nekoliko različitih oblika primene sile u sajber prostoru. Po njemu, sajber sukob je stanje koje je : „napeta situacija između i/ili unutar država i/ili organizovanih grupa u kojoj se izvode nepoželjni sajber napadi kao odmazda“[824], dok je sajber rat: „stanje eskaliranog sajber sukoba između ili unutar država u kojima se sajber napadi preduzimaju od strane državnih aktera protiv sajber infrastrukture kao deo vojne operacije“[825]. Po izvoru, ovakav rat može biti deklarisan i *de facto*. Dakle, po *EastWest* institutu, sajber sukob i rat se razlikuju po intenzitetu i umešanosti vojnih snaga u njegovo vođenje, s tim što je sukob prethodnik rata, i njegovom eskalacijom postaje rat. To dovodi do zaključka sa su sajber sukob i rat slični po sadržaju, ali nisu po nivou agresije. Iako navedenu definiciju ne karakterišu preciznost i razlikovanje ključnih elemenata sukoba, ona ističe sajber napade kao ključne aktivnosti i rata i sukoba u sajber prostoru.

Austrija smatra da je sajber rat “akt rata unutar i oko virtuelnog prostora vođen sredstvima koja se primarno asociraju sa informacionim tehnologijama”, dok u širem smislu predstavlja podršku tradicionalnim vojnim aktivnostima u fizičkom okruženju.[826]

Italija smatra da su sajber ratovanje „aktivnosti i operacije preduzete u sajber području sa svrhom ostvarivanja operativne prednosti od vojnog značaja“[827]

Međutim, postoje i neki konceptualno drugačiji stavovi. Na primer u predlogu teksta rezolucije Ruske Federacije za rezoluciju Generalne skupštine UN 2000. godine, definiše se pojam „informaciono ratovanje“, na sledeći način: „Konfrontacija između država u

[824] Godwin, Kulpin, Rauscher and Yaschenko. "Russia-U.S. Bilateral," 31.

[825] Ibid, 32.

[826] Austria, *Austrian Cyber Security Strategy*, 22.

[827] Italy, *National Strategic Framework,* 13.

informacionom području u cilju oštećivanja informacionih sistema, procesa i resursa, kao i vitalnih struktura, urušavanje političkih, ekonomskih i društvenih sistema, kao i masovna psihološka manipulacija stanovništvom u cilju destabilizacije društva i države“[828].

Već na prvi pogled jasno je da su navedene definiciji veoma raznorodne, kao i da su među njima istaknute one koje nemaju praktičnu vrednost, već samo teorijsku. U skladu sa utvrđenim stavom tokom prethodne analize, sajber sukobi su sukobi koji se odvijaju u sajber prostoru. Međutim, šta je sukob, a šta oružani sukob? Šta je rat? Odgovori na ova pitanja izgledaju očigledni, ali međunarodno pravo ih ni u jednom dokumentu zvanično i precizno ne pruža.

Načelno, ratovanje je proces koji se u cilju oružanog sukoba vodi između strana u sukobu i koji karakteriše upotreba organizovane primene oružane sile. Pored oružane borbe, ratovanje podrazumeva i širok skup drugih organizovanih aktivnosti na podršci i obezbeđenju oružanih operacija. Ono predstavlja *de facto* proces koji se vodi između suprotstavljenih strana.

Ratovanje može imati šire i uže značenje. Po užem značenju ono se odnosi na primenu specifične vrste sile, po vrsti oružja koje se primenjuje, području u kome se primenjuje ili vrsti cilja na koje je usmereno, na primer, sajber ratovanje, pomorsko ratovanje, elektronsko ratovanje, nuklearno ratovanje, psihološko ili ekonomsko ratovanje. U širem smislu, ono se odnosi na ukupni proces sukoba koji uključuje i elemente organizovanog oružanog sukoba između strana u sukobu.

Rat predstavlja stanje oružanog sukoba između međunarodnih subjekata, odnosno period u kome se neka strana nalazi u stanju organizovane oružane borbe protiv druge međunarodne strane. Pri tome, stanje rata može biti formalno deklarisano (lat. *de iure*) ili stvarno, koje se odigrava u stvarnosti bez formalne deklaracije rata između strana u sukobu (*de facto*).

Ipak, jasan je sledeći uslov. Da bi se primenile odredbe Povelje UN, kao osnovnog međunarodnog ugovora, na stanje i posledice sukoba između nacija, neophodno je da

[828] Russia, Submission to the UN G.A. Res 55/140, 3.

svaka država prihvati Povelju, odnosno da bude članica Organizacije UN. Takođe, da bi se primenila neka odredba specifičnog ugovora ili sporazuma koje grade Međunarodno pravo oružanih sukoba, neophodno je da uključene strane u sukobu prihvataju taj ugovor. Na primer, zajednički član 2. Ženevskih konvencija (I-IV) iz 1949. godine, navodi da se konvencija primenjuje na sve međunarodne sukobe ukoliko je bar jedna strana u sukobu ratifikovala konvenciju:

> Pored odredaba koje treba da stupe na snagu još za vreme mira, ova Konvencija će se primenjivati u slučaju objavljenog rata ili svakog drugog oružanog sukoba koji izbije između dveju ili više Visokih strana ugovornica, čak i ako jedna od njih nije priznala ratno stanje. Konvencija će se isto tako primenjivati u svim slučajevima okupacije cele teritorije jedne Visoke strane ugovornice ili njenog dela, čak iako ta okupacija na naiđe ni na kakav vojni otpor. Ako jedna od Sila u sukobu nije učesnik u ovoj Konvenciji, Sile učesnice u Konvenciji ipak će ostati vezane njome u svojim međusobnim odnosima. One će pored toga biti vezane Konvencijom prema toj Sili, ako ta Sila prihvata i primenjuje njene odredbe.[829]

U suprotnom, ukoliko ni jedna od strana u sukobu nije potpisnica nadležne konvencije ili sporazuma, ne postoji ni nadležnost tog ugovora ili sporazuma u sporu između tih strana. Međutim, to ne znači da međunarodni sukobi i njihove posledice ostaju neregulisani. U tom slučaju, nadležno je međunarodno običajno pravo, koje između ostalog, sadrži i humanitarnu stranu pravne regulacije odnosa među subjektima međunarodnog prava.

Nakon što se potvrdi nadležnost odgovarajućeg međunarodnog prava i specifičnog pravnog ugovora na sukob, pristupa se proceni postupaka strana u sukobu u skladu sa njegovim odredbama. Međutim, ovaj zadatak nije ni malo jednostavan. Ni Povelja UN, niti drugi zvanični i obavezujući dokument međunarodne zajednice ne pružaju definiciju rata, oružanog sukoba, primene sile, oružane sile ili odgovarajuće agresije. Taj problem je odavno prepoznat u stručnoj praksi međunarodnog prava, ali do njegovog rešenja nije

[829] I Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, Aug. 12, 1949, 6 UST 3114, 75 UNTS 31; II Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea, Aug. 12, 1949, 6 UST 3217, 75 UNTS 85; III Geneva Convention Relative to the Treatment of Prisoners of War, Aug. 12, 1949, 6 UST 3316, 75 UNTS 135; IV Geneva Convention Relative to the Protection of Civillian Persons in Time of War, Aug. 12, 1949, Art 2, 6UST 3516, 75 UNTS 287.

došlo zbog strogog i sporog načina na koji se usvajaju izvori međunarodnog prava[830] Jedino što međunarodno pravo nedvosmisleno navodi jeste upotreba sile[831], agresija[832], oružana sila[833], oružana snaga[834] i oružani napad[835]. Međutim, čak ni odnos između navedenih pojmova u izvorima međunarodnog prava nije definisan, niti je jasan, pa stoga u svakom pojedinačnom slučaju zahteva posebnu analizu i raspravu koja se uvek i iznova odnosi na utvrđivanje međusobnog odnosa značenja navedenih kategorija.

Do danas je bilo više pokušaja međunarodne zajednice da se to promeni,[836] ali ni jedan od njih nije ima za rezultat ključni formalno-pravni napredak u smislu praktičnog uticaja na sposobnost prava da nedvosmisleno i u potpunosti reguliše oružane sukobe u njegovoj nadležnosti.[837] Međutim, to ne znači da Međunarodno pravo oružanih sukoba nije primenjivo u praksi. Široka praksa međunarodnih sudova i tribunala pokazuje da postojeći izvori međunarodnog prava pružaju osnovu da se nadležni sud u svakom od posmatranih slučajeva izjasni po pitanju utvrđivanja krivice strana u sukobu.

Na navedeni problem neprecizne formulacije i međusobnog odnosa ključnih pojmovnih kategorija međunarodnog prava od značaja za oružane sukobe u slučaju sukoba (ratovanja) u sajber prostoru moraju se dodati i novi, tehnološki generisani problemi. Ti problemi se, pre svega, ali ne isključivo, tiču specifične prirode sredstava kojim se vode

---

[830] James G. Stewart, "Towards a Single Definition of Armed Conflict in International Humanitarian Law: A Critique of Internationalized Armed Conflict," *Revue Internationale de la Croix-Rouge/International Review of the Red Cross* 85, no. 850 (2003): 313-350.

[831] Povelja UN, član 2, paragraf 4: „Svi članovi će se u svojim međunarodnim odnosima uzdržavati od pretnje silom ili od upotrebe sile protiv teritorijalnog integriteta ili političke nezavisnosti svake države, ili od upotrebe sile na bilo koji drugi način koji je nesaglasan sa ciljevima Ujedinjenih nacija“.

[832] Povelja UN, članovi 1, 39, 53.

[833] Povelja UN, preambula, članovi 41, 46.

[834] Povelja UN, članovi 43, 44, 47.

[835] Povelja UN, član 51: „Ništa u ovoj Povelji ne umanjuje urođeno pravo na individualnu ili kolektivnu samoodbranu u slučaju oružanog napada protiv člana Ujedinjenih nacija, dok Savet bezbednosti ne preduzme mere potrebne za očuvanje međunarodnog mira i bezbednosti. O merama koje preduzmu članovi pri vršenju ovoga prava na samoodbranu biće odmah izvešten Savet bezbednosti i one neće ni na koji način da dovedu u pitanje ovlašćenja i odgovornost Saveta bezbednosti da po ovoj Povelji preduzme u svako doba takvu akciju ako je smatra nužnom radi održanja ili vaspostavljanja međunarodnog mira i bezbednosti“.

[836] International Committee of the Red Cross (ICRC), *How is the Term "Armed Conflict" Defined in International Humanitarian Law?* March 2008, https://www.icrc.org/eng/assets/files/other/opinion-paper-armed-conflict.pdf (preuzeto 12. maja 2015).

[837] International Law Association, „Use of Force: Final Report on the Meaning of Armed Conflict,“ in *International Law, The Hague Conference* (2010), http://www.ila-hq.org/en/committees/index.cfm/cid/1022 (preuzeto 12. maja 2015).

sukobi u sajber prostoru (sajber oružja i sajber napada), specifičnog, novog okruženja u kome se vodi sukob (sajber prostora), i učesnika sukoba (sajber boraca), koji se razlikuju od učesnika tradicionalnih oružanih sukoba u fizičkom okruženju.

Da bi se normativno definisao sajber sukob, odnosno sajber agresija ili sajber rat, potrebno je definisati pojam rata, kao i pojmova „upotreba sile", „agresija"[838], „oružana sila", „oružana snaga"[839] i „oružani napad", u smislu njihovog značenja koje imaju u tradicionalnim sukobima u fizičkom okruženju. Navedeni zadatak izgleda teško ostvariv, imajući u vidu da međunarodna zajednica, u toku celokupnog perioda stvaranja Međunarodnog prava oružanih sukoba, a najmanje od 1945. godine do danas, nije uspela da nađe konsenzus u stavu oko toga šta navedeni pojmovi precizno znače. Umesto toga, u cilju praktičnog doprinosa analizi, potrebno je usmeriti se na one pojmove koji pružaju ključni doprinos suštinskom razumevanju i normativnom definisanju kategorija poput „sajber sukoba", „sajber ratovanja" i „sajber napada". Potrebno je, dakle razumeti samu suštinu prirode agresije u sajber prostoru i karakter sajber sukoba i rata.

Povelja UN generalno zabranjuje svaku vrstu upotrebe sile u međunarodnim odnosima, ukoliko ona nije, u skladu sa Poveljom, autorizovana odlukom Saveta bezbednosti UN ili ne predstavlja neposrednu primenu prava na samoodbranu u skladu sa članom 51. Povelje. Da bi se pomenuto pravo ostvarilo nužan uslov je da primarni napad bude takav da daje razlog napadnutoj strani da se brani, primenom recipročnog odgovora silom. Važan napor međunarodne zajednice u nastojanju da donese zajedničku odluku u kojoj bliže definiše silu je bila Rezolucija Generalne skupštine UN broj 2625 iz 1970. godine. Ova rezolucija ponovo deklariše upotrebu sile zločinom. Takođe, ističe da države u svojim odnosima ne treba da je primenjuju u suprotnosti sa odredbama međunarodnog prava (prvenstveno Povelje UN), ali istovremeno ni u čemu bliže ne objašnjava njeno značenje.[840] Tako i Povelja UN i kasnije rezolucije i deklaracije međunarodne zajednice ističu potrebu da se dostigne i osigura stanje mira, a ne definišu šta je stanje rata. Ovo govori u prilog stavu da međunarodna zajednica u vreme kada je donosila Povelju UN **nije ni imala potrebu**

[838] Povelja UN, članovi 1, 39, 53.

[839] Povelja UN, članovi 43, 44, 47.

[840] Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in Accordance with the Charter of the United Nations, G.A. Res. 2625, A/RES/2625(XXV) (Oct. 24, 1970), http://www.un-documents.net/a25r2625.htm (preuzeto 13. maja 2015).

da definiše stanje rata i primenu sile, jer je njihov smisao bio očigledan 1945. godine, kao i da u narednom višedecenijskom periodu prvenstveno zbog suprotstavljenih političkih interesa i stavova najmoćnijih strana u međunarodnoj zajednici nije imala sposobnost stvaranja političkog sporazuma o tom pitanju, koliko god ono bilo fundamentalno.

Povelja UN u pojedinim svojim delovima u smislu uspostavljanja mira između sukobljenih strana pominje neke konkretne primere upotrebe sile, ali ne u smislu da ih definiše, već u smislu uspostavljanja mira. Na primer, članom 42 Povelja UN daje ovlašćenje Savetu bezbednosti da: „…može preduzeti takvu akciju vazduhoplovnim, pomorskim ili kopnenim snagama koja je potrebna radi održanja ili vaspostavljanja međunarodnog mira i bezbednosti. Takva akcija može uključiti demonstracije, blokadu i druge operacije vazduhoplovnim, pomorskim ili suvozemnim snagama članova Ujedinjenih nacija.“[841]. Član 43. navodi da se svi članovi Ujedinjeni nacija obavezuju da na poziv Saveta bezbednosti stave na raspolaganje vlastite oružene snage u cilju uspostavljanja mira.[842] Dakle, posredno se iz navedenih stavova može zaključiti da se preduzimanje sile u međunarodnim odnosima uspostavlja praktičnom primenom oružanih snaga na terenu u cilju uspostavljanja određenih odluka.

Međutim, Povelja UN ne pominje ni u jednom članu pojam „sajber prostor“ iz jednostavnog razloga što on tada nije ni postojao. Da li to znači da akcija Saveta bezbednosti u i kroz sajber prostor ne bi bila legitimna u cilju uspostavljanja mira, odnosno da ne bi mogla biti legalno preduzeta pri očuvanju mira ukoliko je ne bi sprovele oružane snage?

Imajući u vidu navedene dileme i nejasnoće, potrebno je analizirati i kako je međunarodna zajednica pokušala da bliže obrazloži pojam agresije. Pitanje agresije je detaljno analizirano i procenjeno od strane međunarodne zajednice u Rezoluciji Generalne skupštine UN broj 3314 o definisanju agresije iz 1974. godine.[843] Pri tome je važno istaći da ni ova rezolucija, kao ni prethodno pomenuta, nije obavezujući akt međunarodnog prava, iako se kao dodatni izvor prava može upotrebiti u praksi, što je i bio slučaj u

[841] Povelja UN, član 42.

[842] Povelja UN, član 43, stav 1.

[843] Definition of Aggression, United Nations General Assembly Resolution 3314 (XXIX), G.A. Res. 3314, U.N. Doc A/RES/3314 (Dec. 14, 1974), https://daccess-ods.un.org/TMP/5804775.3572464.html (preuzeto 13. maja 2015).

prethodnom periodu, posebno u odlukama međunarodnih sudova. Po rezoluciji, agresija je: „upotreba oružane sile od strane Države protiv suvereniteta, teritorijalnog integriteta ili političke nezavisnosti druge Države ili na bilo koji drugi način nesaglasna sa Poveljom UN, kako je navedeno u ovoj Definiciji“[844]. Pri tome treba imati u vidu da Definicija agresije pod Državom smatra članicu Ujedinjenih nacija. Takođe, Definicija striktno navodi sledeće konkretne oblike preduzimanja sile koje smatra agresijom, uz naglašavanje da taj spisak nije konačan i da Savet bezbednosti može u skladu sa potrebom da donese odluku koji drugi oblici sile nisu u skladu sa odredbama Povelje UN[845]:

> (a) invazija ili napad oružanih snaga jedne države na teritoriju druge države, kao i invazija, napad i zauzimanje teritorije druge države;
>
> (b) bombardovanje teritorije od strane oružanih snaga ili upotreba bilo kog oružja prema teritoriji druge države;
>
> ((c) blokada luka ili obala neke države od strane oružanih snaga;[846]
>
> (d) napad oružanih snaga jedne države na oružane snage druge države;
>
> (e) drugačija upotreba oružanih snaga na teritoriji druge države, nego što je to dogovoreno međusobnim sporazumom;
>
> (f) dopuštanjem nekoj strani da zloupotrebi državnu teritoriju za napad na treću državu.
>
> (g) slanje oružanih bandi, grupa, neregularnih snaga ili najamnika da preduzimaju akte oružane sile prema drugoj državi.[847]

S obzirom da je navedena rezolucija imala primenu u praksi međunarodnog prava u mnogim slučajevima, kao i da ne postoji druga odluka međunarodne zajednice koja ima veću pravnu snagu ili važnosti, navedene odredbe mogu poslužiti za analizu značenja pojma „akt agresije“. Na osnovu njih može se zaključiti sledeće:

- na odluku o prirodi „akta agresije“ ne utiče formalna deklaracija rata.[848]

---

[844] Definition of Aggression, član 1.

[845] Ibid, član 4.

[846] Ovaj argument je upotrebio ministar odbrane Estonije 2007. godine kada je je u medijima izvršio poređenje DDoS napada na Estoniju sa blokadom morskih luka.

Valentinas Mite, „Estonia: Attacks Seen As First Case of ‘Cyberwar’,“ *Radio Free Europe,* May 30, 2007, http://www.rferl.org/content/Article/1076805.html (preuzeto 2. aprila. 2016).

[847] Definition of Aggression, G.A. Res. 3314, član 3.

[848] Ibid, član 3, stav 1.

- agresija je primena oružane sile oružjem ili oružanih snaga prema teritoriji ili oružanim snagama druge države;
- agresija je blokiranje luka ili obala druge države;
- povreda sporazuma koja ugrožava teritorijalni suverenitet a ima posledice u daljoj primeni sile;
- angažovanjem neformalnih snaga da izvršavaju prethodno navedeno sa istim efektima primene sile.

Dakle, može se rezimirati da je agresija u međunarodnim odnosima primena oružanih snaga ili oružja. S obzirom da se oružane snage načelno deklarišu kao organizovane snage pod jedinstvenom kontrolom koje su naoružane, može se doći do zaključka da je organizovana primena oružja neke države ili ime te države primenom oružja na drugu državu akt agresije.

Treći značajan dokument međunarodnog prava u smislu procene da li je neki akt države primena sile ili agresija u smislu međunarodnih odnosa je presuda Međunarodnog suda pravde u slučaju *Nikaragva protiv SAD*. Navedenom presudom, sud je odlučio da su pojedine odredbe navedene u Definiciji agresije protivne međunarodnom pravu (miniranje luka, blokada luka, organizovanja pobunjenika da izvode akte oružane agresije protiv Vlade Nikaragve)[849].

Iako ni u jednom prethodno pominjanom sporazumu, konvenciji ili odluci suda nigde nije pominjan sajber prostor, sajber napad ili bilo kakva upotreba informacionih tehnologija u smislu napada, agresije ili primene sile, to ne mora da bude nepremostiv ograničavajući faktor. Termini u Povelji UN su opšteg karaktera i ne pominju vrstu oružja. Termini navedeni u Definiciji agresije se odnose na primenu oružanih jedinica, dakle na oružje. U navedenim dokumentima se čak ne pominje ni priroda efekata koje ti akti agresije ili oružane sile trebaju da ostvare da bi predstavljali agresiju ili napad (dakle ne pominje se fizičko uništenje ili ranjavanje i ubijanje ljudi kao posledica agresije ili napada). Dakle, postojeće odredbe ne pominju striktno sajber okruženje i aktivnosti, ali ne postoji prepreka da se odnose i na njih.

[849] Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Merits, 1986 I.C.J.Rep. 14, (June 27), http://www.icj-cij.org/docket/files/70/6503.pdf (preuzeto 22. avgusta 2015).

To potvrđuje i *Bečka konvencija o pravu međunarodnih ugovora,* čije generalno pravilo za interpretaciju međunarodnih ugovora određuje da „ugovor će biti interpretiran u dobroj volji i u skladu sa uobičajenim značenjem dodeljenom izrazima u ugovoru u njihovom kontekstu i u svetlu predmeta i svrhe ugovora“.[850]

11.2. Manifestacija državne moći i primena nadležnog prava

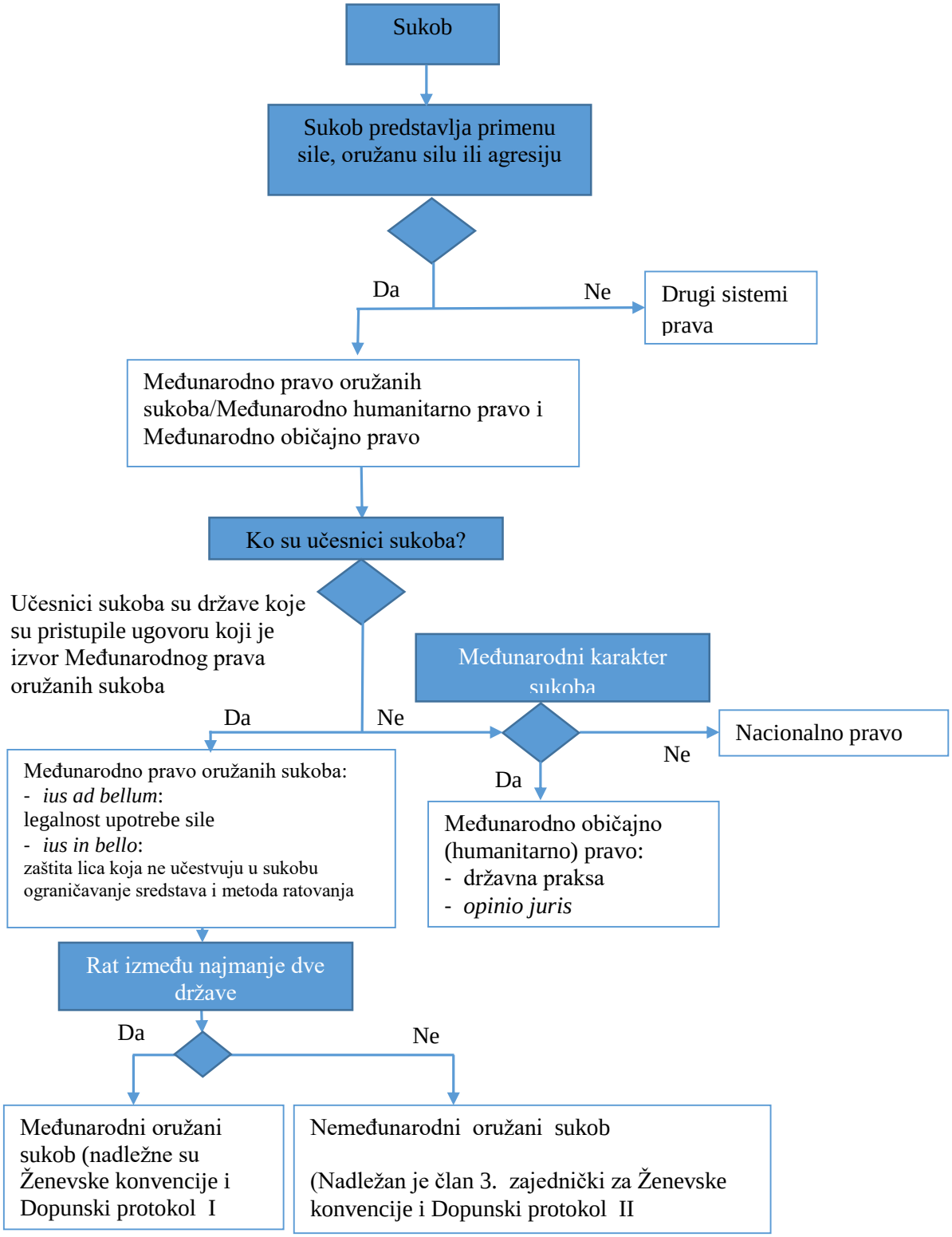
Međunarodno pravo oružanih sukoba se primenjuje na oružane sukobe u međunarodnim odnosima, čiji su učesnici međunarodne strane (države) koje su prihvatile sporazume, odnosno ugovore koje čine navedeno pravo. U slučaju da države nisu prihvatile nadležni međunarodni sporazum ili ugovor (na primer, sistem Ženevskih ili Haških konvencija) ili su ih parcijalno primenile, na sukobe se primenjuje međunarodno običajno pravo, to jest, njegova humanitarna komponenta (Slika 27).

Navedena podela nadležnosti prava u međunarodnoj zajednici se primenjuje na sve vrste međunarodnih sukoba u odnosu na njihovu formu i način vođenja sukoba, pa tako i na sukobe u sajber prostoru. Ova podela je posledica okolnosti da su vrhovni nosioci suvereniteta u međunarodnim odnosima države, a ne naddržavne organizacije, pa stoga same države odlučuju da li će prihvatiti nadležnost nekog sistema prava, pristupanjem međunarodnom sporazumu/ugovoru. Naravno, one to čine formalno nezavisno, ali u suštini njihova odluka zavisi od nacionalnih interesa i njihove sukobljenosti ili poklapanja.

Po Goldsmitu i Posneru, postoje četiri osnovna modela ponašanja država u međunarodnoj zajednici u odnosu na pravac i smer nacionalnih interesa putem kojih se vrši usklađivanje interesa i rešavanje njihove konkurentnosti: poklapanje interesa, koordinacija, saradnja i prisila.[851] U skladu sa navedenim modelima, države između ostalog donose odluke i o pristupanju međunarodnim pravnim sporazumima.

[850] Vienna Convention on the Law of Treaties, May 23, 1969, 1155 U.N.T.S. 331, 8 I.L.M. 679, član 31, stav 1.

[851] Jack l. Goldsmith and Eric A. Posner, *The Limits of International Law* (New York, NY: Oxford University Press, 2005), 12.



Slika 27. Dijagram nadležnosti prava na sukobe u zavisnosti od prirode sukoba, karaktera učesnika sukoba i pristupanje odgovarajućim međunarodnim ugovorima.

Države biraju da li će pristupiti nekom međunarodnom sporazumu, ili će ga prihvatiti, u celini ili parcijalno. Sve države koje prihvataju izvore Međunarodnog prava oružanih sukoba su dužne da se tokom sukoba ponašaju u skladu sa odredbama ugovora. Međutim, odbijanje države da pristupi nekom sporazumu je ne oslobađa odgovornosti za dela učinjena u toku ili u vezi sukoba. Međunarodno običajno pravo potiče od uspostavljene međunarodne pravne prakse i predstavlja jedan od izvora međunarodnog prava. To ističe i Statut Međunarodnog suda pravde[852], koji je vrhovni organ uspostavljen od strane Međunarodne zajednice u skladu sa Poveljom UN. Međunarodno običajno pravo se sastoji od pravne prakse (u relevantnoj oblasti) i subjektivne obaveze pravilnog postupanja država u međunarodnim odnosima, u skladu sa uspostavljenim sistemom verovanja i znanja pravnih stručnjaka u međunarodnim razmerama (lat. *opinio juris*).

Odnos između država zasnovan na moći oslikava se i u strukturi globalnog uređenja, simbolizovanim u njegovim ključnim dokumentima, poput Povelje UN, kao i hijerarhijom međunarodnih organizacija, skoncentrisanih u nadležnostima Saveta bezbednosti UN. Glavni narušavajući faktor primene međunarodnog prava u toku sukoba između država su suprotstavljeni nacionalni interesi i manifestacija diplomatske državne moći u uslovima sukobljenih interesa.

Međunarodno pravo pruža norme i pravila koje regulišu aktivnosti međunarodnih subjekata u sukobima u cilju njihovog sprečavanja i ograničavanja, i umanjivanja njihovih negativnih posledica. Problemi praktične regulacije sukoba u tradicionalnom okruženju nisu posledica tehnološke ili pravno-regulatorne prirode, već nemogućnosti primene prava u praksi kao posledica neravnomerne distribucije moći u međunarodnim odnosima. Nemogućnost praktične primene prava da se efektivno i efikasno primene norme i pravila se može svrstati u područje procesno-zasnovanih problema, koji su indukovani ometajućim uticajem državne moći u sprovođenju njihovih sukobljenih interesa.

Manifestacija državne moći se javlja i u procesu regulisanja oružanih sukoba, bez obzira na njihovo okruženje. Po Goldsmitu i Posneru, međunarodno pravo kao sistem postoji,

[852] Po članu 38(1)(b) Statuta Međunarodnog suda pravde, sud će pri donošenju odluka u skladu sa međunarodnim pravom, poput sporova pred sudom, „primenjivati međunarodne običaje, kao dokaz opšte prakse prihvaćene kao pravo“.

ali ima ograničenja koja mu postavljaju nacionalni interesi i ispoljavanje nacionalne moći.[853] Ovi autori ističu da je međunarodna zajednica u periodima nakon svetskih ratova i u vreme detanta nakon Hladnog rata sa dosta elana pristupala izgradnji sveobuhvatnih međunarodnih organizacija u oblasti trgovine, finansija i ekonomije, i usvajanju međunarodnih sporazuma u oblasti ljudskih prava i vladavine prava, zaštite životne sredine i očuvanja raznolikih kulturnih vrednosti u svetu. Ovaj entuzijazam u izgradnji zajedničkog pravnog sistema se sreće i na regionalnom nivou, na primer u slučaju Evropske Unije.[854] Međutim, u skladu sa tvrdnjom zastupnika realizma u međunarodnim odnosima, periodi kriza pokazuju da se konfliktne situacije u svetu češće rešavaju nasilnom primenom prava, odnosno primenom prava pobednika. Goldsmit i Posner na primeru međunarodnog pravnog sankcionisanja ratnih zločina, koji su se desili tokom sukoba u bivšoj Jugoslaviji, daju ocenu da je osnivanje i omogućavanje rada Međunarodnog krivičnog tribunala za bivšu Jugoslaviju[855] mnogo više bilo rezultat ispoljavanja vojne, diplomatske i finansijske moći NATO saveza (prvenstveno SAD) da ostvare svoje političke interese, nego što je rezultat funkcionisanja međunarodne zajednice.[856] U tom cilju, nacionalna moć SAD je manifestovana kroz finansijski i političko-diplomatski pritisak na države regiona da sarađuju sa navedenim međunarodnim sudom i druge države da sarađuju u procesu uspostavljanja i rada suda.

Drugi karakterističan primer dominacije nacionalne moći nad međunarodnim pravnim sistemom u slučaju regulacije oružanih sukoba je slučaj Međunarodnog suda pravde *Nikaragva protiv SAD*[857]. U navedenom slučaju, sud je presudio u korist Vlade Nikaragve, a protiv Vlade SAD, zbog obuke, naoružavanja, finansiranja i druge podrške opozicionim paramilitarnim snagama takozvanih „kontraša“ u njihovoj nelegalnoj borbi protiv organa i institucija legalno izabrane Vlade Nikaragve. Ta nezakonita pomoć se

[853] Goldsmith and Posner, *The Limits of International Law*.

[854] Na primer, Evropska Unija je politička organizacija nezavisnih država, koje su veliki deo vlastitog suvereniteta delegirali zajednici i uspostavili zajedničku politiku, organe i institucije, koja se u velikoj meri ponaša kao država (što objektivno i jeste, jer se radi o političkom savezu država).

[855] The International Tribunal for the Prosecution of Persons Responsible for Serious Violations of International Humanitarian Law Committed in the Territory of the Former Yugoslavia since 1991, the Hague.

[856] Goldsmith and Posner, *The Limits of International Law*, 116.

[857] Military and Paramilitary Activities In and Against Nicaragua (Nicar. v. U.S.), Merits, 1986 I.C.J.Rep. 14, (June 27), http://www.icj-cij.org/docket/files/70/6503.pdf (preuzeto 22. avgusta 2015).

odnosila na posledicu da su pobunjenici izvršili brojne zločine; na narušavanje suvereniteta Nikaragve nelegalnim preletanjem njene teritorije; na oružanu agresiju miniranjem nikaragvanskih luka i na trgovinski embargo, što je sud ocenio kršenjem međunarodnog prava. [858] SAD su tokom suđenja tvrdile da Međunarodni sud pravde, čije je osnivanje predviđeno Poveljom Ujedinjenih Nacija,[859] nema jurisdikciju da u ovom slučaju sudi ni SAD, niti jednoj drugoj naciji.[860] Američki ambasador u UN, Kirkpatrik, izjavila je tom prilikom da je sud „polu-pravno, polu-nadležno, polu-političko telo koje države nekada priznaju, a nekada ne“[861]. Po saopštavanju presude, zvanični predstavnik Bele kuće je naveo: „Odluke suda nisu pravosnažne. Sud nema moć da naređuje ništa“[862]. Inače, Međunarodni sud pravde ima jurisdikciju da donosi obavezujuće odluke u slučaju sporova između država koje priznaju nadležnost Suda u slučajevima koje podnose Sudu ili su je ranije priznale.[863] Takođe, samo šest godina pre presude Suda protiv SAD, Vlada SAD je priznala jurisdikciju Suda u slučaju zauzimanja njene ambasade u Iranu, od strane studentske islamske revolucionarne grupe[864, 865]. Tom prilikom je uputila zahtev Sudu[866, 867] da preduzme hitne mere u svojoj nadležnosti protiv Vlade Irana, pozivajući se na Statut

[858] *Nicaragua Case*, 1986 I.C.J. Rep 14 (1986), http://www.icj-cij.org/docket/files/70/6503.pdf

[859] *Charter of the United Nations and Statute of the International Court of Justice*, član 7, 36, Poglavlje XIV, članovi 92-96: 21-30, https://treaties.un.org/doc/publication/ctc/uncharter.pdf (preuzeto 22. avgusta 2015).

[860] „Rulling Illustrates World Court's Lack of Real Jurisdiction," *Times Daily*, May 13, 1984, 5D, https://news.google.com/newspapers?nid=1842&dat=19840513&id=e5UpAAAAIBAJ&sjid=tccEAAAAIBAJ&pg=2188,2978824&hl=en (preuzeto 08. januara 2015).

[861] „Rulling illustrates," Times Daily.

[862] Tyler Marshall, „World Court Rules U.S. Aid to Contras Is Illegal", *Los Angeles Times*, June 28 1986, http://articles.latimes.com/1986-06-28/news/mn-25504_1_contras (preuzeto 08. januara 2015).

[863] International Court of Justice (ICJ), *Statute of the International Court of Justice*, http://www.icj-cij.org/documents/?p1=4&p2=2, Article 36.

[864] *The Iran Hostage Crisis: A Chronology of Daily Developments, Report Prepared for the Committee on Foreign Affairs U.S. House of Representatives*, 97th Congress 1st Session, (Washington DC: Foreign Affairs and National Defense Division Congressional Research Service Library of Congress, 1981) https://www.ncjrs.gov/pdffiles1/Digitization/77922NCJRS.pdf

[865] David Patrick Houghton, US Foreign Policy and the Iran Hostage Crisis (Cabridge, UK: Cambridge University Press, 2004).

[866] Roberts B. Owen, Agent for the Government of the United States of America, Request for the Indication of Provisional Measures of Protection Submitted by the Government of the United States of America, http://www.icj-cij.org/docket/files/64/10663.pdf

[867] International Court of Justice (ICJ), Case Concerning United States Diplomatic and Consular Staff in Tehran (Unite States of America v. Iran), Judgment of 24 May 1980, (Official citation: *United States Diplomatic and Consular Staff in Tehran*, Judgment, I. C. J. Reports 1980, p. 3.), stav 1, strana 5.

Međunarodnog suda pravde[868] i pravila Suda[869]. Takođe, Vlada SAD je u više kasnijih slučajeva aktivno diplomatski inicirala i finansijski učestvovala u formiranju specijalnih međunarodnih sudova nadležnih da procesuiraju ratne zločine u različitim regionima.[870]

Iz ovog primera može se zaključiti da su odnosi između država u većoj meri posledica ispoljavanja nacionalne moći pri ostvarivanju nacionalnih interesa, nego što su rezultat vladavine univerzalnog međunarodnog prava zasnovanog na civilizacijskim vrednostima. Države stvaraju međunarodno pravo u većoj meri nego što međunarodno pravo stvara države.

Osnova tradicionalnog pristupa međunarodnog prava u području oružanih sukoba je **teorija pravednog rata**. Ova teorija nastoji da poveže princip legalnosti (primene prava) sa principom pravednosti (univerzalnom civilizacijskom moralno i etičkom kategorijom pravde) prilikom pokretanja sukoba (*ius ad bellum*) i u toku vođenja sukoba (*ius in bello*). Osnova za uspostavljanje teorije pravednog rata u međunarodnim odnosima je moralno prihvatljiva i legitimna sa aspekta dostignutih civilizacijskih vrednosti čovečanstva i uspostavljenog etičko-moralnog sistema ljudskog društva. Međutim, njena implementacija u uslovima konkurencije nacionalnih interesa i sukoba nacionalne moći u međunarodnim odnosima je ne čini referentnim alatom za institucionalnu primenu dostignutih vrednosti čovečanstva kroz instrumente međunarodnog prava, već u većoj meri, dodatnim sredstvom za ispoljavanja nacionalnih interesa dominantnih svetskih sila, posebno u formi vojnog intervencionizma.[871] Primena teorije pravednog rata na situacije koje karakteriše linearno ispoljavanje vojne moći u tradicionalnim oružanim sukobima u praksi dovodi do „zakrivljenja“ prava pod uticajem i delovanjem centara međunarodne moći i najčešće predstavlja formalni oblik regulacije sukoba. U uslovima kompleksnog sukoba u sajber prostoru koji se ispoljava u više ravni i na sasvim drugačiji način,

[868] International Court of Justice (ICJ), *Statute of the International Court of Justice*.

[869] International Court of Justice (ICJ), *Rules of Court* (1978), http://www.icj-cij.org/documents/index.php?p1=4&p2=3& (preuzeto 6. marta 2016).

[870] Međunarodni krivični tribunal za Jugoslaviju, Međunarodni krivični tribunal za Ruandu, Specijalni sud za Sijera Leone, Specijalni tribunal za Liban, Specijalni tribunal za Kambodžu i Ad hok sud za Istočni Timor.

[871] Simon Chesterman, *Just War or Just Peace?: Humanitarian Intervention and International Law* (Oxford, UK: Oxford University Press, 2001).

ugrožena je čak i ta formalna sposobnost nemogućnošću detekcije napada, identifikacije napadača i utvrđivanja odgovornosti država.

11.3. Primena postojećih dopunskih izvora međunarodnog prava po analogiji

Priroda sajber ratovanja je nejasna i složena, čak i bez tradicionalno prisutnih problema oko praktičnog razlikovanja ključnih pojmova i situacija tokom tradicionalnih međunarodnih oružanih sukoba. Somer i Braun smatraju da je "istinski sajber rat događaj koji ima karakteristike konvencionalnog rata, ali koji se isključivo vodi u sajber prostoru" [872]. Stoga, navedeni autori smatraju da je put za određivanje nejasne prirode sajber ratovanja u primeni istih testova koji se primenjuju u slučaju tradicionalnog sukoba. U tu svrhu navode neke ključne dokumente Međunarodnog prava oružanih sukoba, poput sistema Haških konvencija (iz 1899 i 1907. godine), Povelje UN, Konvenciji UN o zabrani genocida[873] ili Konvenciji UN o zabrani ili ograničavanju upotrebe određenih vrsta konvencionalnog naoružanja[874]. Spisak primenjivih konvencija se time ne završava. U stvari, svi izvori međunarodnog prava su ravnopravno primenjivi na sukobe između nacija u sajber prostoru. Takođe, u širem kontekstu, i drugi međunarodni sporazumi, koji nisu stvoreni u cilju regulisanja sukoba, već specifičnih aktivnosti u međunarodnim odnosima, mogu se primeniti i na određene situacije koje nastaju u toku sukoba.

Na primer, prvi izbor za traženje analogija između tradicionalnih propisa i savremenih tehnologija se odnosi na primenu propisa Međunarodne telekomunikacione unije (ITU).[875] Navedeni propisi su počeli da se razvijaju još krajem 19. veka, sa razvojem tada modernih telegrafskih telekomunikacija. Iako potiču iz pretprošlog veka ovi propisi se i

[872] Peter S. Sommer and Ian Brown, „Reducing Systemic Cybersecurity Risk", *OECD/IFP Project on Future Global Shocks* (OECD, 2011), 6, http://www.oecd.org/governance/risk/46889922.pdf (preuzeto 9. februara 2016).

[873] Convention on the Prevention and Punishment of the Crime of Genocide, Dec. 9, 1948, 78 U.N.T.S. 277.

[874] United Nations, *Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May be Deemed to be Excessively Injurious or to Have Indiscriminate Effects (and Protocols) (As Amended on 21 December 2001)*, 10 October 1980, 1342 UNTS 137

[875] International Telecommunication Union.

danas tiču sajber prostora, na primer, u odredbama koje se odnose na podvodne telekomunikacione kablove, koji čine fizičku osnova globalnog sajber prostora.[876]

Savremena digitalizacija svih komunikacija uvodi informaciono-komunikacione tehnologije i sajber prostor u domen važenja navedene konvencije, koje se generalno odnose na komunikacije, a ne njihovu specifičnu primenjenu tehnologiju. Na primer, bežične komunikacije brzo preuzimaju primat nad kablovskim. U okviru bežičnih komunikacija, tehnološki postaju dominantne računarske komunikacije koje omogućavaju brz prenos i veliki protok podataka, čija je funkcija zasnovana na računarskom internet protokolu. Na primer, osnova savremena tehnologija mobilne telefonije u svetu je LTE (eng. *Long-Term Evolution*, 4G LTE), koja je u potpunosti računarska informaciona tehnologija. Savremeni mobilni telefoni, kao i ostali uređaji za telekomunikacije su u stvari računarski uređaji.

Primenljivost tradicionalnih propisa na savremene tehnologije u nekim slučajevima je direktna. Na primer, Međunarodna telekomunikaciona konvencija (ITC) članom 35. zabranjuje članicama da narušavaju telekomunikacione servise drugih članica.[877] To znači da se njene odredbe primenjuju podjednako i na tradicionalne analogne kablovske, kao i na savremene digitalne računarski zasnovane komunikacije, odnosno na sajber prostor. Štaviše, područje moguće primene ovih tradicionalnih ugovora se ne odnosi samo na fizički i logički sloj sajber prostora, već i na informaciono-kognitivni. Na primer, član 37. Konvencije ITU nalaže članicama ITU da preduzmu mere radi prevencije prenosa i širenja lažnih i obmanjujućih signala za opasnost, poziva na uzbunu, lažnih bezbednosnih ili identifikacionih signala i nalaže im saradnju u lociranju i identifikaciji emiterskih stanica (uređaja) koje šalju takve signale sa njihove teritorije.[878]

Značaj ITU za regulisanje međunarodnih odnosa u sajber prostoru je veliki s obzirom da su statut ove organizacije prihvatile 192 države, članice Organizacije UN, uz jednu, koja to nije, a ima međunarodnopravni status (Sveta stolica u Vatikanu). Međutim, uprkos promenljivosti pojedinačnih odredbi pomenutih propisa o međunarodnim

[876] International Telecommunication Union, *International Telecommunication Convention*, Malaga-Terremolinos, 1973, http://www.itu.int/dms_pub/itu-s/oth/02/01/S020100001F4008PDFE.pdf (preuzeto 10. februara 2016).

[877] International Telecommunication Convention, član 35.

[878] International Telecommunication Convention, član 37.

telekomunikacijama na sajber prostor, kao i u slučaju primene propisa o regulisanju međunarodnih sukoba, generalno postoji previše nejasnih i neregulisanih situacija, i nedovoljno odredbi koje mogu da efektivno, efikasno i blagovremeno regulišu sukobe u sajber prostoru, da bi se moglo od njih očekivati da u potpunosti regulišu savremene situacije. Analizirajući prirodu sajber ratovanja, postaje očigledno da analogija između sukoba u sajber prostoru i fizičkom okruženju nije prosta niti je linearna. U tom pogledu, promenljivost tradicionalnog prava u specifičnim situacijama više predstavlja izuzetak, nego dobro uspostavljen pravni okvir.

11.4. Procena karaktera sajber napada u skladu sa međunarodnim pravom

Međunarodno pravo oružanih sukoba sačinjavaju dve velike grupe principa, normi i pravila koje se odnose na legalnost primene sile u međunarodnim odnosima (*ius ad bellum* pravila) i na regulisanje načina upotrebe sile tokom sukoba (*ius in bello* pravila). Obe grupe utiču podjednako na primenu prava na specifične sukobe u sajber prostoru. U skladu *sa ius ad bellum* pravilima, legalan je samo onaj napad na drugu državu koji je isključivo ostvaren u okviru prava na samoodbranu u skladu sa Poveljom UN[879] ili je u skladu sa nadležnom odlukom Saveta bezbednosti UN[880]. Pri tome, reč je o napadu koji predstavljaju primenu oružane sile, primenu sile, ili agresiju, bez obzira da li je izveden u fizičkom ili sajber prostoru. Pokrenuti sukobi se moraju se voditi u skladu sa međunarodnim pravom i običajima rata, odnosno sa *ius in bello* principima ratovanja, tokom svog perioda primene sile (sukoba), od izbijanja, pa do okončanja. Navedena pravila predstavljaju obaveze, ali ujedno i prava za sve učesnike sukobe, i potencijalne učesnike sukoba: napadača, napadnutih, i neutralnih strana.

Dakle, po Povelji UN država može legalno primeniti oružanu silu (ući u rat) u odnosu prema drugoj državi samo u dva slučaja:

- kada se tako brani od druge države (primena prava na samoodbranu definisana članom 51. Povelje UN i

[879] Povelja UN, član 51.

[880] Povelja UN, član 39.

– u skladu sa odlukom Saveta bezbednosti UN u cilju sprovođenja mera za uspostavljanje i očuvanje mira[881] (u skladu sa odredbama člana 39. Povelje UN o kolektivnoj akciji organizacije u cilju održavanja mira u svetu).

Problem predstavlja različita formulacija agresivnog ponašanja u samoj Povelji UN. Povelja naizmenično koristi tri slična, ali različita izraza:

1. "primena sile" u slučaju kada generalno zabranjuje ovu aktivnost u suprotnosti sa odredbama Povelje UN;[882]
2. "primena oružene sile", kada definiše kako će članice UN doprineti održavanju međunarodnog mira i bezbednosti[883], kao i u uvodnom delu Povelje kada napominje da su njeni ciljevi da obezbedi "da se oružana sila ne upotrebljava osim u opštem interesu"[884], i
3. "oružani napad", pri definisanju urođenog individualnog ili kolektivnog prava na samoodbranu[885] (član 51).

Problem predstavlja činjenica, da ni Povelja, niti drugi međunarodno pravni obavezujući dokument ne definiše navedene pojmove, odnosno ne pravi razliku između njihovog značenja. Imajući navedeno u vidu, mnogi pravni stručnjaci postavljaju pitanje da li navedeni pojmovi predstavljaju različite pragove za primenu neke od akcija predviđene Poveljom UN, odnosno pri definisanju nelegalne međunarodne aktivnosti u skladu sa Poveljom, s obzirom da su u navedena tri slučaja primenjeni jasno različiti izrazi?

11.4.1. Legalnost sajber napada

Prethodno navedene i analizirane definicije sajber napada opisuju njihova ključna svojstva iz različitih uglova posmatranja, vojnog, političkog, bezbednosnog i tehničkog. Analizom i procenom navedenih definicija može se doći do zaključka o opštim ključnim karakteristikama sajber napada:

- pokrenuti su namerno,
- sprovode se u sajber prostoru, iz sajber prostora i kroz sajber prostor,

[881] Povelja UN, član 39.
[882] Povelja UN, član 2, para. 4.
[883] Povelja UN, član 41. i 46.
[884] Povelja UN, Uvod.
[885] Povelja UN, član 51.

- ostvaruju se upotrebom informacionih sistema i dejstvo im je usmereno na informacije i informacione sisteme,
- napadači za pristup koriste ranjivosti u samom napadnutom sistemu da zaobiđu sigurnosne mehanizme,
- tokom napada se vrši nekakvo negativno dejstvo na cilj napada,
- efekti napada mogu biti različiti: od narušavanja integriteta sistema ili poverljivosti informacija do uništenja sistema.

Navedene definicije pokazuju da sajber napad nema isto značenje kao i napad u smislu međunarodnog prava. Dok napad u fizičkom okruženju, u sukobu između država, mora biti oružani i predstavlja oblik (oružane) agresije, napad u sajber okruženju načelno znači da je narušena informaciona bezbednost i da je učinjena nekakva neovlašćena radnja nad sistemom u nadležnosti napadnute strane. Znači, u praksi, da bi napad bio podložan Međunarodnom pravu oružanih sukoba potrebno je dokazati da je ekvivalentan oružanom napadu ili agresiji. A pošto se sajber napadi odvijaju direktnim dejstvom u logičkom okruženju sajber prostora (na logičke instrukcije i podatke) teško je naći drugu analogiju, osim po njihovim efektima. Dakle, iako "ne vidimo" napade, oni dostižu nivo oružanih napada ili agresije ukoliko su efekti koje su postigli dejstvom na cilj ekvivalentni ili identični efektima agresije. Veliki broj stručnjaka u svetu prihvata navedeni stav. Na primer, po Talinskom priručniku, stručnjaci međunarodnog prava koji su učestvovali u njegovoj izradi složili su se da primenom kriterijuma za određivanje nivoa ozbiljnosti posledica napada utvrđuje njegova težina i podložnost Međunarodnom pravu oružanih sukoba. Tako su se jednoglasno složili u svom savetodavnom stručnom stavu, da oni sajber napadi koji za posledicu imaju ranjavanje ili ubijanje lica ili oštećivanje ili uništenje materijalne imovine svakako zadovoljavaju uslov za deklarisanje da se radi o upotrebi sile koja podleže primeni međunarodnog prava.[886]

Navedeni kriterijum je izveden iz prakse Međunarodnog suda pravde u slučaju Nikaragva protiv SAD, iz 1986. godine Tom prilikom sud se pozvao na odluku (neobavezujuće) Rezolucije Generalne skupštine broj 3314 (XXIX) (Definicije agresije)[887] prilikom utvrđivanja da podrška pobunjenicima u naoružanju i logističkom opremanju ne

[886] Schmitt, *Tallinn manual*, 55.

[887] Definition of Aggression annexed to General Assembly resolution 3314 (XXIX).

predstavlja "oružani napad" već pretnja ili upotreba sile, odnosno mešanje u unutrašnje poslove suverene države.[888] Tada je sud primenio takozvani kriterijum obima i uticaja aktivnosti (eng. *scale and effects*), kao instrument za procenu da li neko neprijateljsko ponašanje dostiže nivo "upotrebe sile" u smislu međunarodnog prava.

Američki profesor prava, Majkl Šmit je navedeni test 1999. godine prilagodio za primenu u oblasti sajber ratovanja po sledećem okviru za određivanje prirode nekog sajber napada u smislu primene i nadležnosti Međunarodnog prava oružanih sukoba (da li je napad primena sile ili oružane sile) sačinjenom od pitanja i mogućih odgovora:

„(1) Da li je tehnika primenjena u računarskom mrežnom napadu upotreba oružane sile? Jeste, ukoliko je napad namenjen za direktno prouzrokovanje štete na fizičkim objektima ili za povređivanje ljudi;

(2) Ukoliko nije oružana sila, da li je računarski mrežni napad neki drugi oblik upotrebe sile, u skladu sa Poveljom UN? Jeste ukoliko je priroda njegovih posledica istovetna sa posledicama koje karakterišu upotrebu oružane sile;

(3) Ukoliko su računarski mrežni napadi upotreba sile (oružane ili neoružane), da li se mogu smatrati primenom sile u skladu sa principom samoodbrane kako je ona definisana u poglavlju VII Povelje UN ili važeći skup pravnih normi dozvoljava njihovu upotrebu u datim okolnostima?

   a) Ako je odgovor potvrdan, takva upotreba sajber napada će verovatno biti proglašena legalnom.

   b) Ako nije, a takav napad predstavlja upotrebu oružane sile, onda on krši član 2, stav 4 Povelje UN i običajno međunarodno pravo po pitanju zabrane upotrebe sile.

   c) Ukoliko nije, a takav čin predstavlja upotrebu sile, ali ne oružane sile, biće prekršen samo član 2, stav 4. Povelje UN."

(4) Ukoliko računarski mrežni napad nije dostigao prirodu upotrebe sile, da li postoji neka druga zabrana u međunarodnom pravu koja bi zabranila njegovu upotrebu? Najverovatniji propis, ako ne i jedini, bi bila zabrana mešanja u poslove druge države." [889]

[888] Nicaragua vs. US, para. 195.

[889] Michael N. Schmitt, „Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework," *The Columbia Journal of Transnational Law,* Vol. 37 (1999): 885-937, 934-936.

Šmitov okvir nudi ocenu legalnosti sajber napada (računarskih mrežnih napada po tadašnjoj terminologiji MO SAD) na osnovu tri ključna kriterijuma: nameri napadača, posledicama napada i postojanju osnova za primenu prava na samoodbranu (Tabela 13).

Tabela 13. Ključni kriterijumi pri utvrđivanju legalnosti sajber napada po Šmitu (1999).

Kategorija/Dilema	Ključni kriterijum
Procena oružane sile	Namera napadača
Procena drugog oblika sile	Posledice napada
Legalnost napada	U odnosu na pravo na samoodbranu

Međutim, navedena tri kriterijuma se dalje mogu redukovati na jedan. Pravo na samoodbranu je rezultat namere i određenih posledica napada (po intenzitetu i obimu dejstva). Dejstvo na cilj država koja je napadnuta može da utvrdi, ukoliko ima kapacitete da otkrije napad i sagleda njegove posledice. Dakle, za procenu legalnosti napada iz aspekta napadnute države i donošenja odluke da li će na napad uzvratiti drugim napadom, od osnovne važnosti je dokazivanje namere napadača.

S obzirom da je Šmitov okvir dugo godina bio jedini okvir te vrste koji je imao za cilj da pruži model kako tradicionalno pravo oružanih sukoba može regulisati sajber napade, od značaja za temu je analiza da li je i kako to moguće ostvariti.

11.4.2. Ocena namere u sajber napadu

Stav koji se analizira je sledeći: tehnika upotrebljena u sajber napadu predstavlja upotrebu oružane sile ukoliko je namenjena za nanošenje ozleda/ubijanje ljudi i/ili oštećivanje/uništavanje materijalnih stvari.

Svaka aktivnost primene oružane sile ili sile[890] u sukobima je namerna. Namera da se učini štetna posledica je sadržana čak i u nazivu malvera[891] (zlonamernog softvera). Po Ovensu, Damu i Linu, sajber napad se odnosi „namernu aktivnost na izmeni, poremećaju, obmani, degradaciji, ili uništenju računarskih sistema ili računara ili informacija i/ili programa koji se nalaze ili saobraćaju u tim sistemima ili mrežama“[892]. Jensen [893] smatra da je svaki sajber napad, sredstvo, metoda ili tehnika, čijom se primenom može namerno izazvati ranjavanje ili ubijanje ljudi, oštećenje ili uništenje materijalnih stvari i objekata u stvari upotreba sile. Upotreba sile je zabranjena u odnosima između članica UN, a oružana sila je specifična vrsta upotrebe sile.

Nameru u mnogim slučajevima nije neophodno ni dokazivati. Na primer, u slučaju sajber napada na neki izolovani informacioni sistem, za čiju informacionu bezbednost su primenjene stroge mere (na primer, ključne mere su kontrola pristupa, kriptografija, mere bezbednosti lica, ili zaštita informacija), namera napadača postaje očigledna čim se detektuje napad. Na primer, u slučaju napada na iransko nuklearno postrojenje u Natancu, napad nije mogao biti slučajno ostvaren. Kao prvo, nije mogao ni biti unet do informacionih sistema u tajnom postrojenju, fizički odvojenom od sveta i Interneta, bez preduzimanja specijalne tajne operacije. A kada je unet, malver je ostvario specifičnu funkciju prepoznavanja okruženja, sinhronizovanog blokiranja funkcije sistema na kontroli toka gasa kroz centrifuge i izazivanja kaskadnog efekta, koji je u kombinaciji sa netačnim signaliziranjem komandnom centru doveo do uništenja postrojenja.[894] Dakle, analizom samog napada je moguće utvrditi nameru. Sajber napad može biti primena

[890] Upotreba sile se pominje u članu 4 Povelje UN u smislu propisivanja državama članicama UN da se uzdržavaju od pretnje silom ili primene sile protiv teritorijalnog integriteta, političke nezavisnosti ili na drugi način u suprotnosti sa Poveljom.

Oružana sila se pominje u više stavova, a posebno u Preambuli, pri čemu se može zaključiti da je celokupna Povelja UN i sačinjena da spreči upotrebu oružane sile među nacijama i da pruži okvir za dostizanje i očuvanje mira.

[891] Eng. malware – zlonamerni softver.

Izraz malware je nastao spajanjem prefiksa mal (loš, zao) i softvawe (softver).

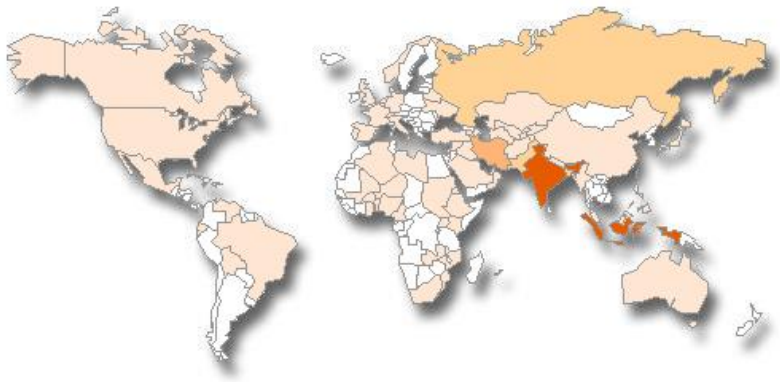
[892] William Owens, Kenneth Dam, Herbert Lin, *Technology, Policy, Law, and Ethics Regarding U.S: Acquisition and Use of Cyberattack Capabilities* (Washington, DC: The National Academic Press, 2009),S-1.

[893] Eric Talbot Jensen, ”Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense,” *Stanford Journal of International Law*, Vol. 38 (2002):. 207.

[894] Ralph Langner, *To Kill a Centrifuge* (Hamburg, DE: The Langer Group, 2013), http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf (preuzeto 23. oktobra 2015).

informacionog sistema, tehnike ili metode, pa se u svim tim slučajevima namera napadača vidi u doslednosti primene tih tehnika, metoda ili u dopremanju malicioznog sistema u okruženje u kome se manifestuje napad (u dodir sa ranjivošću sistema koji se napada).

Međutim, postoje i neki sajber napadi u kojima je moguće da se desi nenamerno dejstvo. Po studiji kompanije *Symantec*, malver Staksnet je pronađen u velikom broju sistema van Irana, širom sveta.[895]



Slika 28. Geografska distribucija malvera Staksnet.[896]

Iako je bio „podešen" programiranim logičkim instrukcijama da stupi u dejstvo u samo jednom specifičnom okruženju u kome su po određenoj šemi bile povezane 984 centrifuge[897] koje služe za obogaćivanje uranijumskog nuklearnog goriva,[898] imao programabilne logičke kontrolere i softver uređaja *Siemens Step7-417*, koji je na automatizovan način kontrolisao rad sistema. Međutim, praksa izrade softvera je pokazala da, u načelu, svaki softver sadrži greške i nedostatke koje u specifičnim situacijama mogu uzrokovati specifične otkaze. Simensov uređaj se nalazi u širokoj upotrebi širom sveta,

[895] Nicolas Falliere, Liam O. Murchu, and Eric Chien, *W32. Stuxnet Dossier, White paper* (Symantec Corp., Security Response 5, 2011).

[896] Ibid.

[897] William J. Broad, John Markoff, and David E. Sanger, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay," *New York Times*, January 15, 2011, http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=0 (preuzeto 25. oktobra 2015).

[898] Langner, *To Kill a Centrifuge*, 9.

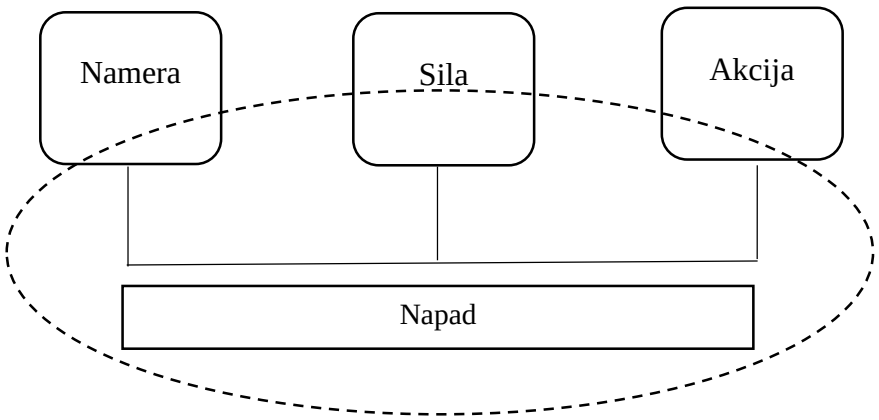
posebno u Evropi, gde se koristi za automatsko upravljanje raznim postrojenjima, uključujući i kritičnim. Sistemi u nuklearnim postrojenjima su skupi i postoji visoka verovatnoća da će njihovi proizvođači koristiti slične ili iste sisteme pri izgradnji različitih delova centrale ili centrala u različitim mestima. Teoretski i praktično je moguće je da zbog ugrađene greške u softveru malvera dođe do sličnih posledica u drugim sistemima u kojim se nenamerno nađe malver. Za otkaz u radu malvera je odgovorna ona strana koja ga je stvorila i postavila. Iako su mnogi stručnjaci isticali svojstvo malvera Staksnet da ima u sebi ugrađenu osobinu prepoznavanja cilja, zbog čega njegovi napadači poštuju princip razlikovanja u sukobima, oni svakako ne mogu da utiču na nenamerne otkaze sistema koji su stvorili.

Po Šmitu[899], da bi država imala pravo na samoodbranu i legalnu upotrebu oružane sile u cilju sprečavanja neprijatelja da je napada, prethodno mora dokazati da je postojala namera države napadača da je napadne. Namera se teško i veoma sporo dokazuje u međunarodnim odnosima, posebno u odnosima sukoba. A u sajber prostoru se može reći da je za najveći broj država u svetu i nemoguće da dokažu nameru napadača. Da dokazivanje namere agresije, državni organi moraju imati ostvaren pristup resursima kojima je napad izveden, u cilju pribavljanja potrebnih dokaza. Pošto napadači nisu voljni da pružaju dokaze o vlastitoj umešanosti u napade, ti dokazi se u slučaju sajber napada najčešće dobavljaju obaveštajnim operacijama u sajber prostoru, za šta kapacitet poseduje mali broj država su svetu. Zbog toga države u praksi retko dokazuju namernu upotrebu sile pre oružanog odgovora. Nelegalno pribavljeni dokazi o umešanosti države u sajber napad (primenom špijunaže) i sami predstavljaju narušavanje prava i ne mogu biti upotrebljeni u postupcima pred međunarodnim sudovima. Osim toga, njihov legitimitet nije kredibilan i prihvatljiv svim stranama u sukobu.

Dakle, namera je nužno svojstvo svakog napada. Drugo svojstvo je primena sile, a treće sama akcija sprovođenja namere za upotrebu te sile. Ukoliko je upotrebljeno oružje, reč je o oružanoj sili, a ako nije, onda je napad primena sile. Dakle, u cilju utvrđivanja razlike između „primene sile“ i „oružane sile“ potrebno je utvrditi da li je sajber napad, odnosno tehnika, metoda ili sistem koji se primenjuje u svojstvu napada, u stvari oružje. Primena

[899] Schmitt, „Computer Network Attack,” 903.

tehnike, metode ili sistema za napad podrazumeva da je ostvaren proces. Ukoliko se napadači mogu dovesti u vezu sa iniciranjem, planiranjem, organizovanjem i preduzimanjem procesa izazivanja štetnih posledica po cilj napada, namera se može dokazati. Zbog toga je neophodno utvrditi iz kojih faza se sastoji svaki napad. Napad ostvaren u sajber prostoru ili kroz sajber prostor je sajber napad. Karakteristika sajber prostora je primena i interakcija informacionih sistema i informacija koje su pohranjene u njima ili se kreću kroz te sisteme. Dakle, potrebno je utvrditi procese kojim se ostvaruje namera agenta pretnje da iskoristi ranjivost i nanese štetnu posledicu cilju.



Slika 29. Elementi napada u sajber prostoru ili kroz sajber prostor.

Profesor Šmit[900] je navedeni kriterijum naknadno modifikovao, tako da su osnovne karakteristike napada koje se moraju utvrditi u postupku njegove procene sledeće:

- **Ozbiljnost** (procena u odnosu na kvalitet, obim i intenzitet posledica napada; napad je ozbiljniji ukoliko su njegove posledice ozbiljnije; ukoliko posledice sajber napada obuhvataju fizičko ozleđivanje pojedinaca ili oštećivanje imovine, reč je o napadu koji odgovara oružanom napadu);
- **Neposrednost** (procena u odnosu na vreme manifestacije posledica napada i trajanje posledica; što se pre posledice pre manifestuju, države imaju manje

[900] Michael N. Schmitt, "Cyber Operations and the Jus ad bellum Revisited," *Villanova Law Review* 56 (2011): 576-577.

mogućnosti da traže miroljubivo rešenje spolja ili da na drugi način spreče negativne efekte napada);

- **Direktnost** (mera odnosa između direktnih posledica napada i krajnjih konsekvenci, što više slabe sekundarni efekti napada, manja je odgovornost napadača za eventualno kršenje prava);
- **Invazivnost** (kvalitet dejstva koji ostvaruje napad na cilj u smislu njegove ozbiljnosti; što je veća, veća je i težina napada, ne računajući špijunažu i ekonomske posledice; mera drastičnosti delovanja napada i rizika koju on podrazumeva; što je sistem branjeniji, potrebna je veća sila za prodiranje u njega)
- **Merljivost** (da li se mogu i kako izmeriti posledice napada, odnosno međusobno razlikovati posledice različitih napada; mogućnost merljivosti posledica, što su uočljivije i merljivije posledice napada, smatraće se da je više pogođen interes države);
- **Pretpostavljeni legitimitet** (sve što nije zabranjeno dozvoljeno je; na primer, propaganda, psihološke operacije, ekonomski pritisak samo po sebi i špijunaža nisu zabranjene, pa su dozvoljene i ne smatraju se primenom sile), i
- **Odgovornost** države (atribucija države kao napadača; procena jačine veze između države, aktivnosti njenih organa i institucija i izvedenog napada) [901, 902]

Međunarodna grupa eksperata okupljena oko Talinskog priručnika je prihvatila navedene kriterijume, s tim što je spisku dodala osmi kriterijumom, "vojni karakter" sajber napada. Navedeni kriterijum podrazumeva ocenu koliko sajber napad u svojoj prirodi ima vojni karakter, sa obrazloženjem da se pojam "upotreba sile" tradicionalno povezuje sa angažovanjem vojnih ili drugih naoružanih formacija.[903] Takođe, Talinski priručnik nudi stav da navedeni kriterijumi nisu konačni, već da svaka država može da ih proširi i modifikuje u skladu sa konkretnom situacijom, kao i da se navedeni kriterijumi trebaju uzeti u obzir zajedno. Na primer, visoko invazivan napad poput *DDoS* napada nema karakter primene oružane sile, jer nema moć nikakvog oštećenja, već samo da privremeno

[901] Schmitt, " Jus ad bellum Revisited."

[902] Katharina Ziolkowski, "Ius ad bellum in Cyberspace – Some Thoughts on the."Schmitt–Criteria*"* for Use of Force", in *4th International Conference on Cyber Conflict,* eds. Christian Czosseck, Rain Ottis and Katharina Ziolkowski, 300 (Tallinn, Estonia: NATO CCD COE Publications, 2012).

[903] Po Pravilu 11 – Definicija upotrebe sile, član 9, stav f, ističe se da Povelja UN naglašava karakter primene vojne sile u direktnim pominjanjem u Preambuli i u okviru smisla koji pruža član 44. Schmitt, *The Tallinn Manual*, 51.

onesposobi napadnuti sistem, i čim prestane njegovo dejstvo, sistem je ponovo operativan.[904]

Šmitov kriterijum je od ključnog značaja za ocenu prirode i legalnosti sajber napada. Kriterijum je uključen u Talinski priručnik, i to u cilju definisanja pojma "upotreba sile", pojedinačno najznačajnijeg pitanja u području sajber sukoba i ratovanja. Po Talinskom priručniku, "sajber operacija predstavlja upotrebu sile kada je njena procena primenom "obima i posledica"[905] uporediva sa ne-sajber operacijama koje dostižu nivo upotrebe sile. Pored vrste i intenziteta posledica, Talinski priručnik predlaže sprovođenje analize koja uključuje navedeni osam kriterijuma.

11.5. Praktična primenljivost kriterijuma "obima i posledica" na sajber ratovanje

Dakle, po Šmitu i Talinskom priručniku, koji nije službeni dokument NATO saveza, već dokument koji je nastao u njegovom projektu i za potrebe NATO, za procenu legalnosti sajber napada koristi se isti test koji je korišćen u slučaju Nikaragva protiv SAD (pravilo 195 presude), a koji se služi primenom procene testa "obima i posledica"[906] napada. Takođe, ovaj instrument se koristi za određivanje odnosa između "oružanih napada" i akata "upotrebe sile". Po stavu većine pravnih stručnjaka u svetu koji se bave navedenim problemom, svi oružani napadi predstavljaju upotrebu sile, ali svaka upotreba sile ne dostiže nivo oružanog napada.

Međutim, postavlja se praktično pitanje, da li je tako u pogledu sajber napada?

Ukoliko se navedeni princip koristi, svaki napad, ili bar većina napada, trebala bi biti uspešno procenjena i karakterisana njegovom primenom utvrđivanja legalnosti napada.

Iako navedeni kriterijum predstavlja nezvanični stav o procenu prirode sajber napada u svetlu međunarodnog prava, iz koga stoji NATO, on nije široko prihvaćen. On nije

[904] Schmitt, *The Tallinn Manual*, 52.

[905] Eng. *Scale and Effects*

Pojam u potpunosti preuzet iz presude Nikaragva protiv SAD, član 195, uveden u presudu radi procene da li su SAD primenile silu u smislu međunarodnog prava protiv Nikaragve, iako nisu izvele direktan napad na njenu teritoriju.

Nicaragua vs. US, para. 195.

[906] Eng. *Scale and Effects*

prihvaćen čak ni od strane SAD, iako su SAD ključna država i svojevrsni politički i vojni lider NATO saveza. Pored navedenog kriterijuma zasnovanog na primeni kriterijuma "obima i posledica" postoji još jedan, koji takođe nije objavljen u formi zvaničnog dokumenta, izrečen 2012. godine od strane zvaničnog predstavnika SAD na službenom skupu Vlade SAD, interagencijskom pravnom skupu u organizaciji Strategijske komande Ministarstva odbrane SAD o pitanjima primene međunarodnog prava na sajber prostor. Tom prilikom, pravni savetnik Stejt departmenta, Harold Koh, je održao govor u kome je na sistematičan način pružio odgovore, odnosno dao stav o 15 ključnih pitanja koja se odnose na primenu međunarodnog prava u sajber prostoru u području odbrane i bezbednosti.[907]

Koh smatra da navedeno pitanje razlikovanja pojmova „upotreba sile" i „oružana sila" nije ni relevantno u pogledu primene prava na samoodbranu. Po Kohu, u praktičnom pogledu primene prava na samoodbranu, SAD imaju neodvojivo pravo da se brane protiv svake nelegalne upotrebe sile. Koh navodi: „Po našem stavu, ne postoji prag za primenu smrtonosne sile da se ona kvalifikuje kao 'oružani napad' koji može naložiti primenu prisilnog odgovora".[908] Koh dalje tvrdi: „Mi primećujemo, s druge strane, da neke druge države i stručnjaci prave razliku između 'primene sile' i 'oružanog napada' aktivirajući pravo na samoodbranu, kao podskup skupa "primene sile", čime prolaze viši prag gravitacije…u tom pogledu postojanje komplikovanih pitanja u odnosu na *ius ad bellum* nije novo pitanje, to je pre primena starih dilema na novi razvoj tehnologije"[909] Dakle, svaka primena sile je osnov za "urođeno pravo na samoodbranu" države. [910]

Međutim, navedeni stav i dalje ne rešava dilemu oko odgovora na pitanje, šta predstavlja akt primene sile jedne države na drugu, odnosno u kom slučaju se može reći da je nastupio napad jedne države na drugu. Tim pre, što u međunarodnom pravu kao jedan od osnovnih principa prava se primenjuje princip po kome suverene države imaju pravo da postupaju po vlastitoj nameri sve dok to nije eksplicitno zabranjeno.[911] sve ono što nije zabranjeno,

[907] Harold Hongju Koh, *Remarks at the USCYBERCOM Inter-Agency Legal Conference,* September 18, 2012, http://www.state.gov/s/l/releases/remarks/197924.htm (preuzeto 11. oktobra 2015).

[908] Harold Hongju Koh, *Remarks*.

[909] Ibid.

[910] S.S. "Lotus" (Fr. v. Turk.), 1927 P.C.I.J. (ser. A) No. 10, at 88 (Sept. 7, 1927).

[911] Princip je razvijen iz odluke Stalnog suda međunarodne pravde u rešavanju slučaja sudara turskog i francuskog parobroda u međunarodnim vodama.

dozvoljeno je. Ovaj opšti princip međunarodnog prava, koga Šmit ističe kao osnovu za jedan od kriterijuma ocene legalnosti sajber napada, Po tom principu, ni špijunaža, ni ekonomske prisila, ni psihološko propagandne operacije u međunarodnim odnosima nisu zabranjene. Ovakav stav je komplementaran u pogledu primene Međunarodnog prava oružanih sukoba, koje je sankcioniše prethodno navedene oblike neoružane agresije, odnosno prisile, ali njegova primena predstavlja na karakterističan način tvrdnju da "pravo ne mora nužno biti i pravedno", što je, s druge strane u suprotnosti sa izvornim principima svakog prava, pa i međunarodnog.

11.6. Primenljivost ključnih principa prava oružanih sukoba na sukobe u sajber prostoru

Principa i pravila ima više i razvijena su u odnosu na specifične uslove i okruženja vođenja sukoba. Najznačajnije za većinu oružanih sukoba i shodno tome najčešću primenu tokom sukoba imaju principi razlikovanja civilnih i vojnih ciljeva, vojne neophodnosti, proporcionalnosti, čovečnosti i neutralnosti.

11.6.1. Razlikovanje u sajber sukobima

Sve strane u sukobu u toku napada moraju praviti razliku između legitimnih (zakonitih)[912] i nelegitimnih (nezakonitih) ciljeva napada. Bez obzira na vrstu, upotrebljeno oružje, ili primenjenu metodu i tehniku napada, jedino vojni ciljevi (koji ostvaruju doprinos oružanoj borbi ili se pripremaju za nju) su legitimni vojni ciljevi koji mogu biti napadnuti.[913] Primena principa razlikovanja se posebno odnosi i razvijena je u *ius in bello* pravilima ratovanja na napade na lica (borbe i neborce) i na napade na objekte (vojne, civilne i one sa dvostrukom namenom u odnosu na borbe i vojno angažovanje). U pogledu upotrebe napada u sajber prostoru jedne države na drugu državu (u idealnom i

[912] Iako ne postoji međunarodni „zakon" misli se na zakonitost u smislu poštovanja prihvaćenog međunarodnog sporazuma, ugovora, konvencije, običajnog prava i odluka nadležnih međunarodnih sudova čiju su nadležnost države prethodno prihvatile ili su se obavezale da će im pristupiti u smislu poštovanja njihovih odredbi.

[913] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), June 8, 1977, 1125 U.N.T.S. 3, entered into force Dec. 7, 1978, u daljem tekstu Protocol I.

pojednostavljenom slučaju), u oba slučaja postoje značajni problemi koji se tiču statusa direktne i posredne mete napada, utvrđivanja identiteta i atribucije napadača.

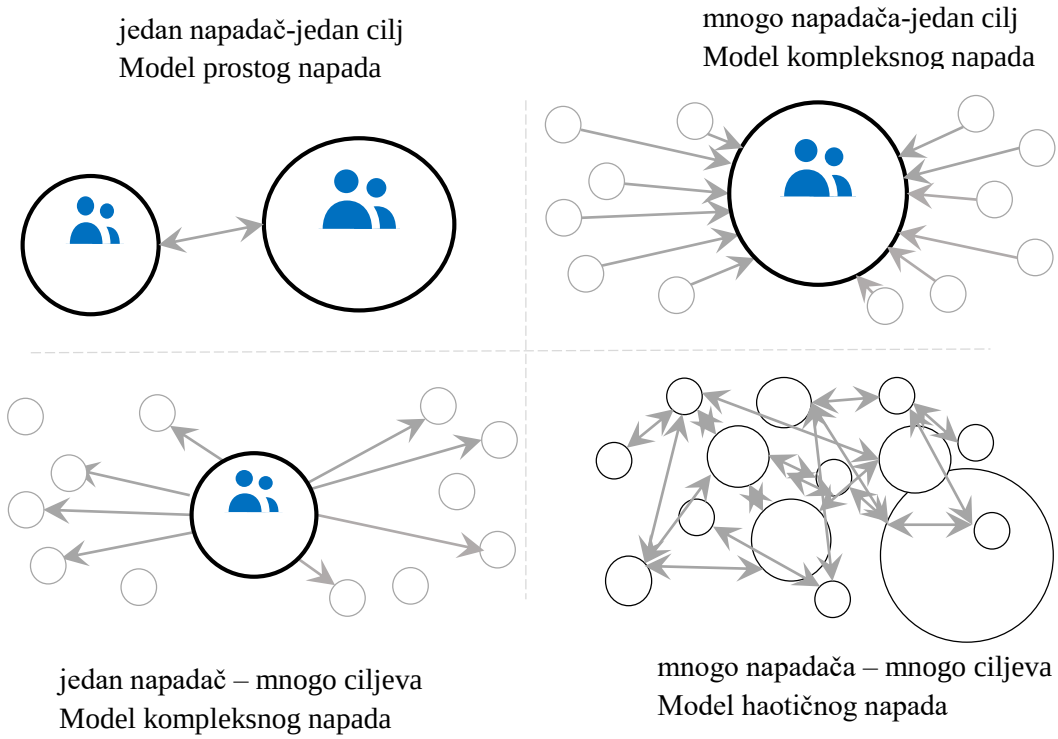
11.6.2. Razlikovanje osoba pri napadu u sajber prostoru

Svaki princip ratovanja je istovremeno i obaveza učesnicima sukoba i njihovo pravo kojim ih međunarodna pravila štite od druge strane. Dopunski protokol I[914] daje pravo pripadnicima oružanih snaga da primenjuju oružanu silu protiv protivničkih pripadnika oružanih snaga. To znači da samo borci mogu primenjivati oružanu silu protiv suparničke strane i da su samo borci ujedno i legitimni ciljevi napada protivničke strane, i to samo dok učestvuju u borbama ili se neposredno pripremaju za borbu. Zato su borci obavezni da se obeleže uniformom i oznakama u toku borbe i neposredne pripreme za borbu. Oni tako identifikuju svoj status borca, kako bi se razlikovali od civila, tačnije neboraca.[915]

[914] Protocol I, art. 43, para. 2.

[915] *Rule 62. Improper Use of the Flags or Military Emblems, Insignia or Uniforms of the Adversary* (International Committee of the Red Cross) in *Customary IHL Database,* https://www.icrc.org/customary-ihl/eng/docs/v1_rul_rule62 (preuzeto 8. januara 2016).

Čak i kada borci iz opravdanih razloga nisu u situaciji da se identifikuju uniformom i oznakama[916] dužni da se privremeno identifikuju otvorenim nošenjem oružja[917].



U odnosu na vremensku dimenziju, efekti napada mogu biti poznati u trenutku napada ili biti odloženi

Slika 30. Mogući uprošćeni modeli napada u sajber prostoru u odnosu na broj napadača i ciljeva napada.

Prethodno navedena (osnovna) pravila razlikovanja očigledno nemaju svoj praktični smisao u situacijama primene sajber napada, odnosno u sajber prostoru. Razloga za to ima više, a ključni se odnose na prirodu izvršenja sajber napada, napadače, metode napada i karakter njihovog dejstva, kao i na izmenjenu ulogu tradicionalno shvaćenih dimenzija prostora i vremena u sajber okruženju. Uloga napadača u sajber prostoru se veoma razlikuje od uloge napadača u tradicionalnom fizičkom okruženju. Takođe, obaveza

[916] Protocol I, art. 39, 44, and 46.
[917] Protocol I, art. 44, para. 3.

programera malvera, operatera ili bilo kog učesnika u lancu pripreme i preduzimanja sajber napada da bude u uniformi, obeležen vojnim oznakama ili naoružan, potpuno gubi smisao u sajber prostoru, jer je za napad nebitno gde se nalazi napadač. Ista situacija je i u slučaju vremenske dimenzije. Efekti sajber napada mogu biti odloženi. Jedan napad može obuhvatiti veliki broj ciljeva u različitim delovima sveta. takođe, mnogo napadača vremenski i prostorno distribuiranih mogu pripremiti vremenski diskretan ili kontinuiran napad na jedan cilj (Slika 30).

I u pogledu učesnika sajber sukoba razlikovanje nije moguće jednostavno ili čak nikako izvršiti. Informacioni sistem u vojnoj upotrebi može biti gotovo identičan, i često jeste identičan "civilnom" informacionom sistemu, ali isto tako, ni programer, operater ili korisnik sistema se ne mogu razlikovati po vojnom statusu i načinu njihove funkcije nad sistemom. Programer malvera može biti napadač, onaj ko neposredno izvršava napad, ali ne mora biti. U zavisnosti od minornih razlika u proceduri i organizaciji preduzimanja sajber napada, koje nikako ne mogu biti poznate napadnutoj strani, programer softvera i operater koji u nekom koraku učestvuju u pripremi napada mogu imati status borca ili neborca, pa čak i civila, a u skladu sa tim statusom imaju i prava u odnosu na sukob. Da li je civilni programer van vojne organizacije u tom slučaju borac, civil koji nelegalno učestvuje u borbama ili osoba sa potpunim statusom civila van sukoba ne može biti poznato nikome sem organizaciji napadača. Sajber napadi se uvek pripremaju i izvode prikriveno, u formi specijalne tajne operacije, uobičajeno u više različitih faza. Te faze su, načelno, obaveštajna priprema, nalaženje i procena ranjivosti cilja napada (eng. *target vulnerability assesment*), testiranje upada u sistem (eng. *penetration testing*), priprema eksploita i sadržaja ili instrukcije dela koji izvršava neposredno dejstvo napada (eng. *exploits and payloads planning and programming*), neposredno pokretanje napada (targeting), ubacivanje softvera u ciljani sistem (eng. *delivering*), Istraživanje ciljanog sistema radi prikupljanja potrebnih informacija za napad ili o dejstvu napada (eng. *exploitation*), izvršenje dejstva napada (eng. *payload execution*) i druge, u odnosu na vrstu cilja i izabranu tehniku i metodu napada. U svim nabrojanim fazama napadi se pripremaju i izvode izvan borbene zone (ili zone operacija), a za rezultat napada nije bitno da li ove faze planiraju, pripremaju i izvršavaju pripadnici oružanih snaga, civili ili automatizovani inteligentni sistemi.

Pored toga, u skladu sa rastućim trendom, civilno-vojne, odnosno javno-privatne saradnje u oblasti sajber bezbednosti i odbrane, privatne kompanije su sve češće angažovane na pripremi informacionih sistema i neposrednoj pripremi i izvođenju operacija za potrebe oružanih snaga. U mnogim državama, a posebno u SAD brojne privatne kompanije su angažovane na zadacima koje podrazumevaju ne samo planiranje i organizaciju, već i izvođenje ofanzivnih vojnih operacija.

U svakom slučaju, status u sukobu civila angažovanih na planiranju, organizaciji, podršci, obezbeđenju ili neposrednom izvršenju ofanzivnih sajber operacija može biti različit. On se može kretati od (legalnog) učesnika u sukobu, ilegalnog učesnika sukoba, plaćenika, ili špijuna. U skladu sa tim statusom, oni se od strane protivnika mogu smatrati civilima, neborcima (koji ne učestvuju u sukobu, niti ga neposredno pripremaju), legitimnom vojnom metom, borcima sa punim pravima u sukobu, špijunima ili plaćenicima, koji nemaju ni pravo učestvovanja u borbama, niti pravo na status ratnih zarobljenika.[918] Međutim, bez obzira na utvrđivanje njihove uloge i odgovarajućeg statusa, priroda sukoba u sajber prostoru čini da nema praktičnog načina da se odredi status navedenih učesnika sukoba, bilo da su oni civili ili pripadnici oružanih snaga, bez obzira da li su učesnici sajber sukoba direktno uključeni u sajber napade ili nisu. Dok je u tradicionalnim sukobima u fizičkom okruženju pripadnost oružanim snagama jedan od ključnih parametara za primenu principa razlikovanja lica u sukobima, pošto naoružani borci i izvode oružana vojna dejstva, za praksu sukoba u sajber prostoru u funkcionalnom i organizacionom pogledu, ta pripadnost je potpuno nerelevantna i stoga je njihovo razlikovanje uniformom i označavanjem grbovima besmisleno. Posledica je da se princip razlikovanja lica u sajber sukobu ne može u praksi primeniti, niti poštovati. Činjenica da vojne snage strana u sukobu ni po čemu nisu ograničene pri izboru naoružanja i vrste vojnih dejstava, osim radi poštovanja principa *ius in bello* pravila ratovanja omogućava ima da preduzimaju napade primenom tradicionalnog naoružanja sa fizičkim efektom u nekim akcijama odgovora na sajber napade. Nemogućnost principa razlikovanja lica kao vojnih ciljeva napada u toku oružanih sukoba može dovesti do nemogućnosti praktične primene prava, i u nekim slučajevima čak dovesti do eskalacije sukoba.

[918] Protocol I, art. 47, para. 1.

11.6.3. Proporcionalnost u sajber sukobima

Primena principa proporcionalnosti u toku oružanih sukoba je regulisana članovima 51. i 57 Dopunskog protokola I.[919] Princip proporcionalnosti u toku sukoba zahteva od strana u sukobu da ne preduzimaju one napade, od kojih se može očekivati da izazovu usputno ranjavanje i gubitak života civila, oštećenje civilnih objekata ili kombinaciju navedenih posledica, a koji se mogu smatrati prekomernom u odnosu na direktnu vojnu prednost koja je tim napadom ostvarena.[920] Navedeni princip se smatra univerzalnim i temeljnim principom ratovanja, pa je sadržan i u drugim izvorima Međunarodnog prava oružanih sukoba. Na primer, pominje se i u Protokolu II Ženevskim konvencijama, kao i u Dopunjenom Protokolu II o konvenciji određenim vrstam konvencionalnog naoružanja.[921] U opštem slučaju, u sukobima u fizičkom okruženju, njegove odredbe su jasne. Međutim, prilikom donošenja odluke o razmatranju o nadležnosti po tužbama koju je pred Međunarodni sud pravde podnela Savezna Republika Jugoslavija (SRJ) protiv deset država NATO, a zbog bombardovanja mimo odluke Saveta bezbednosti UN 1999. godine i gađanje civilnih ciljeva uz civilne žrtve, uključujući putnički voz pun civila na mostu i nacionalnu radio-televiziju, Specijalni komitet međunarodnog krivičnog tribunala za bivšu Jugoslaviju je dao sledeći komentar:

> Osnovni problem u vezi principa proporcionalnosti se ne tiče toga da li ona postoji ili ne, već šta ona znači i kako može biti primenjena…Na žalost, većina primena principa proporcionalnosti nije potpuno jasna. Mnogo je lakše formulisati princip proporcionalnosti u opštem smislu, nego ga primeniti u specifičnom skupu okolnosti zato što se poređenje često obavlja između različitih kvantiteta i vrednosti. [922]

Problemi u praktičnoj primeni principa proporcionalnosti u tradicionalnim sukobima se značajno uvećavaju u sajber okruženju. Zbog dualne prirode informaciono-komunikacionih tehnologija, i posebno njihove fizičke infrastrukture, gotovo je

[919] Protocol I, art. 51(5)(b), art. 57.

[920] Protocol I, art. 51(5)(b), art. 57.

[921] Protocol II to the Convention on Certain Conventional Weapons, Article 3(3) (*ibid.*, § 4); Amended Protocol II to the Convention on Certain Conventional Weapons, Article 3(8) (*ibid.*, § 4).

[922] The ICTY Committee Established to Review the NATO Bombing Campaign Against the Federal Republic of Yugoslavia, *Final Report to the Prosecutor*, press release, June 13, 2000, para. 48.

nemoguće u praksi primeniti navedeni princip, bar u pogledu ograničenja razarajućeg dejstva na telekomunikacionu infrastrukturu sajber prostora, bez obzira na to da li se ona nalazi u podvodnom[923], svemirskom[924], kopnenom okruženju, ili u elektromagnetnom spektru[925].

11.6.4. Problemi detekcije napada, atribucije napadača i odgovornosti država u sajber ratovanju

Svaka država ima obavezu da poštuje sve principe međunarodnog prava oružanih sukoba. Države time ispunjavaju vlastitu međunarodnu odgovornost i ujedno ostvaruju humanitarno pravo u toku sukoba, kao i svi učesnici sukoba i neutralne strane zahvaćene sukobom. Primena principa proporcionalnosti, izbora primene odgovarajuće i neophodne sile u odnosu na vojni doprinos napada, razlikovanja vojnih i civilnih ciljeva napada, ograničavanja izbora metoda i sredstava ratovanja, poverenja u odnosu na zakonite postupke suprotne strane i drugi principi ratovanja su decenijama prisutni u realnosti međunarodnih sukoba. Pa ipak, istorija i praksa oružanih sukoba nam pokazuju da se države ne pridržavaju propisanih principa u svim sukobima i u svakoj situaciji u fizičkom okruženju.

Čak i u slučaju da je primenom nekog instrumenta prava moguće ostvariti funkcionalan i jednoznačan sistem analogije između tradicionalnog prava i situacija sukoba u sajber prostoru, kakav je na primeri opšti test Međunarodnog suda pravde, ili Šmitov test, primenjen na situacije sajber sukoba, imajući u vidu specifičnu prirodu sajber napada i sajber ratovanja, postavlja se pitanje praktične primenljivost takvih normi, pravila i instrumenata. Za razliku od sukoba u fizičkom prostoru, proces kojim se ostvaruje sajber napad, kao i sami efekti sajber napada nisu očigledni. Posledice napada se po prirodi sajber napada ne mogu uvek, niti na vreme otkriti, a napadači ne mogu biti identifikovati.

---

[923] Paul Saffo, "Disrupting Undersea Cables: Cyberspace's Hidden Vulnerabilities," *Atlantic Council,* April 24, 2013, http://www.atlanticcouncil.org/blogs/new-atlanticist/disrupting-undersea-cables-cyberspaces-hidden-vulnerability (preuzeto 1. novembra 2015).

[924] Zachary Keck, "China's Next Super Weapon Revealed: Satellite Destroyers" *The National Interest,* April 15, 2015, http://nationalinterest.org/blog/the-buzz/chinas-next-superweapon-revealed-satellite-destroyers-12640 (preuzeto 3. novembra 2015).

[925] "Russian Military Unveils Revolutionary Electronic Warfare System," *Sputnik News,* March 4, 2015, http://sputniknews.com/military/20150304/1019042643.html (preuzeto 5. novembra 2015).

Shodno tome, ne može se utvrditi praktična odgovornost napadača za napade, niti odgovornost države za takvu radnju. Bez tih uslova nije moguća primena praktična primena međunarodnog prava u cilju regulacije sukoba u sajber prostoru.

U većini slučajeva nije moguće utvrditi ko je pisao programski kod malvera upotrebljenih za napade. Tragove koje nalaze lica koja vrše forenzičku analizu su takve prirode da ne predstavljaju materijalne dokaze o identitetu napadača. Konačno, autor malvera ne mora biti i napadač, jer savremena praksa u području sajber odbrane pokazuje da su specijalizovane kompanije aktivno i intenzivno uključene u proces kreiranja metoda i sistema za preduzimanje napada u sajber prostoru. Sam proces sajber napada se tehnički ne razlikuje u slučaju špijunaže i nastojanja da se napadnuti sistem ošteti. U nekim slučajevima ni sama primenjena tehnika napada ne omogućava atribuciju napadača, kao na primer, u slučaju napada zloupotrebom sistema adresiranja na Internetu (eng. *Domain Name System* - DNS), sistema samoregulacije optimalnog toka saobraćaja (eng. *Border Gateway Protocol* - BGP), ili primenom nekih specifičnih metoda napada popu *DDoS* napada ili *BotNet* mreža.

Dakle, u primeni međunarodnog prava na područje sukoba u sajber prostoru postoje opšta i specifična ograničenja. Opšta ograničenja se odnose na analognu primenljivost *ius ad bellum* i *ius in bello* sistema koji je stvoren da reguliše sukobe u fizičkom okruženju, na nove i posebne situacije sukoba u sajber prostoru. Specifični problemi se ogledaju u praktičnoj nemogućnosti da se primeni međunarodno pravo na situacije u sajber prostoru, i to posebno u sledećem:

a) detekciji da su se napad ili agresija u sajber prostoru dogodili;
b) identifikacija i atribucija napadača;
c) utvrđivanja postojanja odgovornosti subjekta međunarodnog prava za preduzeti napad i/ili agresiju u sajber prostoru.

11.7. Problemi uzrokovani tehnološkim ograničenjima

Problemi detekcije sajber napada, identifikacije i atribucije napadača od strane napadnutih ili neutralnih učesnika sukoba nastaju zbog kao posledica postojanja mogućnosti da napadači prikriveno izvedu napade. Ovakva mogućnost je zasnovana na samoj prirodi sajber napada, prikazanoj na modelima sajber napada "*cyber kill chain*" i

PrEP. U svakom slučaju, sajber napad je proces koji predstavlja pronalaženje i iskorišćavanje ranjivosti u napadnutom sistemu u cilju neovlašćenog upada u sistem i preduzimanjem daljih koraka napadača u skladu sa njihovim zamislima i namerama. Ukoliko je ranjivost mete poznata, postoji velika verovatnoća da će je lica zadužena za informacionu bezbednost otkloniti ili preduzeti mere da posledice napada budu što manje. Sajber napad je uspešan sve dok napadnuta strana nije svesna njegovog delovanja. Kada postane svesna sistem ili proces koji je zahvaćen dejstvom napada se izoluje iz mreže, ili mu se prekida njegova funkcija kako bi se maksimalno umanjile posledice napada. Sajber napadi najčešće i prestaju da budu i funkcionalno delotvorni u cilju doprinosa napadačima od trenutka njihovog otkrivanja.

11.7.1. Detekcija napada

Problem detekcije napada se odnosi na utvrđivanje okolnosti da je napad pokrenut, da je u toku njegovo ostvarivanje i dejstvo na cilj. Uzroci ovog problema su što napadnuta strana nije svesna ranjivosti ine ostvaruje potpunu kontrolu nad procesima, servisima i sistemima u svojoj nadležnosti. Zahvaljujući rastućoj kompleksnosti informacionih sistema, tu kontrolu odavno nije moguće ostvariti bez primene adekvatnih automatizovanih sistema za detekciju napada, odnosno analizu sopstvenih resursa.

Problem detekcije napada je ključni problem primene Međunarodnog prava oružanih sukoba na sukobe u sajber prostoru, a ne razlikovanje da li je sajber napad akt primene sile, oružane sile ili agresije. Da bi se mogla izvršiti procena primenljivosti *ius ad bellum* i *ius in bello* normi i pravila, nužan uslov je da je napad poznat napadnutoj strani.

Problem detekcije je svojstven za ratovanje u sajber prostoru. On gotovo da i ne postoji u fizičkom okruženju. Sama primena vojnih sistema naoružanja je vrlo očigledna. Sila i dejstvo vojnog naoružanja su lako uočljivi svim učesnicima sukoba, a to se odnosi čak i na lično, odnosno pešadijsko naoružanje. Dejstvo vojnog naoružanja je praćeno za zvučnim, svetlosnim, kinetičkim, toplotnim i hemijskim manifestacijama koje su lako uočljive bez ikakvih posebnih sistema za njihovu detekciju. Delovanje oružja ili projektila na cilj je trenutno i vrlo brzo se manifestuje po ispaljivanju od stran napadača. Savremeno naoružanje je instalirano na velikim i uočljivim borbenim sistemima, kao što su avioni, tenkovi, brodovi ili rakete. Ti vojni sistemi su i sami lako uočljivi. Posledice napada u

fizičkom okruženju su destrukcija, razaranje, ranjava ili uništavanje živog sveta, tako da ni po efektima nije moguće ne primetiti delovanje naoružanja.

S druge strane dejstvo sajber napada je po principu primene, svrsi i dizajnu prikriveno. U informacionoj bezbednosti moguće je prikriti prisustvo i dejstvo malicioznog softvera ili procesa. Moguće je preusmeriti rad legitimnih procesa i servisa i vremenski upravljati njihovim delovanjem. Za detekciju napada je najčešće neophodan poseban sistem ili postupak. Čak i kada je napad uspešan, on može ostati dugo vremena neotkriven. Čak i kada je efekat napada vidljiv, administratori sistema ne moraju znati da je reč o napadu, jer postoji mogućnost da se radi o slučajnoj ili nenamernoj grešci rada sistema, kakve su vrlo moguće, s obzirom na postajanje softverskih grešaka u svim sistemima. Napad na informacioni sistem se može izvesti na svakom od sedam nivoa modela komunikacija po ISO/IEC modelu[926], dok se napadi kinetičkom silom izvode i manifestuju samo na fizičkom nivou. Sajber napadi se potencijalno teže otkrivaju i što istovremeno mogu da ugrožavaju veći broj svojstava informacija i sistema (dostupnost, poverljivost, integritet, autentičnost, neporecivost), nego što je to slučaj u fizičkom okruženju.

Dejstvo napadača po strukturi i vremenu može biti kompleksno. Na primer, mogući su modeli napada:

- jedan napadač - jedan cilj,
- jedan napadač - mnogo ciljeva,
- mnogo napadača - jedan cilj ili
- mnogo napadača - mnogo ciljeva.

Takođe, dejstvo napada može biti vremenski odloženo.

Što je savremeno informaciono okruženje kompleksnije, povećava se broj uključenih i povezanih sistema, procesa i servisa, a sa njim i broj ranjivosti koje napadači mogu iskoristiti za napad i teže identifikovati sve procese u sopstvenom okruženju. Ukoliko napadnuta strana nema informaciju o tome da je napadnuta, o tome šta se u toku napada

[926] International Organization for Standardization, *ISO/IEC 7498-1:1994 Information technology -- Open Systems Interconnection -- Basic Reference Model: The Basic Model* (Geneva, Switzerland: ISO, 1994).

desilo, koje informacije, sistemi, procesi i resursi su joj ugroženi, odnosno ko je napadač, nije moguća praktična i efektivna primena Međunarodnog prava oružanog sukoba.

Otkrivanje napada ne zavisi samo od prirode sajber napada i umešnosti napadača da prikrije vlastito delovanje, već i od efikasnosti sistema informacione bezbednosti branilaca. Aktivnosti branilaca u odnosu na trenutak otkrivanja napada u sajber prostoru mogu biti a) **preventivne**, b) **detektivne** i c) **reaktivne**. U savremenim informacionim sistemima centralna pažnja se stavlja na preventivne mere odbrane od napada i na reaktivne mere kada se napad desi. Napadači teško mogu biti sigurni u mere detekcije napada, i one se odnose na utvrđivanje obrazaca ponašanje u sistemu, praćenje digitalnih potpisa datoteka, kao i na detekciju procesa u sistemu na osnovu analize i obrazaca ponašanja, praćenju anomalija, statistiku, kao i na preventivno delovanje, poput testiranja upada u sisteme ili procenu ranjivosti sistema. Sve to zahteva dodatno angažovanje tehničkih i personalnih resursa za detekciju napada, senzora, sistema za detekciju i prevenciju napada, što znači dodatne tehnologije, koja sa sobom donosi i nove ranjivosti.[927, 928] To je često nemoguće u velikim sistemima, kakvi su sistemi kritične (industrijske) infrastrukture, koji u svakom potencijalnom sajber sukobu spadaju u ciljeve sa najvećom verovatnoćom napada. U takvim velikim sistemima, zanavljanje sistemskih komponenti sa novim, koje imaju unapređenu bezbednost je često ekonomski nerentabilno i zahteva velike resurse, bez obzira što bi takva mera značajno unapredila bezbednost. Konačno, po samoj definiciji informacione bezbednosti, nikada nije moguće otkriti i otkloniti sve moguće ranjivosti koje akteri pretnje (sajber napadači) mogu iskoristiti. U procesu upravljanja rizikom informacione bezbednosti zbog toga se vrši procena prihvatljivih i neprihvatljivih rizika i samo oni neprihvatljivi rizici se otklanjaju. Međutim u vojnom okruženju i u situaciji političkog sukoba svi rizici po informacionu bezbednost, pa čak i oni najmanji mogu biti zloupotrebljeni od stane protivnika i njihove posledice mogu potencijalno biti katastrofalne.

[927] Jamal Raiyn, "A Survey of Cyber Attack Detection Strategies," *International Journal of Security and its Application* 8, no. 1 (2014): 247-256.

[928] Shailendra Singh and Sanjay Silakari, "A Survey of Cyber Attack Detection Systems," *International Journal of Computer Science and Network Security* 9, no. 5 (2009): 1-10.

11.7.2. Identifikacija i atribucija napadača

Problem identifikacije i atribucije napadača se odnosi na utvrđivanje identiteta napadača i dokazivanja da je neki konkretan napadač (entitet) počinio napad. Identifikacija je utvrđivanje identiteta entiteta od koga je potekao napad, njegovo prepoznavanje kao jedinstvene ličnosti, njegovo precizno razlikovanje od bilo kog drugog entiteta (sistema ili lica).[929] Atribucija je utvrđivanje odgovornosti entiteta za učinjeni napad. Atribucija je potreban proces u sajber okruženju zato što u sajber prostoru nema očigledne potvrde da je neko onaj za koga se predstavlja.

Proces autentifikacije u fizičkom svetu se ostvaruje identifikovanjem osobe i potvrdom da ta osoba zaista jeste ta za koju se predstavlja. Ta potvrda se ostvaruje nečim što posedujemo (na primer, lična karta), što znamo (na primer lozinka) i što jesmo (neka biometrijska mera ili sama osoba u fizičkom okruženju). Međutim, u sajber okruženju sve, ili gotovo sve može biti lažno predstavljeno ili pak moguće je zloupotrebiti nečiji identitet ili resurse. Neke metode napada se u suštini i sastoje u primeni te metode, kao na primer, *BotNet* napadi. Napad na sistem može doći sa nečijeg računara, a da njegov vlasnik nije ni svestan da je učestvovao u napadu. Njegov sistem je u tom slučaju zloupotrebljen, bez njegovog znanja i odgovornosti. Pošto su napadi u sajber prostoru podrazumevano prikriveni, atribucija napadača je neophodna. Ona podrazumeva šire i dodatne aktivnosti od identifikacije i autentifikacije nekog entiteta. Zbog toga je potrebno izvršiti atribuciju napadača, odnosno utvrđivanje njegove odgovornosti za napad. Neka osoba je odgovorna za neku aktivnost ili za posledicu te aktivnosti ukoliko je izvršila autorizaciju procesa ili aktivnosti koja je dovela do te posledice.[930] Atribucija je stvar dokazivanja, ali ne u sudsko-proceduralnom postupku, već u pravno-legalnom, koji predstoji sudskom postupku. Atribucija se odnosi na utvrđivanje odgovornosti za neki akt, ali i namere koja stoji iza neke aktivnosti. U međunarodnom krivičnom pravu u nekim slučajevima, kao što je pitanje genocida, ni namera nije dozvoljena.

[929] Autentifikacija podrazumeva identifikaciju i verifikaciju (potvrdu da je predstavljeni identitet tačan), pa je zbog toga to dvostepeni proces.

[930] Eliza Mik, "Identification and Attribution.," in *SelectedWorks of Eliza Mik* (Singapore Management University, 2007), 45.

Problem atribucije se u opštem smislu može redukovati na problem identifikacije, ali samo u situaciji kada je strana država podrazumevano odgovorna za neku akciju koja je preduzeta u odgovornosti njenog državnog suvereniteta, sa njene teritorije ili od strane lica u njenoj personalnoj jurisdikciji, što je čest slučaj u toku ratnog sukoba između dve države. U periodu mira, nije dovoljno utvrditi da je neki entitet pokrenuo napad, da bi se utvrdila odgovornost države. Zbog toga se identifikacija, autorizacija i atribucija u sajber okruženju moraju posmatrati zajedno.

Međutim, iako u sajber prostoru svi komunikacioni uređaji (serveri, ruteri, svičevi) beleže tragove u obliku metapodataka o ostvarenoj komunikaciji, kompleksnost globalnog sajber prostora onemogućava da svi ti podaci budu dostupni svakome u svakom trenutku. To je naročito slučaj u vreme političkih sukoba, odnosno rata. U toku ratnog sukoba, nije moguće da napadnuta strana insistirajući traži informacije o mrežnoj komunikaciji sa nekog uređaja koji je u nadležnosti druge države (teritorijalnoj nadležnosti, ukoliko je na teritoriji te države ili personalnoj, ukoliko je napad upućen sa servera u privatnom vlasništvu, koji koristi domen koji je dodeljen toj državi). U slučaju sajber sukoba, u odsustvu potpune saradnje između država, atribucija napadača je vrlo često nemoguća. Ključna aktivnosti u omogućavanju atribucije je sajber forenzika. Međutim, sajber forenzika zahteva institucionalnu saradnju između strana u sukobu i neutralnih tranzitnih strana, što je u slučaju političkih sukoba često neizvodljivo.

Zbog toga je čest slučaj da se neka država optužuje za izvedene sajber napade bez javno obelodanjenih dokaza. U tim slučajevima dokazi ne postoje, ili su pribavljeni na nelegalan način, na primer špijunažom, i stoga nisu ni međunarodno validni, jer nisu obostrano verifikovani.

Dakle, problem atribucije u toku sukoba je značajno ograničen. To dodatno usložava mogućnost da napadi budu ostvareni u „neumreženom“ modu. Većina ciljeva sajber napada u toku sukoba su važni sistemi, poput borbenih sredstava, telekomunikacionih sistema, centara za komandovanje, sistema kritične infrastrukture. Sajber napadi na njih se zato moraju izvesti na način da napadači uspešno prevaziđu takozvani izolacioni prostor (eng. *air gap*) između informacionih sistema i okolnih informacionih mreža. Takvi informacioni sistemi zbog očuvanja informacione bezbednosti nisu namenjeni za povezivanje sa javnim mrežama i okruženjem. Na primer, ključne faze najpoznatije

operacije sajber ratovanja, podmetanje Staksnet malvera u informacioni industrijski kontrolni sistem nuklearnog postrojenja Natanz u Iranu, nisu se odvijale na javnim mrežama, jer su sistemi za kontrolu nuklearnih centrifuga izolovani od spoljnih mreža, već u fizičkom svetu, neposrednim operativnim radom obaveštajaca na terenu. Kada se napadi izvode uz pomoć lica u napadnutom sistemu, ili prevazilaženjem prostorno-vremenske barijere između napadnutog sistema i okruženja, identifikacija i atribucija napadača je skoro nemoguća. Atribucija sajber napadača je ključni uslov za rad nadležnog suda i primenu prava. Nemogućnost identifikacije napadača i njegove atribucije u uslovima međunarodnih sukoba nosi sa sobom i dodatne opasnosti. Podmetanjem lažnih dokaza u cilju optuživanja treće strane za preduzimanje sajber napada je verovatna opcija u sukobima između država. To znači da je donošenje procena o poreklu napada na osnovu motiva nepouzdano i štetno po međunarodni mir.

Konačno, u pravnom pogledu, ukoliko nije identifikovan napadač, nije izvršeno dokazivanje njegove umešanosti u napad i odgovornost za posledice napada, nije moguće utvrditi ni odgovornost države. A bez državne odgovornosti za napad nema ni efektivne primene međunarodnog prava na sajber ratovanje.

12. ZAKLJUČAK

Sajber ratovanje je ratovanje u sajber prostoru. Konceptualno i u praksi, ono je različito od svih dosadašnjih formi ratovanja. Da bi se pojmovno odredili njegovo značenje i karakter, nužan uslov je prethodno definisanje fenomena sajber prostora. Ovaj fenomen je u potpunosti tehnološki zasnovan, menja se i razvija u skladu sa razvojem informaciono-komunikacionih tehnologija. Tokom perioda svog razvoja, sajber prostor je uvek imao istu, univerzalnu strukturu zasnovanu na slojevima, odnosno ista područja postojanja njegovih ključnih elemenata i funkcija: fizički, logički i kognitivni sloj. Logički sloj je centralni u pogledu omogućavanja funkcionisanja sajber prostora kao novog operativnog okruženja u kome se izvode međunarodni sukobi. On predstavlja područje matematičko-logičkih odnosa, definisanih logičkim pravilima i instrukcijama koje nastaju umnim radom ljudi. Algoritmi utiču na podatke i pokreću softver, koji pokreće hardver.

Sajber prostor je umrežen na nivou podataka. Podaci su element koji povezuje sva tri sloja sajber prostora. Podaci predstavljaju informacije u kontekstu, koje imaju ontološko značenje razumljivo ljudima, ali i veštačkim inteligentnim sistemima. Računari obrađuju podatke i omogućavaju kompleksnu automatizaciju procesa zasnovanih na podacima. Sajber ratovanje je ograničeno na sajber prostor i da bi se izvodilo, neophodna je primena informacionih sistema čija je funkcija zasnovana na tim matematičko-logičkim algoritmima. Prisustvo informaciono-komunikacionih sistema u fizičkom i društvenom okruženju stvara uslove za preduzimanje sajber napada, sukoba i ratovanja. Ključni faktor koji to omogućava je postojanje ugrađenih nedostataka i mana u informacionim sistemima i sajber prostoru. Ti nedostaci postaju ranjivosti ukoliko ih poznaje napadač i stekne sposobnost da ih iskoristi za pokretanje napada na informacioni sistem žrtve. Oružje kojim se preduzimaju sajber napadi nema materijalnu prirodu, ono je pre svega proces pronalaženja i iskorišćavanja ranjivosti u napadnutom sistemu i probijanja ili zaobilaženja bezbednosnih mehanizama zaštite tih sistema. Sajber napadi se izvode narušavanjem informacione bezbednosti napadnutih sistema, dok im posledice zavise od namene sistema, okruženja, primenjenih mera bezbednosti, znanja, sposobnosti i namere napadača. Uspešno izvedeni napadi u sajber prostoru ostavljaju posledice po napadnuti

sistem, koje zavise od uticaja informacionog sistema čija je informaciona bezbednost ugrožena napadom na njegovu funkciju i stanje. Sajber ratovanje je fundamentalno drugačiji oblik vođenja sukoba na međunarodnom nivou od tradicionalnih sukoba u fizičkom okruženju, koji je zasnovan na mogućnosti anonimne i prikrivene primene znanja o informacionoj bezbednosti.

Za sukobe u sajber prostoru nije od značaja okolnost da li je deklarisano stanje rata ili je u toku sukob u fizičkom kruženju. Pored toga, sama tehnika izvođenja napada je identična u svakom slučaju namernog narušavanja informacione bezbednosti napadnutog sistema, bez obzira da li je reč o obaveštajnoj ili borbenoj operaciji u sajber prostoru. Iako su tehnike i etape napada slične, efekti i posledice napada mogu biti veoma različite. Efekti napada mogu biti i prikriveni i vremenski odloženi. Tako se dolazi do situacije u kojoj tradicionalno Međunarodno pravo oružanih sukoba fundamentalno različito reguliše tehnički identične aktivnosti. Ova okolnost čini da primena analogije u cilju omogućavanja tradicionalnog Međunarodnog prava oružanih sukoba nije, niti može biti efikasna.

Sajber prostor, kao okruženje, i sajber napadi, kao elementi sukoba u sajber prostoru, su bili ključni predmet istraživanja. Cilj istraživanja je bilo utvrđivanje prirode sajber ratovanja, njegovih specifičnosti i načina moguće međunarodnopravne regulacije. Radi dokazivanja postavljenih hipoteza, prihvaćen je multidisciplinaran i interdisciplinaran pristup istraživanju. Sam sajber prostor se sastoji od tri osnovna nivoa realnosti (fizički, logički i kognitivni) čiji se sadržaji razlikuju, zbog čega je jedinstveni predmet istraživanja sagledan i analiziran u različitim aspektima. Na izbor takvog pristupa uticala je: potreba za redukovanjem kompleksnog okruženja koje je posledica visoke zastupljenosti informaciono-komunikacionih tehnologija u savremenom društvu; velika brzina i intenzivna dinamika razvoja tehnologija; univerzalna važnost i značaj ovih tehnologija za savremeni svet; kao i mogućnosti da se one primene za prikriveno i anonimno izvođenje napada, koji po svojim efektima mogu biti ekvivalentni tradicionalnim oružanim napadima u fizičkom okruženju.

U skladu sa osnovnom hipotezom istraživanja, došlo se do rezultata da se razvoj sajber ratovanja ne može pouzdano predvideti u dužem vremenskom periodu, niti je moguće njegovo efikasno regulisanje primenom Međunarodnog prava oružanih sukoba po

principu analogije sa situacijama u tradicionalnom ratovanju u fizičkom okruženju. Početni korak analize u istraživanju ove hipoteze je bilo utvrđivanje uzroka i izvora sajber ratovanja i sukoba. Kvalitativnom analizom više izvora zasnovanih na pristupu i stavovima predstavnika realizma u međunarodnim odnosima, utvrđen je značaj ovog pristupa u razumevanju i objašnjavanju motiva koji pokreću nastanak sukoba na međunarodnom nivou.

Na situacije sukoba u sajber prostoru u praktičnom smislu ne može efikasno biti primenjena podela na pravo mira i na pravo rata, pošto se sukobi u sajber prostoru odvijaju istovremeno i nezavisno od stanja rata i mira. Regulacija sukoba u sajber prostoru se mora zasnivati podjednako i istovremeno na različitim sistemima međunarodnog prava, poput ratnog i običajnog prava, uz istovremen uslov da mora biti usklađena i sa unutrašnjim nacionalnim pravnim sistemima.

Analizom potencijalnih učesnika sukoba u sajber prostoru identifikovani su osnovni nivoi na kojima se sajber ratovanje izvodi: naddržavni, nacionalni i organizacioni nivo. Izvođenjem studija slučaja o razvoju kapaciteta za sajber odbranu i ratovanje u Evropskoj Uniji, NATO i zajednici „Pet očiju“ došlo se do zaključka da je osnov za ispoljavanja nacionalne moći u sajber prostoru zasnovan na snazi i usmerenosti nacionalnih interesa, a ne na veličini i obimu zajednice i raspoloživih materijalnih resursa. Analizom studije slučaja regiona i država koje karakteriše veliki broj izbijanja sukoba u prethodnom periodu, uz nedovoljno razvijene kapacitete za primenu informaciono-komunikacionih tehnologija, došlo se do zaključka da je nužan osnov za izbijanje sukoba u sajber prostoru razvijeni sistem znanja u oblasti tehnologija i informacione bezbednosti. To je dovelo do zaključka da je sajber ratovanje posledica prirodnog procesa konkurencije nacionalnih interesa u međunarodnim okvirima, zasnovano na razvoju odgovarajućih tehnologija i znanja. Kao takvo, ono predstavlja specifičnu primenu znanja iz oblasti informacione bezbednosti u sajber prostoru za primenu sile nad protivnikom. Karakter sajber ratovanja prvenstveno zavisi od karaktera informacione bezbednosti i primene tehnologija, u čemu se nalazi i uzrok specifične prirode sajber ratovanja.

Analizom reprezentativnih modela napada u sajber prostoru, predloženih od strane Hera, i Hatčinsa, Kloperta i Amina, utvrđeno je da napade u sajber prostoru treba shvatiti kao **procese** iskorišćavanja ranjivosti u napadnutom sistemu, a ne kao primenu „sajber

oružja“. Navedeni zaključak značajno utiče na opravdanost primene analogije pravnih rešenja tradicionalnog sistema prava na situacije ratovanja u sajber okruženju. Izvođenjem dokaza da je sajber ratovanje tehnološki zasnovana primena sile nad protivnikom, sa istim uzrocima kao i tradicionalno ratovanje u fizičkom okruženju, ali sa različitim tehnološkim karakteristikama, došlo se do zaključka da se sukobi u sajber prostoru konceptualno i karakterno razlikuju od sukoba u fizičkom okruženju, iako imaju iste uzroke i ciljeve.

To nije jedina posledica tehnološke zasnovanosti sajber ratovanja. Imajući u vidu brzinu razvoja informaciono-komunikacionih tehnologija i dugoročnu nepredvidivost njenog razvoja, nije moguće pouzdano predvideti buduće forme sukobe u sajber prostoru, njihov značaj, uticaj i moguće efekte njihovog dejstva. To takođe znači da i nije moguće efikasno međunarodnopravno regulisanje specifičnog sistema primene prava na područje sajber ratovanja pristupom u kome se primenjuje novo tumačenje tradicionalnog prava u cilju rešavanja problema u primeni prava koji su posledica tehnoloških faktora.

U toku utvrđivanja ontološkog značenja sajber prostora i sajber ratovanja utvrđeno je da sama tehnologija i njena inherentna ograničenja predstavljaju faktor koji onemogućava jednoznačnu i pouzdanu detekciju sajber napada, identifikaciju i atribuciju napadača i utvrđivanje državne odgovornosti za napade. Navedene karakteristike sajber napada ujedno otežavaju svaku praktičnu primenu pravnog sistema u regulisanju sajber sukoba i ratovanja. Primena tradicionalnog Međunarodnog prava oružanih sukoba po analogiji na situacije u sajber prostoru je stoga moguća u teorijskom pogledu, ali praktično nije. Da bi se ovakva situacija prevazišla i ujedno očuvali nacionalni interesi koji pokreću primenu sile u sajber prostoru, trenutno jedini efikasan način regulisanja sukoba u sajber prostoru je široka primena međunarodnog javnog prava u odgovarajućim situacijama. Okosnica ovakvog rešenja je proces zaključivanje bilateralnih i multilateralnih sporazuma u cilju uzajamne kontrole, nadzora i razvoja kapaciteta i aktivnosti operacija u sajber prostoru. Analiza Goldsmita i Posnera daje potvrdu da ovakva rešenja imaju najviše šansi za uspeh, čak i u situaciji uzajamnog kršenja odredbi sporazuma i postojanja konkurencije nacionalnih interesa. U međunarodnoj zajednici postoje instrumenti za sprečavanje nastanka sukoba i svode se na primenu mehanizama za mirno rešavanje sporova i kontrolu sukoba. Savremene informaciono-komunikacione tehnologije pružaju osnov svim

akterima u međunarodnoj zajednici, bez obzira na političku, vojnu ili ekonomsku moć da ispolje svoje interese, jer kao osnov moći uvode specifično znanje i veštinu primene znanja koja su rezultat područja istraživanja računarskih nauka, informaciono-komunikacionih tehnologija i informacione bezbednosti. Znanje u navedenim oblastima je najčešće proporcionalno ekonomskoj, industrijskoj, društvenoj, političkoj i vojnoj moći država, ali nekada i one države, pa i međunarodni faktori koji nemaju međunarodnopravni legitimitet mogu da poseduju potrebno znanje i veštine da pokreću napade u sajber prostoru. To dovodi do povećanja broja aktera na međunarodnom nivou koji su sposobni da vode sukobe u sajber prostoru. Ključni uzrok za ovakvu situaciju je okolnost da preduzimanje napada u sajber prostoru predstavlja specifičnu primenu znanja i veština ugrožavanja informacione bezbednosti u sajber prostoru.

Sukobi u sajber prostoru nisu prvi oblik tehnološki zasnovanih sukoba, već je to konstantan cilj međunarodne zajednice. Pa ipak, ti napori nisu zaustavili razvoj naoružanja koje je bilo predmet njihove regulacije. Štaviše, rastuća umreženost i povezivanje sajber prostora, živog sveta i fizičkog okruženja na nivou podataka, pruža mogućnost za obimniju i ozbiljniju primenu sajber ratovanja u budućnosti sa ozbiljnijim efektima. To znači, čak i da se ostvari trenutni uspeh u regulaciji upotrebe informaciono-komunikacionih tehnologija u svrhu vođenja sukoba, takav uspeh može biti samo trenutnog karaktera.

Navedeni zaključci do koji se došlo tokom istraživanja pokazuju da primenu informacionih tehnologija za sukobe u sajber prostoru nije moguće efikasno regulisati primenom tradicionalnog prava oružanih sukoba, koje je nastalo na osnovu prakse i potrebe regulisanja sukoba u fizičkom okruženju. Primena tradicionalnog prava na nove situacije u sajber prostoru ima kapacitet za teorijsko rešenje problema, ali nema moć praktične regulacije situacija sukoba u sajber prostoru. To ograničenje je tehnološke prirode i ne može se nadomestiti međunarodnopravnom regulacijom. Ono se pre svega odnosi na nemogućnost pravovremene i potpune detekcije sajber napada, identifikacije i atribucije napadača i utvrđivanja odgovornosti država za napade.

Imajući u vidu način ispoljavanja nacionalne moći u međunarodnim odnosima, ograničenja procesa nastanka međunarodnog prava, tehnološku prirodu informaciono-komunikacionih tehnologija i brzinu njihovog razvoja, rešenje koje ima sposobnost

najefikasnije i najpraktičnije regulacije međunarodnih odnosa predstavlja pristup zaključivanja bilateralnih i multilateralnih ugovora između zainteresovanih strana. Kao elementi koji podržavaju stavove takvih ugovora mogu se upotrebiti sve pozitivne norme, principi i propisi međunarodnog javnog prava, svi izvori prava i svi opšti principi prava oko kojih se slažu strane potpisnici. Navedeni pristup je pokazao uspeh u regulisanju i ograničavanju trke u nuklearnom naoružanju tokom hladnog rata između vojnih supersila i imao je veću moć ograničavanja opasnosti od sukoba ovim oružjem od neobavezujućih deklaracija i sporazuma o legalnosti nuklearnog naoružanja.

Primera za navedeni pristup u svetu već ima, i oni se odnose na sporazume u oblasti sajber bezbednosti između ključnih svetskih sila poput SAD i Rusije, odnosno SAD i Kine. Iako nema moć da otkloni probleme nastale kao posledica brzog razvoja informaciono-komunikacionih tehnologija i sporog razvoja međunarodnog javnog prava, ovakav pristup ima i najmanje potrebe za time, čime omogućava praktično uspostavljanje odnosa poštovanja i mira, uz omogućavanje zainteresovanim stranama dalji razvoj sposobnosti za sajber odbranu.

LITERATURA

1. ABI Research. „$10 Billion Defense Cybersecurity Spending Boosts Cyberwarfare Technologies,“ November 12, 2015. https://www.abiresearch.com/press/10-billion-defense-cybersecurity-spending-boosts-c/ (preuzeto 12. januara 2016).
2. ABI Research/ITU. *Global Cybersecurity Index & Cyberwellnes Profiles Report* (2015). https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf (preuzeto 1. februara 2016).
3. AdaCore. „Safe and Secure Software - An Invitation to Ada 2005.“ http://www.adacore.com/knowledge/technical-papers/safe-secure/ (preuzeto 18. januara 2016).
4. Agence-France Presse, “Project Loon: Google Baloon that Beams down Internet Reaches Sri Lanka,” *The Guardian*, February 16, 2016, http://www.theguardian.com/technology/2016/feb/16/project-loon-google-balloon-that-beams-down-internet-reaches-sri-lanka (preuzeto 17. februara 2016).
5. Ali, Idrees and Andrea Shalal. „F-35 Chief Cites 'Good, Bad and Ugly' About No. 1 U.S. Arms Program.“ *Reuters*, March 24, 2016. http://www.reuters.com/article/us-lockheed-f35-software-idUSKCN0WP26V (preuzeto 27. marta 2016).
6. Amos, Stan W. and Mike R. James. *Principles of Transistor Circuits.* Woburn, MA: Newnes Butterworth-Heinemann, 2000.
7. Anderson, Nate. “Confirmed: US and Israel Created Stuxnet, Lost Control of it.” *Ars Technica*, June 1, 2012, http://arstechnica.com/tech-policy/2012/06/confirmed-us-israel-created-stuxnet-lost-control-of-it/ (preuzeto 14. Decembra 2015).
8. Rettman, Andrew. „Sweden: Who Needs NATO, When You Have the Lisbon Treaty?“ *EU Observer*, April 22. 2013, https://euobserver.com/news/119894 (preuzeto 22. april 2016).
9. *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), Judgment.* I.C.J. Reports 2007.
10. Arbeitsgemeinschaft Kriegsursachenforschung (AKUF). „Definition and Typology of War.“ http://www.wiso.uni-hamburg.de/en/fachbereiche/sozialwissenschaften/forschung/akuf/akuf/kriegsdefinition-und-kriegstypologie/#c84532 (preuzeto 13. septembra 2015).
11. Arbeitsgemeinschaft Kriegsursachenforschung AKUF. http://www.wiso.uni-hamburg.de/en/fachbereiche/sozialwissenschaften/forschung/akuf/akuf/ (preuzeto 13. septembra 2015).
12. Ariane 501 Inquiry Board Report. *ARIANE 5, Flight 501 Failure*, Paris, July 19, 1996. http://esamultimedia.esa.int/docs/esa-x-1819eng.pdf (preuzeto 15. decembra 2015).
13. Arimatsu, Louise. “A Treaty for Governing Cyber-weapons.” In *2012 4th International Conference on Cyber Con, Proceedings*, edited by Christian Czosseck, Rain Ottis and Katherina Ziolkowski, 91-109. Tallinn: NATO CCD COE Publications, 2012.

https://ccdcoe.org/cycon/2012/proceedings/d3r1s6_arimatsu.pdf (preuzeto 23. septembra, 2015).
14. Armitage Richard L. and Joseph S. Nye. Center for Strategic and International Studies (CSIS). *CSIS Commission on Smart Power: A Smarter, More Secure America*, http://csis.org/files/media/csis/pubs/071106_csissmartpowerreport.pdf (preuzeto 24. februara 2016).
15. Arquilla, John, and David Ronfeldt, eds. *In Athena's Camp, Preparing For Conflict in the Information Age.* Santa Monica, CA: Rand Corporation, 1997.
16. Arquilla, John and Douglas A. Borer, eds. *Information Strategy and Warfare: A Guide to Theory and Practice.* London, UK: Routledge, 2007.
17. *ATIS Telecom Glossary.* http://www.atis.org/glossary/ (preuzeto 15. decembra 2015).
18. Austin, Greg. „Russia's Cyber Power." *New Europe*, October 26, 2014. http://neurope.eu/article/russia%E2%80%99s-cyber-power/ (preuzeto 20. februara 2016).
19. Austria, Bundeskanzleramt Osterreich. *Austrian Cyber Security Strategy*, 2013. http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world (preuzeto 12. januara 2016).
20. Azizian, Nazanin. „Defense Intelligence Information Enterprise (DI2E)." Office of the Under Secretary of Defense for Intelligence, October 29, 2014, PowerPoint Presentation, 5. http://www.dtic.mil/ndia/2014system/16835WedTrack6Azizian.pdf (preuzeto 22. januara 2016).
21. Bamford, James. „NSA Snooping Was Only the Beginning, Meet the Spy Chief Leading Us Into Cyberwar." *Wired*, June 12, 2013. http://www.wired.com/2013/06/general-keith-alexander-cyberwar/, (preuzeto 20. maja 2015).
22. Bamford, James. „The Most Wanted Man in the World." *Wired*, August 22, 2014. http://www.wired.com/2014/08/edward-snowden/ (preuzeto 22. novembra 2015).
23. Bamford, James. *The Shadow Factory: The Ultra-Secret NSA from 9/11 to the Eavesdropping on America.* New York: Anchor Books, 2008.
24. Obama, Barack and Xi Jinping. "Joint News Conference" (News Conference, White House, September 25, 2015). *C-span.* http://www.c-span.org/video/?328351-3/president-obama-chinese-president-xi-joint-news-conference (preuzeto 15. januara 2016).
25. Barker, William C. *Guideline for Identifying an Information System as a National Security System, SP 800-59*. National Institute of Standards and Technology – NIST, 2003.
26. Bassiouni, Cherif M. „International Crimer: The Ratione Materiae of International Criminal Law." In *International Criminal Law. Vol. 1, Sources, Subjects, and Contents*, edited by Bassiouni M. Cherif. Leiden, Netherlands: Martinus Nijhoff Publishers, 2008.
27. Belasco, Amy. *The Cost of Iraq, Afghanistan, and Other Global War* (CRS Report No. RL 33110). Washington, DC: Congressional Research Service, 2014. https://www.fas.org/sgp/crs/natsec/RL33110.pdf.

28. Bertuglia, Cristoforo Sergio and Franco Vaio. *Nonlinearity, Chaos & Complexity, the Dynamics of Natural and Social Systems*. New York, NY: Oxford University Press, 2005.
29. Blaker, James R. *Transforming Military Force, The Legacy of Arthur Cebrowski and Network Centric Warfare*. Westport, CT: Preager Security International, 2007.
30. Bloomberg. *The Bloomberg Innovation Index: High-Tech Companies*, http://www.bloomberg.com/graphics/2015-innovative-countries/ (preuzeto 2. Januara 2016).
31. Boot, Max. *War Made New: Technology, Warfare, and the Course of History, 1500 to Today*. New York, NY:Penguin Group, 2006.
32. Booz Alen Hamilton. „Booz Allen Statement on Reports of Leaked Information," press release, June 11, 2013. http://www.boozallen.com/media-center/press-releases/2013/06/statement-reports-leaked-information-060913 (preuzeto 20. decembra 2015).
33. Brewin, Bob. „NSA Seeks to Open Classified Network to Allies." May 17, 2007. http://www.govexec.com/defense/2007/05/nsa-seeks-to-open-classified-network-to-allies/24458/ (preuzeto 20. maja 2015).
34. *British Standard ISO/IEC 25010:2011, Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models*. http://janus.uclan.ac.uk/pagray/BS-ISO-IEC%2025010%202011%20quality%20requirements%20models.pdf (preuzeto 20. decembra 2015).
35. Broad, William J., John Markoff, and David E. Sanger. "Israeli Test on Worm Called Crucial in Iran Nuclear Delay." *New York Times*, January 15, 2011. http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=0 (preuzeto 25. oktobra 2015).
36. Brown, Marcel. „World, Meet the Internet." *This Day in Tech History.* http://thisdayintechhistory.com/07/03/world-meet-the-internet/ (preuzeto 13. aprila 2016).
37. Buffaloe, David L. "Defining Asymmetric Warfare." *The Land Warfare Papers, Institute of Land Warfare* 58 (2006): 1-34. https://www.ausa.org/SiteCollectionDocuments/ILW%20Web-ExclusivePubs/Land%20Warfare%20Papers/LWP_58.pdf (preuzeto 10. novembra 2015).
38. Bunker, Robert J. and Charles „Sid" Heal, eds. *Fifth Dimensional Operations: Space-Time-Cyber Dimensionality in Conflict and War—A Terrorism Research Center Book.* Bloomington, IN: iUniverse LLC, 2014.
39. Canada, Government of Canada. *Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada,* 2010. http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/index-eng.aspx (preuzeto 12. januara 2016).
40. Castells, Manuel. "Information Technology, Globalization and Social Development," *United Nations Research Institute for Social Development (UNRISD) Publications*, 114 (September 1999): 1-23, http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?id=29033 (accessed 11 November, 2015).

41. Cavusoglu, Huseyin, Hasan Cavusoglu, and Jun Zhang. "Economics of Security Patch Management." In *Workshop on the Economics of Information Security - WEIS*. Robinson College, University of Cambridge, England, 2006.
42. Cebrowski Arthur K. and John J. Garstka. "Network-centric Warfare: Its Origin and Future." *US Naval Institute Proceedings*, 124, no. 1 (1998): 28-35.
43. Cebrowski, Arthur K. Quoted in Samantha L. Quigley. „Transformation Chief Outlines Strategy for New Battlefield.“ *American Forces Press Service,* August 5, 2004. http://www.au.af.mil/au/awc/awcgate/transformation/oft_cebrowski_new_battlefield_strategy.pdf (preuzeto 9. septembra 2015).
44. Center for Cyber and Information Security (CCIS). „Cyber Security Versus Information Security.“ https://ccis.no/cyber-security-versus-information-security/ (preuzeto 22. maja 2014).
45. Center For Strategic & International Studies. Smart Power Initiative, http://csis.org/program/smart-power-initiative.
46. CERT Romania. *Hotărârea nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României şi a Planului de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică*. 2013, 7. http://www.cert-ro.eu/files/doc/StrategiaDeSecuritateCiberneticaARomaniei.pdf (preuzeto 13. januara 2016).
47. Chagnon, Napoleon A. "Life Histories, Blood Revenge, and Warfare in a Tribal Population." *Science* 239, no. 4843 (1988): 985-992.
48. Chairman of the Joint Chiefs of Staff (CJCS). *Memorandum 0363-08, The Definition of Cyberspace.* July 10, 2008.
49. Chandler, Alfred, D., Jr. *Strategy and Structre: Chapters in the History of American Industrial Enterprise*. Cambridge, MA: MIT Press, 1962.
50. *Charter of the United Nations and Statute of the International Court of Justice*, član 7, 36, Poglavlje XIV, članovi 92-96: 21-30. https://treaties.un.org/doc/publication/ctc/uncharter.pdf (preuzeto 22. avgusta 2015).
51. Pellerin, Cheryl „DoD Advances Elements of Joint Information Environment,“ *U.S. Department of Defense Website*, March 24, 2015. http://www.defense.gov/News-Article-View/Article/604340 (preuzeto 22. januara 2016).
52. Chesterman, Simon. *Just war or just peace? Humanitarian Intervention and International Law.* Oxford, UK: Oxford University Press, 2001.
53. Clarke, Richard A. and Robert K. Knake. *Cyber War: The Next Threat to National Security and What to Do About It.* New York, NY: HarperCollins Publishers, 2010.
54. Committee on National Security Systems. *National Information Assurance (IA) Glossary, CNSS Instruction No. 4009*, 26 April 2010.
55. Comparative Constitutions Project. *Chronology of Constitutional Events, Version 1.2*. http://comparativeconstitutionsproject.org/download-data/ (preuzeto 2. januara 2016).
56. Computer History Musem. *Moore's Law*. http://www.computerhistory.org/revolution/digital-logic/12/267 (preuzeto 5. oktobra 2015).

57. Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May be Deemed to be Excessively Injurious or to Have Indiscriminate Effects, Protocol on Blinding Laser Weapons (As Amended on 21 December 2001), 10 October 1980, 1342 UNTS 137.
58. Convention on the Prevention and Punishment of the Crime of Genocide, Dec. 9, 1948, 78 U.N.T.S. 277.
59. Convention on the Prohibition of Military or any Other Hostile Use of Environmental Modification Techniques, December 10, 1976, 31 UST 333, 1108 UNTS 152.
60. Coser, Lewis A. *The Functions of Social Conflict*. Vol. 9. London, UK: Routledge, 1956.
61. Coskun, Vedat, Karem Ok, and Busra Ozdenizci. *Near field communication: From Theory to Practice.* Chicester, UK: John Wiley & Sons Ltd, 2010.
62. Crawford, Neta C. *U.S. Costs of War Through 2014: $4.4 Trillion and Counting, Summary of Costs for the U.S. Wars in Iraq, Afghanistan and Pakistan*, June 25, 2014, http://watson.brown.edu/costsofwar/files/cow/imce/papers/2014/US%20Costs%20of%20Wars%20through%202014.pdf (preuzeto 23. marta 2016).
63. *Critical Infrastructure Identification, Prioritization, and Protection. Homeland Security Presidential Directive/HSPD-7,* 17 December 2003. https://www.dhs.gov/homeland-security-presidential-directive-7 (preuzeto 15. avgusta 2015).
64. *Critical Infrastructure Protection. Presidential Decision Directive/PDD-63,*22 May 1998. http://fas.org/irp/offdocs/pdd/pdd-63.htm (preuzeto 15. avgusta 2015).
65. *Critical Infrastructure Security and Resilience. Presidential Policy Directive/PPD-21*, 12 February 2013. https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil (preuzeto 15. avgusta 2015).
66. Cuba. Submission to the United Nations General Assembly Resolution G.A. Res 58/373, U.N. Doc A/RES/58/373 (September 17, 2003). https://disarmament-library.un.org/UNODA/Library.nsf/c793d171848bac2b85256d7500700384/b69c21ea9dcbb95785256dc10058b4c9/$FILE/sg58.373.pdf (preuzeto 27. novembra 2015).
67. *Cyberspace Operations: Joint Publication 3-12*. Washington, DC: U.S. Joint Chiefs of Staff, 2013. http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf (preuzeto 19. novembra 2015).
68. Czosseck, Christian and Karlis Podins. "A Vulnerability-Based Model of Cyber Weapons and its Implications for Cyber Conflict." *Proceedings of the European Conference on Information Warfare and Security.* Academic Conferences, Limited, 2012: 246.
69. Dawson, Doyne. "The Origins of War: Biological and Anthropological Theories." *History and Theory* 35, no. 1 (February 1996): 1-28.
70. Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in Accordance with the Charter of the United Nations. G.A. Res. 2625, A/RES/2625(XXV) (Oct. 24, 1970). http://www.un-documents.net/a25r2625.htm (preuzeto 13. maja 2015).

71. Defense Advanced Research Projects Agency. „Where the Future Becomes Now.“ http://www.darpa.mil/about-us/darpa-history-and-timeline (preuzeto 18. decembra 2015).
72. Defense Information Systems Agency (DISA). „Enabling The Joint Information Environment (JIE): Shaping the Enterprise for the Conflicts of Tomorrow,“ 5 May 2014. http://www.disa.mil/~/media/Files/DISA/About/JIE101_000.pdf (preuzeto 2. februara 2016).
73. Defense Information Systems Agency (DISA). *Evolving Operations*, January 12, 2015, http://disa.mil/News/Stories/2014/Evolving-Ops (preuzeto 3. Septembar 2015).
74. Definition of Aggression. United Nations General Assembly Resolution 3314 (XXIX). G.A. Res. 3314, U.N. Doc A/RES/3314 (Dec. 14, 1974). https://daccess-ods.un.org/TMP/5804775.3572464.html (preuzeto 13. maja 2015).
75. Delio, Michelle. „Linux: Fewer Bugs than Rivals.“ *Wired*, December 14, 2004. http://archive.wired.com/software/coolapps/news/2004/12/66022 (preuzeto 24. januar 2016).
76. Dempsey, Martin E. “Defending the Nation at Network Speed.“ Brookings Institution, June 27, 2013. http://www.brookings.edu/~/media/events/2013/6/27%20cybersecurity%20dempsey/martin%20e%20dempsey%20prepared%20remarks.pdf (preuzeto 12. Decembra 2016).
77. Denning, Peter J. "Is Computer Science Science?." *Communications of the ACM* 48, no. 4 (2005): 27-31.
78. *Department of Defense Dictionary of Military and Associated Terms: Joint Publication 1-02.* Washington, DC: Joint Chiefs of Staff. 2001. http://www.bits.de/NRANEU/others/jp-doctrine/jp1_02%2801%29.pdf. (preuzeto 22. decembra 2015).
79. *Department of Defense Dictionary of Military and Associated Terms: Joint Publication 1-02.* Washington, DC: Joint Chiefs of Staff, 2001 (as amended through 26 August 2008), 141, http://www.bits.de/NRANEU/others/jp-doctrine/jp1_02%288-08%29.pdf (preuzeto 22. decembra 2015).
80. *Department of Defense Dictionary of Military and Associated Terms: Joint Publication 1-02.* Washington, DC: Joint Chiefs of Staff, 2010 (as amended through 15 February 2013). http://www.bits.de/NRANEU/others/jp-doctrine/jp1_02%282-13%29%5B1%5D.pdf (preuzeto 22. decembra 2015).
81. *Department of Defense Dictionary of Military and Associated Terms: Joint Publication 1-02,* Washington, DC: Joint Chiefs of Staff, 2001 (as amended through 15 January 2015).
82. *Department of Defense Dictionary of Military and Associated Terms,* Joint Publication (JP) 1-02. Washington, DC: Joint Chiefs of Staff, 1994 (as amended through 6 April 1999). http://www.bits.de/NRANEU/others/jp-doctrine/jp1_02(99).pdf (preuzeto 23. decembra 2015).
83. *Department of Defense Dictionary of Military and Associated Terms,* Joint Publication (JP)1-02, Washington, DC: Joint Chiefs of Staff, 2001 (as amended through 14 August 2002). http://www.bits.de/NRANEU/others/jp-doctrine/jp1_02(02).pdf (preuzeto 23. decembra 2015).

84. Department of Homeland Security. *DHS Budget*. http://www.dhs.gov/dhs-budget (preuzeto 18. Decembra 2015).
85. Department of Homeland Security. *Operational and Support Components.* http://www.dhs.gov/components-directorates-and-offices (preuzeto 18. Decembra 2015).
86. Department of the Army Headquarters. *FM 3-0, Operations: Appendix A, Principles of War and Operations* (2011), Washington, DC. https://fas.org/irp/doddir/army/fm3-0.pdf (preuzeto 9. septembra 2015).
87. Devaney, R.L., Peter B. Siegel, and A. John Mallinckrodt. „A First Course in Chaotic Dynamical Systems: Theory and Experiment.“ *Computers in Physics*, 7, no. 4 (1994): 416-417.
88. Dotzel, Guenter. „Oberon-2 and Modula-2 Technical Publication.“ *The ModulaTor*, 10 and 11 (November and December 1992). http://www.modulaware.com/mdlt28.htm (preuzeto 22. marta 2016).
89. Downes, Larry. *The Laws of Disruption: Harnessing the New Forces that Govern Life and Business in the Digital Age*. New York: Basic Books, 2009.
90. Drew, James. „USAF Nominates JASSM Missile to Host New Computer-killing Weapon.“ *Fight Global*, May 14, 2015. https://www.flightglobal.com/news/articles/usaf-nominates-jassm-missile-to-host-new-computer-killing-412348/ (preuzeto 12. novembra 2015).
91. Drezner, Daniel W. „Get Smart; How to Cram for 2012.“ *Foreign Policy*, June 20, 2011.http://www.foreignpolicy.com/articles/2011/06/20/get_smart_how_to_cram_for_2012, (preuzeto 12. avgusta 2015).
92. Dutta, Soumitra, Bruno Lanvin and Sacha Wunsch-Vincent, eds. *The Global Innovation Index 2015: Effective Innovation Policies for Development.* Cornell University, INSEAD, WIPO, 2015. https://www.globalinnovationindex.org/userfiles/file/reportpdf/GII-2015-v5.pdf (preuzeto 2. januara 2016).
93. Duvall, Paul M., Steve Matyas, and Andrew Glover. *Continuous Integration: Improving Software Quality and Reducing Risk*. New York: Pearson Education, 2007.
94. Echevarria, Antulio J., II. „Fourth-Generation War and Other Myths.“ *Strategic Studies Institute* (2005).
95. Eckstein, Zvi and Daniel Tsiddon. "Macroeconomic Consequences of Terror: Theory and the Case of Israel." *Journal of Monetary Economics* 51, no. 5 (July 2004): 971-1002.
96. Einarsson, Bo, ed. *Accuracy and Reliability in Scientific Computing*. Vol. 18. Philadelphia, PA: SIAM, 2005.
97. Eisenhower, Dwight D. *Farewell Address*, Eisenhower Presidential Library, Museum & Boyhood Home. https://www.eisenhower.archives.gov/research/online_documents/farewell_address.html, (preuzeto 15. decembra 2015).
98. Eldar, Yonina Chana. „Quantum Signal Processing.“ PhD diss., Massachusetts Institute of Technology, Cambridge, 2002. https://dspace.mit.edu/bitstream/handle/1721.1/16805/50544999-MIT.pdf?sequence=2 (preuzeto 20. avgusta 2015).

99. Ellefson, Alex. „$14 Million an Hour for 13 Years: War on Terror's Astounding Cost.“ *AlterNet*, December 29, 2014, http://www.alternet.org/world/14-million-hour-war-terror-has-cost-16-trillion (preuzeto 23. mart 2016).
100. *Encyclopaedia Britannica*, http://www.britannica.com/.
101. Epstein, Jack. "Big Surveillance Project For the Amazon Jungle Teeters Over Scandals." *The Christian Science Monitor*, January 25, 1996. http://www.csmonitor.com/1996/0125/25071.html/%28page%29/2 (preuzeto 12. avgusta 2015).
102. European Defence Agency. *Cyber Defence Fact Sheet.* February 10, 2015. https://www.eda.europa.eu/docs/default-source/eda-factsheets/2015-02-10-factsheet_cyber-defence (preuzeto 14. novembra 2015).
103. European Network and Information Security Agency (ENISA). *Shortlisting network and information security standards and good practices, Version 1.0* (2012). https://resilience.enisa.europa.eu/article-13/shortlist-of-networks-and-information-security-standards (preuzeto 4. januara 2016).
104. European Union Agency for Network and Information Secuirty (ENISA). “National Cyber Security Strategies in the World.” https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world (preuzeto 10. Novembra 2015).
105. EuropeanValues.info Association. „Definition of the Most Basic European Values and Their Significance for Our Modern Society“. http://europaeischewerte.info/fileadmin/templates/Documents/ewdef_en.pdf, (preuzeto 29. januara 2016).
106. Evans, Dave. *The Internet of Things: How the Next Evolution of the Internet Is Changing Everything*. Cisco White Paper (April 2011). http://www.iotsworldcongress.com/documents/4643185/0/IoT_IBSG_0411FINAL+Cisco.pdf (preuzeto 10. januara 2016).
107. Evarstine, Brian. “Inside the Air Force's Drone Operations.” *Air Force Times*, June 22, 2015. http://www.airforcetimes.com/story/military/2015/06/22/air-force-drone-operations-creech/28881503/ (preuzeto 4. septembra 2015).
108. Facebook. Internet.org. https://info.internet.org/en/.
109. Falliere, Nicolas, Liam O. Murchu, and Eric Chien. *W32. Stuxnet Dossier, White paper.* Symantec Corp., Security Response 5, 2011.
110. Fanning William J., Jr. "The Origin of the Term "Blitzkrieg": Another View." *The Journal of Military History* 61, no. 2 (1997): 283-302. http://search.proquest.com.nduezproxy.idm.oclc.org/docview/195641425?accountid=12686 (preuzeto 18. oktobra 2015).
111. Federal Information Security Management Act of 2002 (FISMA), Pub. L. No. 107-347, Title III, 116 Stat. 2899, 2002.
112. Ferdinando, Lisa. „Joint Information Environment is 'Operational Imperative'.“ *US Army*, July 9, 2015. http://www.army.mil/article/152064/Joint_information_environment_is__operational_imperative_/ (preuzeto 22. jaunuara 2016).
113. Ferguson, R. Brian. *Yanomami Warfare: A Political History*. Santa Fe, NM: School of American Research Press, 1995.
114. Finland, Ministry of Defence, Secretariat of the Security and Defence Committee. *Finland’s Cyber Security Strategy*, 2013.

http://www.enisa.europa.eu/media/news-items/new-cyber-security-strategies-of-austria-finland-worldwide (preuzeto 9. januara 2016).
115. Firebaugh, Glenn. *Seven Rules for Social Research*. Princeton, NJ: Princeton University Press, 2008.
116. FR Germany, Federal Ministry of the Interior. *Cyber Security Strategy for Germany,* 2011. https://www.bsi.bund.de (preuzeto 6. januara 2016).
117. France, Agence Nationale de la Securite des Systemes d'Information. *Information Systems Defence and Security: France's Strategy*, 2011. http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world (preuzeto 6. januara 2016).
118. Freeman, Charles W., Jr. *Arts of Power: Statecraft and Diplomacy*. Washington, DC: United States Institute of Peace, 1997.
119. Gady, Franz-Stefan and Greg Austin. *Russia, the United States, and Cyber Diplomacy: Opening the Doors.* EastWest Institute, 2010.
120. Gallagher, Ryan. „Operation Socialist: The Inside Story of How British Spies Hacked Belgium's Largest Telco." *The Intercept*, December 13, 2014. https://theintercept.com/2014/12/13/belgacom-hack-gchq-inside-story/ (preuzeto 12. avgusta 2015).
121. Gartner. „Gartner Says 4.9 Billion Connected "Things" Will Be in Use in 2015," press release, Bacelona, Spain, November 11, 2014. http://www.gartner.com/newsroom/id/2905717 (preuzeto 10. januara 2016).
122. Gerasimov, Valerii. "Cennost' Nauki v Predvidenii [The Value of Science in Foresight]." *Voyenno-Promyshlennyy Kuryer*, February 27, 2013. http://www.vpk-news.ru/articles/14632 (accessed November 12, 2015).
123. Gerden, Eugene. „$500 Million for New Russian Cyber Army." *SC Magazine*, November 6, 2014. http://www.scmagazineuk.com/500-million-for-new-russian-cyber-army/article/381720/ (preuzeto 20. februara 2016).
124. Germany Federal Office for Information Security (BSI). „Glossary/Terminology, Bundesmat fur Sicherheit in der Informationstechnik, 2014. https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Glossar/cs_Glossar_A.html;jsessionid=C8733A22C9EABECEC04B7FDDDE34C451.2_cid294 (preuzeto 25. marta 2016).
125. Gharib, Ali. „Pentagon Gives Blackwater New Contract." *North America Inter Press Service*, September 28, 2007. http://ipsnorthamerica.net/news.php?idnews=1078 (preuzeto 22. januara 2016).
126. Ghosh, Anup K., Chuck Howell, and James A. Whittaker. "Building Software Securely from the Ground Up." *IEEE software* 19, no. 1 (2002): 14.
127. Greenwald, Glenn. „Edward Snowden: NSA Whistleblower Answers Reader Questions." The Guardian, June 17, 2013. http://www.theguardian.com/world/2013/jun/17/edward-snowden-nsa-files-whistleblower (preuzeto 12. avgusta 2015).
128. Greenwald, Glenn. *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State.* New York: Henry Holt and Company, 2014.
129. Glenn, Russel W. „Thoughts on "Hybrid" Conflict." *Small Wars Journal.* http://smallwarsjournal.com/blog/journal/docs-temp/188-glenn.pdf (preuzeto 10. oktobra 2015).

130. Global Firepower (GFP). http://www.globalfirepower.com/ (preuzeto 2. januara 2016).
131. Godwin James B. III, Andrey Kulpin, Karl Frederick Rauscher and Valery Yaschenko, eds. *Russia-U.S. Bilateral on Cybersecurity: Critical Terminology Foundations 2.* New York, NY: The EastWest Institute, 2014, 22.
132. Goldberg, David. „What Every Computer Scientist Should Know About Floating-Point Arithmetic.“ *ACM Computing Surveys*, 23, no. 1 (1991): 5-48. http://perso.ens-lyon.fr/jean-michel.muller/goldberg.pdf (preuzeto 20. oktobra 2015).
133. Goldsmith, Jack L. and Eric A. Posner. *The Limits of International Law*. New York, NY: Oxford University Press, 2005.
134. Google. Project Loon. http://www.google.com/loon/.
135. Government Communications Headquarters (GCHQ). „Chancellor's Speech to GCHQ on Cyber Security,“ public announcement, November 17, 2015. https://www.gov.uk/government/speeches/chancellors-speech-to-gchq-on-cyber-security (preuzeto 20. februara 2016).
136. Grant, Charles. „What are European Values?“ *The Guardian*, March 25, 2007. http://www.theguardian.com/commentisfree/2007/mar/25/whyvaluesmatterinawidere (preuzeto 10. oktobra 2015).
137. Greenberg, Andy. „Here’s a Spy Firm’s Price List for Secret Hacker Techniques.“ *Wired*, November 18, 2015. http://www.wired.com/2015/11/heres-a-spy-firms-price-list-for-secret-hacker-techniques/ (preuzeto 23. januara 2016).
138. Greenberg, Andy. „New Dark-web Market is Selling Zero-day Exploits to Hackers.“ *Wired*, April 17, 2015. http://www.wired.com/2015/04/therealdeal-zero-day-exploits/ (preuzeto 18. aprila 2016).
139. Gumplowicz, Ludwig. *Outlines of Sociology.* Translated by Frederick W. Moore. New York, NY: Arno Press, 1975.
140. Gustin, Joseph F. *Cyber Terrorism: A Guide for Facility Managers.* Lilburn, GA: The Fairmont Press, Inc., 2003.
141. Haigh, Thomas. "The Tears of Donald Knuth." *Communications Of The ACM* 58, no. 1 (January 2015): 40-44, http://cacm.acm.org/magazines/2015/1/181633-the-tears-of-donald-knuth/abstract (preuzeto 30. januara 2016).
142. Halman, Loek, Inge Sieben and Marga van Zundert. *Atlas of European Values. Trends and Traditions at the Turn of the Century*. Leiden, Netherlands: Brill, 2011.
143. Hardin, Garrett. “The Tragedy of Commons.” *Science*, 162, no. 3859 (1968):1243-1248. http://www.sciencemag.org/cgi/content/full/162/3859/1243 (preuzeto 5. septembra 2015).
144. Harding, Luke. „How Edward Snowden Went from Loyal NSA Contractor to Whistleblower.“ *The Guardian*, February 1, 2014. http://www.theguardian.com/world/2014/feb/01/edward-snowden-intelligence-leak-nsa-contractor-extract (preuzeto 22. novembra 2015).
145. Harris, Marvin. "Animal Capture and Yanomamo Warfare: Retrospect and New eEidence." *Journal of Anthropological Research* (1984): 183-201.
146. Hathaway, Oona A. et al. “The Law of Cyber-Attack.” *California Law Review* 100, no. 4 (2012): 817-885.
147. Hedges, Chris. *What Every Person Should Know About War.* New York, NY: Free Press, 2003.

148. Hegre, Havard, Ranveig Gissinger, and Nils Petter Gleditsch. "Globalization and Internal Conflict.“ In *Globalization and Conflict,* edited by Gerald Schneider, Katherine Barbieri and Nils Petter Gleditsch, 251-275. Boulder, CO: Rowman and Littlefield, 2003.
149. Hellemans, Alexander. „Two Steps Closer to a Quantum Internet.“ *IEEE Spectrum*, December 30, 2015, http://spectrum.ieee.org/telecom/security/two-steps-closer-to-a-quantum-internet (preuzeto 4. januara 2016).
150. Hempel, Jessi. “Inside Facebook’s Ambitious Plan to Connect the Whole World.” *Wired*, January 19, 2016. http://www.wired.com/2016/01/facebook-zuckerberg-internet-org/ (preuzeto 17. Februara 2016).
151. Hengqing, W., Huang, P., Dyer, J., Archinal, A., Fagan, J., “Countermeasures for GPS signal spoofing” in *Proceedings of the 18th International Technical Meeting of the Satellite Division of The Institute of Navigation* (*ION GNSS 2005*), Long Beach, 2005, 1285-1290.
152. Herr, Trey. "PrEP: A Framework for Malware and Cyber Weapons." Proceedings of the International Conference on Information Warfare and Security 2014: 84-91.
153. Heuser, Beatrice. „Small Wars in the Age of Clausewitz: The Watershed Between Partisan War and People's War.“ *Journal of Strategic Studies* 33, no.1 (2010): 139-162, http://dx.doi.org/10.1080/01402391003603623 (preuzeto 15. februara 2016).
154. Hildreth, Steven A. “Cyberwarfare*.” CRS Report for Congress RL30735*. Congressional Research Service, Library of Congress, Washington, DC (2001). http://www.fas.org/irp/crs/RL30735.pdf.
155. Hill, Brandon. „Lockheed's F-22 Raptor Gets Zapped by International Date Line.“ *Daily Tech*, February 26, 2007. http://www.dailytech.com/Lockheeds+F22+Raptor+Gets+Zapped+by+International+Date+Line/article6225.htm (preuzeto 12. aprila 2015).
156. Hodge, Nathan. „Layoffs at Blackwter Worldwide (Xe).“ *Wired*, February 19, 2009, http://www.wired.com/dangerroom/2009/02/more-trouble-at/#more, (preuzeto 22. januara 2016).
157. Hofstede, Geert, Gert Jan Hofstede, and Michael Minkov. *Cultures and Organizations: Software of the Mind*. Vol. 2. London: McGraw-Hill, 1991.
158. Hofstede, Geert. *Culture's Consequences: International Differences in Work-related Values*. Vol. 5. Thousand Oaks, CA: Sage Publications, 2001.
159. Holthausk, Kai. *Processess and Services: White Box Versus Black Box.* Third Sky. http://www.thirdsky.com/downloads/ProcessesandServicesDifference.pdf (preuzeto 20. decembra 2015).
160. Houghton, David Patrick. *US Foreign Policy and the Iran Hostage Crisis*. Cabridge, UK: Cambridge University Press, 2004.
161. Hruska, Joel „Intel’s Former Chief Architect: Moore’s Law Will Be Dead within a Decade.“ *ExtremeTech,* August 30 2013. http://www.extremetech.com/computing/165331-intels-former-chief-architect-moores-law-will-be-dead-within-a-decade (preuzeto 15. februara 2016).
162. Hufbauer, Gary Clyde, Jeffrey J. Schott, and Kimberly Ann Elliott. *Economic Sanctions Reconsidered: History and Current Policy Vol. 1*. Washington, DC, Institute for International Economics, 1990.

163. Hull, Fredrik and Gin Sivanesar. "Introducing cyber." *Journal of Business Continuity & Emergency Planning* 7, no. 2 (2013): 97-102.
164. Hussain, Asaf, Bill Law, and Tim Haq. *Engagement with Cultures: From Diversity to Interculturalism*. Leicester: University of Leicester, Institute of Lifelong Learning, 2006.
165. Hutchins, Eric M., Michael J. Cloppert, and Rohan M. Amin. "Intelligence-driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains." *Leading Issues in Information Warfare & Security Research* 1 (2011):80.
166. I Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, Aug. 12, 1949, 6 UST 3114, 75 UNTS 31.
167. ICT Data and Statistics Division, Telecommunication Bureau, International Telecommunication Union. *ICT Fact & Figures.* https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf (preuzeto 10. januara 2016).
168. II Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea, Aug. 12, 1949, 6 UST 3217, 75 UNTS 85.
169. III Geneva Convention Relative to the Treatment of Prisoners of War, Aug. 12, 1949, 6 UST 3316, 75 UNTS 135.
170. India. *National Cyber Security Policy*, 2013. http://deity.gov.in/content/national-cyber-security-policy-2013-1 (preuzeto 6. januara 2016).
171. *Information Operations, Joint Publication 3-13*. Washington, DC: U.S. Joint Chiefs of Staff, 2014. http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf (preuzeto 19. novembra 2015).
172. Information Technology Infrastructure Library (ITIL). *ITIL Version 3 Service Strategy.* Norwich, UK: The Stationery Office, 2011. ftp://83.229.216.22/ITIL/ITIL%20Version%203%20%282011%29/01%20-%20ITIL%20V3%202011%20Service%20Strategy%20SS.pdf.
173. Inglehart, Ronald, and Christian Welzel. "Changing Mass Priorities: The Link between Modernization and Democracy." *Perspectives on Politics* Vol. 8, No. 02 (2010): 551-567.
174. Institute of Electrical and Electronics Engineers. *754-2008 - IEEE Standard for Floating-Point Arithmetic.* August 29, 2008. http://ieeexplore.ieee.org/servlet/opac?punumber=4610933 (preuzeto 10. decembra 2015).
175. Intel Corporation. "Over 6 Decades of Continued Transistor Shrinkage, Innovation," press release, May 1, 2011. http://www.intel.com/content/dam/www/public/us/en/documents/backgrounders/standards-22-nanometers-technology-backgrounder.pdf (preuzeto 5. oktobra 2015).
176. International Committee of the Red Cross (ICRC). *How is the Term "Armed Conflict" Defined in International Humanitarian Law?"* March 2008. https://www.icrc.org/eng/assets/files/other/opinion-paper-armed-conflict.pdf (preuzeto 12. maja 2015).
177. International Convention against the Recruitment, Use, Financing and Training of Mercenaries, G.A. Res. 44/34, U.N. Doc A/44/34 (Dec. 4, 1989).

http://www.un.org/documents/ga/res/44/a44r034.htm (preuzeto 22. januara 2016).
178. International Court of Justice (ICJ). *Rules of Court* (1978). Adopted on 14 April 1978 and Entered Into force on 1 July 1978. http://www.icj-cij.org/documents/index.php?p1=4&p2=3&.
179. International Court of Justice (ICJ). *Statute of the International Court of Justice*. http://www.icj-cij.org/documents/?p1=4&p2=2.
180. International Law Association. „Use of Force: Final Report on the Meaning of Armed Conflict.“ In *International Law, The Hague Conference* (2010). http://www.ila-hq.org/en/committees/index.cfm/cid/1022 (preuzeto 12. maja 2015).
181. International Organization for Standardization and International Electrotechnical Commission. *ISO/IEC 13335-1:2004 (en), Information technology — Security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security.* Geneva, Switzerland: ISO/IEC, 2004.
182. International Organization for Standardization and International Electrotechnical Commission. *ISO/IEC 27000:2016(en), Information technology — Security techniques — Information security management systems — Overview and vocabulary.* Geneva, Switzerland: ISO/IEC, 2016.
183. International Organization for Standardization and International Electrotechnical Commission. *ISO/IEC 27032:2012, Information technology — Security techniques — Guidelines for cybersecurity.* Geneva, Switzerland: ISO/IEC, 2012.
184. International Organization for Standardization and International Electrotechnical Commission. *ISO/IEC 9126-1:2001, Software engineering -- Product quality -- Part 1: Quality model.* Geneva, Switzerland: ISO/IEC, 2001.
185. International Organization for Standardization and International Electrotechnical Commission. *ISO/IEC 25010:2011, Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models.* Geneva, Switzerland: ISO, 2011.
186. International Organization for Standardization, *ISO 27005:2011 Information technology -- Security techniques -- Information security risk management* (Geneva, Switzerland: ISO, 2011).
187. International Organization for Standardization and International Electrotechnical Commission. „ISO/IEC Glossary of IT Security Terminology.“ ISO/IEC, 2013. http://www.jtc1sc27.din.de/cmd?level=tpl-bereich&menuid=64540&languageid=en&cmsareaid=64540 (preuzeto 18. novembra 2015).
188. International Organization for Standardization. *ISO 27005:2011 Information technology -- Security techniques -- Information security risk management.* Geneva, Switzerland: ISO, 2011.
189. International Organization for Standardization and International Electrotechnical Commission. *ISO/IEC 7498-1:1994 Information technology -- Open Systems Interconnection -- Basic Reference Model: The Basic Model.* Geneva, Switzerland: ISO, 1994.
190. International Telecommunication Union (ITU). *ITU Terms and Definitions.* http://www.itu.int/net/ITU-

R/index.asp?redirect=true&category=information&rlink=terminology-database&lang=en&adsearch=&SearchTerminology=cyberspace&collection=normative&sector=all&language=all&part=abbreviationterm&kind=anywhere&StartRecord=1&NumberRecords=50 (preuzeto 10. Novembra 2015).
191. International Telecommunication Union. *Global ICT Developments*, 2001-2015. https://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2015/stat_page_all_charts_2015.xls (preuzeto 10.januara 2016).
192. International Telecommunication Union. *ICT Development Index, 2015*, http://www.itu.int/net4/ITU-D/idi/2015/ (preuzeto 2. Januara 2016).
193. International Telecommunication Union. *ICT Facts and Figures 2015*. https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx (preuzeto 10. januara 2016).
194. International Telecommunication Union. *International Telecommunication Convention*. Malaga-Terremolinos, 1973. http://www.itu.int/dms_pub/itu-s/oth/02/01/S020100001F4008PDFE.pdf (preuzeto 10. februara 2016).
195. Internet Engineering Task Force. „Internet Security Glossary Version 2.“ *The IETF Trust*, 2007. http://tools.ietf.org/html/rfc4949 (preuzeto 18. novembra 2015).
196. Internet Hall of Fame, “Donald Davies” http://www.internethalloffame.org/inductees/donald-davies (preuzeto 18. Decembra 2015).
197. Internet World Stats. *Internet Usage Statistics, The Internet Big Picture, World Internet Users and 2015 Population Statistics.* http://www.internetworldstats.com/stats.htm (preuzeto 17. januara 2016).
198. International Organization for Standardization and International Electrotechnical Commission. *ISO/IEC 27032:2012, Information technology — Security techniques — Guidelines for cybersecurity*. Geneva, Switzerland, 2012.
199. Israel, Government of Israel. *Resolution No. 3611: Advancing National Cyberspace Capabilities* 2011.http://www.pmo.gov.il/English/PrimeMinistersOffice/DivisionsAndAuthorities/cyber/Documents/Advancing%20National%20Cyberspace%20Capabilities.pdf (preuzeto 6. januara 2016).
200. International Telecommunication Union. *Definition of Cybersecurity*. http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx (preuzeto 6. januara 2016).
201. IV Geneva Convention Relative to the Protection of Civillian Persons in Time of War, Aug. 12, 1949, Art 2, 6UST 3516, 75 UNTS 287.
202. Jablonsky, David. "US Military Doctrine and the Revolution in Military Affairs." *Parameters* 24, no. 3 (1994): 18.
203. Japan, Government of Japan. *National Security Strategy*, 2013. http://www.cas.go.jp/jp/siryou/ (preuzeto 9. januara 2016).
204. Jensen, Eric Talbot. ”Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense.” *Stanford Journal of International Law*, Vol. 38 (2002).
205. Johnson, Neil F. (2009). "Chapter 1: Two's Company, Three is Complexity." *Simply complexity: A Clear Guide to Complexity Theory.* London, UK: Oneworld Publications, 2009.

http://www.uvm.edu/rsenr/nr385se/readings/complexity.pdf (preuzeto 7. septembra 2015).
206. *Joint Doctrine for Information Operations, Joint Publication 3-13*. Washington, DC: U.S. Joint Chiefs of Staff, 1998. http://www.c4i.org/jp3_13.pdf (preuzeto 19. novembra 2015).
207. *Joint Tactics, Techniques and Procedures for Joint Intelligence Preparation of the Battlespace: Joint Publication 2-01.3.* Washington, DC: Joint Chiefs of Staff, 2000. http://webapp1.dlib.indiana.edu/virtual_disk_library/index.cgi/4240529/FID521/pdfdocs/jel/new_pubs/jp2_01_3.pdf (preuzeto 22. decembra 2015).
208. Joyce, Rob. „USENIX Enigma 2016 - NSA TAO Chief on Disrupting Nation State Hackers.“ *USENIX Enigma Conference.* https://www.youtube.com/watch?v=bDJb8WOJYdA (preuzeto 06. marta 2016).
209. Jung, Ho-Won, Seung-Gweon Kim and Chang-Shin Chung. "Measuring Software Product Quality: A Survey of ISO/IEC 9126." *IEEE Software* 5 (2004): 88-92.
210. Kadtke, James and Linton Wells II. *Policy Challenges of Accelerating Technological Change: Security Policy and Strategy Implications of Parallel Scientific Revolutions* Washington, DC: Center for Technology and National Security Policy, National Defense University, 2003.
211. Kaplan, David M. *Ricoeur's critical theory*. Albany, NY: SUNY Press, 2003, 167.
212. Karp, Jonathan. "Contractors in War Zone Face Legal Front; Private Firms Like Blackwater could be Held Liable for Casualties during Military Tasks." *Wall Street Journal*, March 8, 2007, Eastern edition. http://search.proquest.com.nduezproxy.idm.oclc.org/docview/398964304?accountid=12686 (preuzeto 22. januara 2016);
213. Keck, Zachary. „China's Next Super Weapon Revealed: Satellite Destroyers.“ *The National Interest*, April 15, 2015. http://www.nationalinterest.org/blog/the-buzz/chinas-next-superweapon-revealed-satellite-destroyers-12640 (preuzeto 23. marta 2016).
214. Kende, Istvan. „Twenty-Five Years of Local Wars.“ *Journal of Peace Research*, 8, no. 1 (1971): 5-22. http://www.jstor.org/stable/422559 (preuzeto 15. avgusta 2015).
215. Kissel, Richard, ed. *National Institute of Standards and Technology Glossary of Key Information Security Terms.* U.S. Department of Commerce, 2013. http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf (preuzeto 25. marta 2016).
216. Koh, Harold Hongju. *Remarks at the USCYBERCOM Inter-Agency Legal Conference.* September 18, 2012. http://www.state.gov/s/l/releases/remarks/197924.htm (preuzeto 11. oktobra 2015).
217. Konsbruck, Robert Lee. *Impacts of Information Technology on Society in the New Century* (2002).
218. Koopman, Phil. „Embedded Software Costs $15-$40 per Line of Code.“ http://betterembsw.blogspot.rs/2010/10/embedded-software-costs-15-40-per-line.html (preuzeto 24. marta 2016).

219. Kuehl, Daniel T. "From Cyberspace to Cyberpower: Defining the Problem." *Cyberpower and National Security* (2009): 26-28.
220. Kuenssberg, Laura. "State Multiculturalism has Failed, Says David Cameron." *BBC News*, February 5, 2011, http://www.bbc.com/news/uk-politics-12371994 (preuzeto 23. februara 2016).
221. Kurzweil, Ray. *The Singularity is Near: When Humans Transcend Biology*. New York, NY: Viking, 2005.
222. Kushner, David. "How Kaspersky Lab Tracked Down the Malware that Stymied Iran's Nuclear-fuel Enrichment Program." *IEEE Spectrum*, February 26, 2013, http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet/ (preuzeto 12. Decembra 2015).
223. Kushner, David. „The Real Story of Stuxnet." IEEE Spectrum, Februar 26, 2013. http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet (preuzeto 22. oktobra 2015).
224. Lachow, Irving. "Cyber Terrorism: Menace or Myth?." In *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart H. Starr and Larry Wentz, 437-464. Washington DC: Potomac Books, 2009.
225. Landwehr, Carl E. „Cybersecurity: From Engineering to Science." *The Next Wave*, 19, no.2 (2012), 2-5. https://www.nsa.gov/research/tnw/tnw192/articles/pdfs/TNW_19_2_Web.pdf (preuzeto 3. oktobra 2015).
226. Langner, Ralph. *To Kill a Centrifuge.* Hamburg, DE: The Langer Group, 2013. http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf (preuzeto 23. oktobra 2015).
227. Lardner, Richard. „NSA Overhauls Corporate Structure in Effort to Improve Operations." *Inside the Air Force*, 11, no. 25 (2000). http://cryptome.org/nsa-redo.htm (preuzeto 10. avgusta 2015).
228. Le Lann, Gérard. "An analysis of the Ariane 5 flight 501 failure-a system engineering perspective." in *Engineering of Computer-Based Systems, 1997. Proceedings., International Conference and Workshop*, 339-346, IEEE, 1997, http://www.niwotridge.com/Resources/Ariane5Resources/78890339.pdf (preuzeto 15. decembra 2015).
229. Leavitt, Harold J. „Applied Organization Change in Industry: Structural, Technical, and Human Approaches." In *New Perspectives in Organizational Research*, edited by Cooper S, Harold J. Leavitt and Shelly K., 55-71. Chicester, UK: John Wiley and Sons, 1964.
230. Leavitt, Harold J., and James G. March. *Applied Organizational Change in Industry: Structural, Technological and Humanistic Approaches*. Pittsburgh: Carnegie Institute of Technology, Graduate School of Industrial Administration, 1962.
231. Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 679.
232. Leibnitz Institute for the Social Studies. „EVS Waves – Study Overview." *Gesis*, December 21, 2015. http://www.gesis.org/en/services/data-analysis/survey-data/european-values-study/study-overview/ (preuzeto 22. januara 2016).
233. Leibniz Institute for the Social Sciences. „European Values Study." *Gesis*, January 25, 2016. http://www.gesis.org/en/services/data-analysis/survey-data/european-values-study/ (preuzeto 22. januara 2016).

234. Leiner, Barry M., Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, and Stephen Wolff, „Brief History of the Internet,“ *Internet Society*, http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet (preuzeto 12. januara 2016).
235. Leonie Industries. „Top Secret America.“ *The Washington Post*. http://projects.washingtonpost.com/top-secret-america/companies/leonie-industries/ (preuzeto 20. februara 2016).
236. Leonie. Cyber Operations Planner (closed). *Bullhornreach*. http://www.bullhornreach.com/job/793005_cyber-operations-planner-kabul-afghanistan (preuzeto 20.februara 2016).
237. Lewis, James A. and Katrina Timin, Center for Strategic and International Studies. *Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization.* United Nations Institute for Disarmament Research - UNIDIR, 2011. http://unidir.org/files/publications/pdfs/cybersecurity-and-cyberwarfare-preliminary-assessment-of-national-doctrine-and-organization-380.pdf (preuzeto 13. decembra 2015).
238. Liang, Qiao and Wang Xiangsui. *Unrestricted Warfare.* Beijing: PLA Literature and Arts Publishing House, 1999.
239. Lima, Joao. „Top 10 biggest data centres from around the world.“ *Computer Business Review*, http://www.cbronline.com/news/data-centre/infrastructure/top-10-biggest-data-centres-from-around-the-world-4545356 (preuzeto 30. novembra 2015).
240. Limnéll, Jarno. „The Danger of Mixing Cyberespionage with Cyberwarfare.“ *Wired.* http://www.wired.com/insights/2013/07/the-danger-of-mixing-cyberespionage-with-cyberwarfare/ (preuzeto 25. februara 2016).
241. Lin, Herbert "The Development of Software for Ballistic-missile Defense." *Scientific American*, 253, no. 6 (1985).
242. Lin, Herbert. "Cyber conflict and international humanitarian law." *International Review of the Red Cross* 94, no. 886 (2012): 515-531.
243. Lind, William S. „Understanding Fourth Generation War.“ *Military Review*, (September-October 2004): 12-16.
244. Lind, William S., Keith Nightengale, John F. Schmitt, Joseph W. Sutton, Garry I. Wilson. "The Changing Face of War: Into the Fourth Generation." *Marine Corps Gazzette*, 73, no. 10 (1989): 22-26, https://www.mca-marines.org/files/The%20Changing%20Face%20of%20War%20-%20Into%20the%20Fourth%20Generation.pdf (preuzeto 18. oktobra 2015).
245. Lockheed Martin Corporation. *Joint Strike Fighter Air Vehicle C++ Coding Standards For the System Development and Demonstration Program*, Document Number 2RDU00001 Rev C, December 2005 http://www.stroustrup.com/JSF-AV-rules.pdf.
246. Lockheed Martin, F-35 Lightning II, „How much does the F-35 Cost? Producing, Operating and Supporting a 5th Generation Fighter,“ https://www.f35.com/about/fast-facts/cost (preuzeto 13. januara 2016).
247. Lodewyckx, Peter. „Nauke odbrane: Da li postoje?.“ *Vojno delo* 2011, 78-82.
248. Logie, Christopher. „The Literacy of Tracking: A Comparative Analysis of Tracking within Two Bushman Posthunter Communities.“ Submitted in partial fulfilment of degree requirements for a coursework Master of Arts in Culture,

Communication and Media Studies, University of KwaZulu-Natal, Durban, 2010. http://www.cybertracker.org/downloads/tracking/Logie-2010-Literacy-of-tracking.pdf
249. Lowder, Jeff. „Why the "Risk = Threats x Vulnerabilities x Impact" Formula is Mathematical Nonsense." *BlogInfoSec*, entry posted August 23, 2010. http://www.bloginfosec.com/2010/08/23/why-the-risk-threats-x-vulnerabilities-x-impact-formula-is-mathematical-nonsense/ (preuzeto 28. februara 2016).
250. Lukić, Radomir. „Da li je pravo nauka?" Predavanje, 29. januar 1966. Reči u vremenu – zvučni zapisi predavanja na Kolarcu, DVD – Video, Zadužbina Ilije M. Kolarca, Centar za izdavačku delatnost, Beograd, 2007.
251. MacAskill, Ewen and James Ball. „Portrait of the NSA: No Detail too Small in Quest for Total Surveillance." *The Guardian*, November 2, 2013. http://www.theguardian.com/world/2013/nov/02/nsa-portrait-total-surveillance (preuzeto 12. avgusta 2015).
252. MacAskill, Ewen, Julian Borger, Nick Hopkins, Nick Davies and James Ball. „GCHQ Taps Fibre-optic Cables for Secret Access to World's Communications." *The Guardian*, June 21, 2013. http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa (preuzeto 11. avgusta 2015).
253. Macksey, Kenneth. *Guderian: Creator of the Blitzkrieg.* New York, NY: Stein and Day, 1976.
254. Mahoney, Michael S. "The history of computing in the history of technology." *Annals of the History of Computing* 10, no. 2 (1988): 113-125, http://www.princeton.edu/~hos/mike/articles/hcht.pdf (preuzeto 30. januara 2016).
255. Mandelbrot, Benoit B. "The Fractals and the Geometry of Nature." (1982), http://users.math.yale.edu/~bbm3/web_pdfs/encyclopediaBritannica.pdf .
256. Mansfield, Edwin. *Technological Change:An Introduction to a Vital Area of Modern Economics*. New York: Norton, 1971, 10.
257. Marshall, Tyler. „World Court Rules U.S. Aid to Contras Is Illegal." *Los Angeles Times*, June 28 1986. http://articles.latimes.com/1986-06-28/news/mn-25504_1_contras (preuzeto 08. januara 2015).
258. McAfee (Intel Company). "57% Believe a Cyber Arms Race is Currently Taking Place, Reveals McAfee-Sponsored Cyber Defense Report." http://www.businesswire.com/news/mcafee/20120130005063/en/57-Cyber-Arms-Race-Place-Reveals-McAfee-Sponsored (preuzeto 1. februara 2016).
259. McConnell, Steve. *Code complete.* Upper Saddle River, NJ: Pearson Education, 2004.
260. McGraw, Gary. *Software security: Building Security In.* Vol. 1. Boston, MA: Addison-Wesley Professional, 2006.
261. Mcleod, Laurie and Bill Doolin. „Information Systems Development as Situated Socio-technical Change: A Process Approach." *European Journal of Information Systems* 21, no. 2 (2012): 176-191. http://search.proquest.com.nduezproxy.idm.oclc.org/docview/926222149?accountid=12686 (preuzeto 18. avgusta 2015).
262. Menn, Joseph. "Exclusive: U.S. Tried Stuxnet-style Campaign against North Kora but Failed – Sources." *Reuters*, May 29, 2015,

http://www.reuters.com/article/us-usa-northkorea-stuxnet-idUSKBN0OE2DM20150529 (preuzeto 14. Decembra 2015).
263. Mesthene, Emmanuel G. *Technological Change: Its Impact on Man and Society*. Harvard, MA: Harvard University Press, 1970.
264. *Metadata for Percentage of Individuals Using Internet 2000-2014* (Excel datoteka). https://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2015/Individuals_Internet_2000-2014.xls (preuzeto 10. januara 2016).
265. Metcalfe, Benjamin. "Metcalfe's Law After 40 Years of Ethernet." *Computer* 46, no. 12 (2013): 26-31.
266. Metropolis, Nicholas, Jack Howlett and Gian-Carlo Rota, eds., *A History of Computing in the Twentieth Century: A Collection of Essays.* New York, NY: Academic Press, Inc, 1980.
267. Metz, Cade. "Why Do We Call Them Internet Packets? His Name Was Donald Davies." *Wired,* September 10, 2012. http://www.wired.com/2012/09/donald-davies/ (preuzeto 13. novembra 2015).
268. Meyer, Bertrand. „Those Who Say Code Does not Matter, and Those Who Say Languages Do not Matter." *BLOG@CACM*, entry posted April 15, 2014. http://cacm.acm.org/blogs/blog-cacm/173827-those-who-say-code-does-not-matter/fulltext (preuzeto 22. marta 2016).
269. Microsoft, TechNet. „Microsoft Security Bulletin MS15-010 – Critical," February 10, 2015. https://technet.microsoft.com/library/security/MS15-010, (preuzeto 28. marta 2016).
270. Mik, Eliza "Identification and Attribution." In *SelectedWorks of Eliza Mik.* Singapore Management University, 2007.
271. Military and Paramilitary Activities In and Against Nicaragua (Nicar. v. U.S.), Merits, 1986 I.C.J.Rep. 14, (June 27). http://www.icj-cij.org/docket/files/70/6503.pdf (preuzeto 22. avgusta 2015).
272. Mills, Charles Wright. *Power, Politics, and People: The Collected Essays of C. Wright Mills*. Oxford University Press, USA, 1963.
273. Ministerium für Inneres und Kommunales des Landes Nordrhein-Westfalen (Ministarstvo unutrašnjih poslova i lokalne uprave pokrajine Severne Vestfalije). "Bericht des Ministeriums für Inneres und Kommunales über die Übergriffe am Hauptbahnhof Köln in der Silvesternacht." (Izveštaj Ministarstva unutrašnjih poslova i lokalne uprave o napadima na Centralnoj stanici u Kelnu tokom Novogodišnje noći), 10 Januar 2016. http://www.mik.nrw.de/fileadmin/user_upload/Redakteure/Dokumente/Themen_und_Aufgaben/Schutz_und_Sicherheit/160111ssia/160111berichtmik.pdf (preuzeto 22.februara 2016).
274. Mite, Valentinas. „Estonia: Attacks Seen As First Case of 'Cyberwar'." Radio Free Europe, May 30, 2007. http://www.rferl.org/content/Article/1076805.html (preuzeto 2. aprila. 2016).
275. Mladenović, Dragan i Danko Jovanović. „Open Source UAV in MANET Combat Environment." *5th International Scientific Conference on Defensive Technologies, OTEH 2012*, Belgrade, September 2012.
276. Mladenović, Dragan, Danko Jovanović, Mirjana Drakulić. „Tehnološki, vojni i društveni preduslovi primene sajber ratovanja." *Vojnotehnički glasnik*, 1 (2012), 70-98.

277. Mladenović, Dragan, Danko Jovanović, Mirjana Drakulić. "Definisanje sajber ratovanja." *Vojnotehnički glasnik* 60, no. 2 (2012): 84-117.
278. Mladenović, Dragan. „International Legal Regulation of Cyber Conflict: Problems and a Proposed Solution.“ Capstone paper, Information Resources Management College, National Defense University, 2015.
279. Mladenovic, Dragan. „SAF Organizational Culture and Cyber Defense Development.“ Final paper for the Organizational Culture for Strategic Leaders OCL 15-01 course, Information Resources Management College, NDU, August 2014.
280. Mladenović, Dragan. „Sajber ratovanje: Neslućene mogućnosti novih tehnologija.“ *Magazin Odbrana*, 191 (1. septembar 2013), Specijalni prilog broj 93, http://www.odbrana.mod.gov.rs/specijalni%20prilog/93/Specijalni%20prilog%2093%20-%20Sajber%20ratovanje.pdf (preuzeto 10. decembra 2015).
281. Mladenović, Dragan. *Međunarodni aspekt sajber ratovanja*. Beograd, Srbija: Medija centar Odbrana, 2012.
282. *Mobile-cellular Telephone Subscriptions 2000-2014* (Excel datoteka). https://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2015/Mobile_cellular_2000-2014.xls (preuzeto 10. januara 2016).
283. *Montevideo Convention on the Rights and Duties of States*. Montevideo, December 26, 1933, http://www.oas.org/juridico/english/treaties/a-40.html (preuzeto 12. februara 2016).
284. Moore, Gordon E. "Cramming More Components onto Integrated Circuits." *Electronics*, (April 19, 1965), 114-117.
285. Morgenthau, Hans J. *In Defense of the National Interest: A Critical Examination of American Foreign Policy*. New York, NY: Knopf, 1951.
286. Morgenthau, Hans J. *Politics Among Nations: The Struggle for Power and Peace*, Fifth Edition, Revised. New York, NY: Knopf, 1978. https://www.mtholyoke.edu/acad/intrel/morg6.htm (preuzeto 9. septembra 2015).
287. Mortimer, Edward. „Globalisation ant the Role of United Nations in the 21st Century“ (speech at the meeting organized by the Hellenic Foundation for European & Foreign Policy (ELIAMEP) and the United Nations Information Centre, Athens, Greece, January 19, 2001), http://www.eliamep.gr/old/eliamep/files/op0104.PDF (preuzeto 6. septembra 2015).
288. Moura, Jose M.F. „What Is Signal Processing?“ *IEEE Signal Processing Magazine*, 26, no. 6 (2009). http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5230869 (preuzeto 18. Avgusta 2015).
289. Nakashima, Ellen and Joby Warrick. “Stuxnet was Work of U.S. and Israeli Experts, Officials Say.” *The Washington Post*, June 2, 2012, https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html (preuzeto 14. Decembra 2015).
290. Nakashima, Ellen and Joby Warrick. „For NSA Chief, Terrorist Threat Drives Passion to ‘Collect it All’.“ July 14, 2013, *The Washington Post.*

https://www.washingtonpost.com/world/national-security/for-nsa-chief-terrorist-threat-drives-passion-to-collect-it-all/2013/07/14/3d26ef80-ea49-11e2-a301-ea5a8116d211_story.html (preuzeto 30. novembra 2015).
291. Naor, Ziv. "Why a Small Probability of Terror Generates a Large Macroeconomic Impact." *Defence And Peace Economics* 26, no. 6 (December 2015): 583-599.
292. National Institute of Standards and Technology. *Managing Information Security Risk, Organization, Mission, and Information System View*. Gaithersburg, MD: National Institute of Standards and Technology, 2012.
293. National Security Agency. „NSA Culture, 1980s to the 21st Century-a SID Perspective.“ *Cryptologic Quarterly*, 30, no. 4 (Winter/Spring 2011): 79-85, http://www.nsa.gov/public_info/_files/cryptologic_quarterly/nsa_culture.pdf (preuzeto 11. oktobra 2015).
294. National Security Agency. „Ukusa Agreement Release 1940-1956.“ June 24, 2010. https://www.nsa.gov/public_info/declass/ukusa.shtml (preuzeto 20. maja 2015).
295. *National Security Presidential Directive/NSPD-16,* July 2002. https://fas.org/irp/offdocs/nspd/index.html (preuzeto 15. avgusta 2015).
296. National Security Service. *National Security Agency/Central Security Service Core Values, Clear Vision,* 2010. http://www.nsa.gov/about/_files/CoreValues.pdf (preuzeto 26. februara 2016).
297. *National Strategy to Secure Cyberspace. National Security Presidential Directive /NSPD-38,* 7 July 2004. https://fas.org/irp/offdocs/nspd/index.html (preuzeto 15. avgusta 2015).
298. North Atlantic Treaty Organization (NATO). Wales Summit Declaration [Press release 120, issued on September 5, 2014]. http://www.nato.int/cps/en/natohq/official_texts_112964.htm(preuzeto 22. decembra 2015).
299. NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). “NSA Director: The Ability to Move Information Freely Should Not Be Controlled,“ May 27, 2015, Tallinn, Estonia. https://ccdcoe.org/nsa-director-ability-move-information-freely-should-not-be-controlled.html (preuzeto 22 februara 2016).
300. NATO Cooperative Cyber Defence Centre of Excellence. *Cyber Definitions*. https://ccdcoe.org/cyber-definitions.html; https://data.opentechinstitute.org/dataset/cyber-security-definitions/resource/c6ab94f6-0323-44a3-970f-549df5da0939, (preuzeto 10. Novembra 2015).
301. NATO Cooperative Cyber Defence Centre of Excellence. *Cyber Security Strategy Documents*, https://ccdcoe.org/strategies-policies.html, (preuzeto 12. januara 2015).
302. NATO. „Military Organisation and Structures,“ July 15, 2014. http://www.nato.int/cps/en/natolive/topics_49608.htm (preuzeto 12. decembra 2015).
303. NATO. „NATO Publishes Defence Expenditures Data for 2014 and Estimates for 2015: Financial and Economic Data Relating to NATO Defence,“ Communique PR/CP(2015)093-COR1, press release, Bruxelles, Belgique, NATO Press & Media, 22 June 2015.

http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2015_06/20150622_PR_CP_2015_093-v2.pdf (preuzeto 12. decembra 2015).
304. NATO. „NATO-EU: A Strategic Partnership," September 28, 2015. http://www.nato.int/cps/en/natohq/topics_49217.htm (preuzeto 22. februara 2016).
305. Naur, Peter, and Brian Randell, eds. *Software Engineering: Report of a Conference sponsored by the NATO Science Committee* (Garmisch, Germany, 7-11 Oct. 1968). Brussels: Scientific Affairs Division, NATO, 1969.
306. Nejgel, Ernest. *Struktura nauke: problemi logike naučnog objašnjenja*. Beograd, Srbija: Nolit, 1974.
307. Nelson, Bill, Rodney Choi, Michael Iacobucci, Mark Mitchell, and Greg Gagnon. "Cyberterror Prospects and Implications." 1999, http://calhoun.nps.edu/bitstream/handle/10945/27344/Cyberterror%20Prospects%20and%20Implications.pdf?sequence=1.
308. Netherlands, Ministry of Defence. *The Defence Cyber Strategy*, 2012. http://www.ccdcoe.org/strategies/Defence_Cyber_Strategy_NDL.pdf (preuzeto 12. januara 2016).
309. NetMarketShare. „Desktop Operating System Market Share," March 2016. https://www.netmarketshare.com/operating-system-market-share.aspx?qprid=10&qpcustomd=0, (preuzeto 28. marta 2016).
310. New Zealand, Ministry for Communications and Information Technology. *New Zealand's Cyber Security Strategy,* 2011. http://www.dpmc.govt.nz/sites/all/files/publications/nz-cyber-security-strategy-june-2011_0.pdf (preuzeto 12. januara 2016).
311. Newitz, Annelee. „The Bizarre Evolution of the Word "Cyber"." *io9 Gizmodo*, September 16, 2013. http://io9.gizmodo.com/today-cyber-means-war-but-back-in-the-1990s-it-mean-1325671487 (preuzeto 8. Novembra 2015).
312. Nicolescu, Basarab „Methodology of Transdisciplinarity – Levels of Reality, Logic of the Included Middle and Complexity." *Transdisciplinary Journal of Engineering and Science*, 1, no. 1 (December 2010):19-38, http://www.basarab-nicolescu.fr/Docs_Notice/TJESNo_1_12_2010.pdf (preuzeto 15. februara 2016).
313. Chomsky, Noam. „The Golden Age: A Look at the Original Roots of Artificial Intelligence, Cognitive Science, and Neuroscience." Keynote Panel, *Symposium: „Brains, Minds and Machines.*" MIT - Massachusetts Institute of Technology, delimički transkript preuzet sa http://languagelog.ldc.upenn.edu/myl/PinkerChomskyMIT.html (preuzeto 30. marta 2016).
314. Norvig, Peter. „On Chomsky and the Two Cultures of Statistical Learning." http://norvig.com/chomsky.html (preuzeto 30. marta 2016).
315. NSA Office of Public Affairs. *NSA/CSS Strategy*, 2010. http://www.nsa.gov/about/_files/nsacss_strategy.pdf (preuzeto 11. oktobra 2015).
316. Nye, Joseph S. "Soft Power." *Foreign Policy*, no. 80 (1990): 153–71.
317. Nye, Joseph S. „Combining Hard and Soft Power." *Foreign Affairs*, July/August 2009 Issue, https://www.foreignaffairs.com/articles/2009-07-01/get-smart (preuzeto 5. septembra 2015).
318. Nye, Joseph S. *The future of power.* New York, NY: PublicAffairs, 2011.

319. O'Harrow, Robert Jr. „Blackwater Contracts, Short on Detail.“ *The Washington Post*, December 8, 2007, http://search.proquest.com.nduezproxy.idm.oclc.org/docview/410171424?accountid=12686 (preuzeto 22. januara 2016).
320. One Laptop Per Child, http://one.laptop.org/.
321. Open Technology Institute (OTI). *Cyber Security Definitions*, https://data.opentechinstitute.org/dataset/cyber-security-definitions (preuzeto 23. decembra 2015).
322. Open Technology Institute. *Global Cyber Definitions Data (Updated).* https://data.opentechinstitute.org/dataset/cyber-security-definitions/resource/c6ab94f6-0323-44a3-970f-549df5da0939 (preuzeto 10. Novembra 2015).
323. Osiander, Andreas. "Sovereignty, International Relations, and the Westphalian Myth." *International Organization*, 55, 2001: 251-287.
324. Ottis, Rain and Peeter Lorents. "Cyberspace: Definition and Implications." *Proceedings Of The International Conference On Information Warfare & Security* (January 2010): 267-270.
325. Owens, William A. „The Emerging US System-of-systems.“ *Strategic Forum*, 63 (February 1996).
326. Owens, William, Kenneth Dam, Herbert Lin. *Technology, Policy, Law, and Ethics Regarding U.S: Acquisition and Use of Cyberattack Capabilities.* Washington, DC: The National Academic Press, 2009.
327. *Oxford English Dictionary*. http://www.oed.com/.
328. Oxford University. *A Dictionary of Computing.* New York, NY: Oxford University Press, 2004.
329. Pace, Steve. *America's Next Lethal War Machine.* New York, NY: McGraw-Hill, 1999. http://imagery.vnfawing.com/PDF-Archive/F-22-Raptor.pdf (preuzeto 11. februara 2015).
330. Pawlak, Patryk, ed. *Riding the Digital Wave: The Impact of Cyber Capacity Building on Human Development* (report). Paris: Institute for Security Studies, 2014. http://www.iss.europa.eu/uploads/media/Report_21_Cyber.pdf, 73, (preuzeto 11. februara 2015).
331. Peace Research Institute Oslo (PRIO). *ACLED - Armed Conflict Location and Event Data*. https://www.prio.org/Data/Armed-Conflict/Armed-Conflict-Location-and-Event-Data/ (preuzeto 21. februara 2016).
332. Neumann, Peter G. *Illustrative Risks to the Public in the Use of Computer Systems and Related Technology*. (Menlo Park, CA: SRI International, 2015. http://www.csl.sri.com/users/neumann/illustrative.html#8 (preuzeto 25. januara 2015).
333. Petranović, Branko. *Istorija Jugoslavije 1918-1988: Kraljevina Jugoslavija 1918-1941*. Beograd: Nolit, 1988.
334. Pettersson, Therése and Peter Wallensteen. „Armed Conflicts, 1946-2014.“ *Journal of Peace Research* 52, no. 4, (2015).
335. Philippines. Submission to the United Nations General Assembly Resolution G.A. Res 56/164, U.N. Doc A/RES/56/164 (July 3, 2001). http://www.un.org/documents/ga/docs/56/a56164.pdf.
336. Pierre, Andrew J. and Lucy Edwards Despard. "Guderian: Center of the Blitzkrieg." *Foreign Affairs* 55, no. 1 (October 1976).

337. Poincaré, Henri. *Science and Hypothesis*. New York, NY: Science Press, 1905.
338. Poland, Ministry of Administration and Digitisation, Internal Security Agency. *Cyberspace Protection Policy of the Republic of Poland*, 2013. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/copy_of_PO_NCSS.pdf (preuzeto 12. januara 2016).
339. Policastri, Joan and Stone, Sergio D., 2013. International Humanitarian Law. *American Society of International Law* (ASIL) https://www.asil.org/sites/default/files/ERG_International%20Humanitarian%20Law%20(test).pdf , 20.
340. Pomerantsev, Peter. "How Putin is Reinventing Warfare." *Foreign Policy*, May 5, 2014. http://foreignpolicy.com/2014/05/05/how-putin-is-reinventing-warfare/ (preuzeto 12. novembra 2014).
341. Population Reference Bureau – PBR. *World Population Data Sheet*, 2013. http://www.prb.org/pdf13/2013-population-data-sheet_eng.pdf (preuzeto 15. septembra 2015).
342. Posner, Eric A and Alan O. Sykes. "Fundamentals of International Law" in *Economic Foundations of International Law*. Harvard, MA: Harvard University Press, 2013.
343. Presidency of the Council of Ministers, Government of Italy. *National Strategic Framework for Cyberspace Security,* 2013. https://www.ccdcoe.org/strategies-policies.html (preuzeto 9. januara 2016).
344. Priemer, Roland. *Introductory Signal Processing.* Singapore: World Scientific, 1991.
345. Priest Dana, and William M. Arkin. „Top Secret America." *The Washington Post*, 2010. http://projects.washingtonpost.com/top-secret-america/ (preuzeto 12. januara 2016).
346. Priest, Dana and William M. Arkin. „A Hidden World, Growing Beyond Control." *The Washington Post*, July 19, 2010. http://projects.washingtonpost.com/top-secret-america/articles/a-hidden-world-growing-beyond-control/print/ (preuzeto 20. februara 2016).
347. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, 16 ILM 1391 (1977).
348. Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or other Gases, and of Bacteriological Methods of Warfare, 17 June 1925, 26 U.S.T. 571, 94 L.N.T.S. 65, 14 I.L.M. 49 (1975).
349. Protocol on Non-Detectable Fragments, 1342 U.N.T.S. 168, 19 I.L.M. 1529, entered into force Dec. 2, 1983.
350. Qualys. *The Laws of Vulnerabilities: Six Axioms for Understanding Risk* (2006). https://www.qualys.com/docs/Laws-Report.pdf (preuzeto 8. jula 2015).
351. Raiyn, Jamal. "A Survey of Cyber Attack Detection Strategies." *International Journal of Security and its Application* 8, no. 1 (2014): 247-256.
352. Ramsden, Jeremy J. „An Introduction to Complexity" in *Complexity and Secuirty,* eds. Jeremy J. Ramsden and Paata J. Kervalishvili. Amsterdam, Netherlands: IOS Press, 2008. Proceedings of the NATO Advanced Research Workshop on Complexity and Security, Tbilisi, Georgia, 2007.
353. Rauscher, Karl F. "Protecting Communications Infrastructure." *Bell Labs Technical Journal* 9, no. 2 (2004).

354. *Rečnik srpskohrvatskoga književnog jezika, Drugo fototipsko izdanje*, 1990, knjiga prva A-E. Novi Sad, Zagreb, 1967.
355. Regidi, Anirudh. „Moore's Law: The Legendary Computing Rule is Dying, Thanks to Smartphones." *Firstpost*, February 16, 2016. http://tech.firstpost.com/news-analysis/moores-law-the-legendary-computing-rule-is-dying-thanks-to-smartphones-299363.html (preuzeto 17. februara 2016).
356. Reuters. „NSA Tapped German Chancellery for Decades, WikiLeaks Claims." *The Guardian*, July 8, 2015. http://www.theguardian.com/us-news/2015/jul/08/nsa-tapped-german-chancellery-decades-wikileaks-claims-merkel, (preuzeto 12. avgusta 2015).
357. Rid, Thomas, and Peter McBurney. "Cyber-weapons." *RUSI Journal* 157, no. 1 (2012): 6-13.
358. Riley, Charles. „Booz Alen Hamilton in Spotlight Over Leak." *CNN*, June 10, 2013. http://money.cnn.com/2013/06/10/news/booz-allen-hamilton-leak/index.html, (preuzeto 20. novembra 2015).
359. Roan, Stanley R. „NATO's 'Neutral' European Partners: Valuable Contributors or Free Riders?." *NATO Review Magazine*, 2013. http://www.nato.int/docu/review/2013/partnerships-nato-2013/NATOs-neutral-European-partners/EN/index.htm (preuzeto 22. februara 2016).
360. Robb, John. „How fast, Frequent and FAKE Terrorism Could Sink the EU." *Global Guerrillas Weblog*, March 22, 2016, http://globalguerrillas.typepad.com/globalguerrillas/2016/03/index.html (preuzeto 25. marta 2016).
361. Robinson, Neil, Agnieszka Walczak, Sophie-Charlotte Brune, Alain Esterle and Pablo Rodriguez. *Stocktaking Study of Military Cyber Defence Capabilities in the European Union (milCyberCAP) Unclassified Summary.* RAND Europe. http://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR286/RAND_RR286.pdf (preuzeto 5. januara 2016).
362. Rockart, John F., and Michael S. Scott Morton. "Implications of Changes in Information Technology for Corporate Strategy." *Interfaces* 14 (January-February 1984): 84–95. http://dspace.mit.edu/bitstream/handle/1721.1/2040/swp-1408-09891521-cisr-098.pdf?sequence=1 (preuzeto 18. avgusta 2015).
363. Röhrig, Wolfgang and Rob Smeaton. „Cyber Security and Cyber Defence in the European Union: Oportunities, Synergies and Challenges." *Cyber Security Review*. http://www.cybersecurity-review.com/articles/cyber-security-and-cyber-defence-in-the-european-union (preuzeto 14. novembra 2015).
364. Roland, Alex and Philip Shiman. *Strategic Computing: DARPA and the Quest for Machine Intelligence, 1983-1993.* Cambridge, MA: The MIT Press, 2002.
365. *Rule 62. Improper Use of the Flags or Military Emblems, Insignia or Uniforms of the Adversary* (International Committee of the Red Cross). In *Customary IHL Database*. https://www.icrc.org/customary-ihl/eng/docs/v1_rul_rule62 (preuzeto 8. januara 2016).
366. Rumer, Yu B. "Translation of 'Systematization of Codons in the Genetic Code [III]'by Yu. B. Rumer (1969)." *Philosophical Transactions of the Royal Society A* 374, no. 2063 (2016): 20150448.
367. Russia. Submission to the United Nations General Assembly Resolution G.A. Res. 54/213, U.N. Doc. A/RES/54/213 (August 10, 1999). https://disarmament-

library.un.org/UNODA/Library.nsf/f4c497d5f90e302d85257631005152d2/fae7e8060174f22c8525764e0051ce60/$FILE/A-54-213.pdf, 10.
368. Russia. Submission to the United Nations General Assembly Resolution G.A. Res 55/140, U.N. Doc A/RES/55/140, (July 10, 2000). http://www.un.org/documents/ga/docs/55/a55140.pdf, 3-4.
369. Ryan, Julie J.C.H and Daniel J. Ryan. „Risk Management.“ Course material for the Information Assurance and Critical Infrastructure Protection Course, Information Resources Management College, National Defense University.
370. S.S. "Lotus" (Fr. v. Turk.), 1927 P.C.I.J. (ser. A) No. 10, at 88 (Sept. 7, 1927).
371. Saffo, Paul. “Disrupting Undersea Cables: Cyberspace’s Hidden Vulnerabilities.” *Atlantic Council*, April 24, 2013. http://www.atlanticcouncil.org/blogs/new-atlanticist/disrupting-undersea-cables-cyberspaces-hidden-vulnerability (preuzeto 1. novembra 2015).
372. Sanger, D. E. „Obama Lets N.S.A. Exploit Some Internet Flaws, Officials Say.“ *The New York Times*, April 12, 2014. http://www.nytimes.com/2014/04/13/us/politics/obama-lets-nsa-exploit-some-internet-flaws-officials-say.html?_r=0 (preuzeto 18. aprila 2016).
373. Sanger, David E. „Obama Order Sped Up Wave of Cyberattacks Against Iran.“ *The New York Times*, June 1, 2012. http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r=0 (preuzeto 22. oktobra 2015).
374. Scahill, Jeremy. *Blackwater: The Rise of the World’s Most Powerful Mercenary Army.* London, UK: Serpent’s Tail, 2007.
375. Schelling, Thomas C. "The strategy of conflict." Cambridge, MA: Harvard University Press, 1960.
376. Schindler, John R. “The Coming Age of Special War.” *The XX Committee* (blog), September 20, 2013. http://20committee.com/2013/09/20/the-coming-age-of-special-war/ (preuzeto 15. septembra 2015).
377. Schmid, Gerhard. "On the Existence of a Global System for the Interception of Private and Commercial Communications (ECHELON Interception System), 2001/2098(INI)." *European Parliament: Temporary Committee on the ECHELON Interception System*, July 11, 2001. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A5-2001-0264+0+DOC+XML+V0//EN (preuzeto 12. avgusta 2015).
378. Schmitt, Michael N. "Cyber Operations and the Jus ad Bellum Revisited." *Villanova Law Review* 56 (2011): 576-577.
379. Schmitt, Michael N. „Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework.“ *The Columbia Journal of Transnational Law*, Vol. 37 (1999): 885-937.
380. Schmitt, Michael N., ed. *Tallinn Manual On The International Law Applicable to Cyber Warfare.* Cambridge: Cambridge University Press, 2013. http://issuu.com/nato_ccd_coe/docs/tallinnmanual.
381. Schneider, Fred B. „Blueprint for a science of cybersecurity.“ *The Next Wave*, 19. no. 2 (2012): 47-57.
382. Schwab, Klaus. *The Global Competitiveness Report 2015-2016*, World Economic Forum. http://www3.weforum.org/docs/gcr/2015-

2016/Global_Competitiveness_Report_2015-2016.pdf (preuzeto 2. januara 2016).
383. Scott, Chris. „DISA Industry Day: Times Have Changed.“ *CTOvision.com.* https://ctovision.com/2013/08/disa-industry-day-times-have-changed/ (preuzeto 7. novembra 2015).
384. Seligman, Lara. „F-35 Will Fly Until 2070 — Six Years Longer Than Planned.“ *Defense News,* March 25, 2016. http://www.defensenews.com/story/defense/air-space/2016/03/24/f-35-fly-until-2070-six-years-longer-than-planned/82224282/ (preuzeto 27. marta 2016).
385. Senge, Peter. *The Fifth Discipline: The Art and Science of the Learning Organization.* New York, NY: Currency Doubleday, 1990.
386. Shachtman, Noah. „26 Years After Gibson, Pentagon Defines ‘Cyberspace’.“ *Wired,* May 23, 2008, http://www.wired.com/2008/05/pentagon-define/ (preuzeto 12. decembra 2015).
387. Shamir, Adi. „The Cryptographers’ Panel.” *RSA Conference 2015.* http://www.rsaconference.com/speakers/adi-shamir (preuzeto 29. Februara 2016).
388. Sheridan, Greg. *The Partnership: The Inside Story of the US-Australian Alliance Under Bush and Howard.* Sydney, Australia, University of New South Wales Ltd., 2006.
389. Shirey, Robert W. *Internet Security Glossary,* ver. 2nd. IETF Network Working Group. https://tools.ietf.org/html/rfc4949#page-3 (preuzeto 29. septembra 2015).
390. Shorrock, Tim. „Blackwater: One of the Pentagon’s Top Contractors for Afghanistan Training.“ *The Nation,* March 31, 2015, http://www.thenation.com/article/blackwater-still-top-pentagon-contractor-afghanistan-training/ (preuzeto 22. januara 2016).
391. Singer, Peter W. „The Regulation of New Warfare.“ *The Brookings Institution,* February 2010. http://www.brookings.edu/research/opinions/2010/02/27-defense-regulations-singer#, (preuzeto 27. decembra 2013).
392. Singh, Shailendra, and Sanjay Silakari. “A Survey of Cyber Attack Detection Systems.” *International Journal of Computer Science and Network Security* 9, no. 5 (2009): 1-10.
393. Singularity Institute for Artificial Intelligence. „What is the Singularity?“ September 8, 2011. http://singinst.org/overview/whatisthesingularity/ (preuzeto 24. marta 2016. sa Interent Archive, Wayback Machine https://web.archive.org/web/20110908014050/http://singinst.org:80/overview/whatisthesingularity/).
394. Sommer, Peter S. and Ian Brown. „Reducing Systemic Cybersecurity Risk.“ *OECD/IFP Project on Future Global Shocks.* OECD, 2011. http://www.oecd.org/governance/risk/46889922.pdf (preuzeto 9. februara 2016).
395. South Africa, Department of Defence Republic of South Africa. *South African Defence Review,* (2012), 79, http://www.sadefencereview2012.org/publications/publications.htm
396. Spain. Submission to the United Nations General Assembly Resolution G.A. Res 64/129, U.N. Doc A/RES/64/129/Add.1 (January 28, 2010). http://www.unhcr.org/4b8fd5889.html.
397. Sponsel, Leslie E. "Yanomami: An Arena of Conflict and Aggression in the Amazon." *Aggressive Behavior* 24, no. 2 (1998): 97-122.

398. Springer, Michael. “57 Cities Now Have Free Wi-Fi, but They’re Not Thinking Big Enough.” *Mic*, October 9, 2013. http://mic.com/articles/66891/57-cities-now-have-free-wi-fi-but-they-re-not-thinking-big-enough#.n8ljLl2cL (preuzeto 17. Februara 2016).
399. Sternstein, Aliya „The Military’s Cybersecurity Budget in 4 Charts.“ *Defense One*, March 16, 2015. http://www.defenseone.com/management/2015/03/militarys-cybersecurity-budget-4-charts/107679/ (preuzeto 20. decembra 2015).
400. Stewart, James G. "Towards a Single Definition of Armed Conflict in International Humanitarian Law: A Critique of Internationalized Armed Conflict." *Revue Internationale de la Croix-Rouge/International Review of the Red Cross* 85, no. 850 (2003): 313-350.
401. Stroustrup, Bjarne „C++ Applications.“ http://www.stroustrup.com/applications.html (preuzeto 23. marta 2016).
402. Suh, Steve D., and Iulian Neamtiu. "Studying Software Evolution for Taming Software Complexity." In *21st Australian Software Engineering Conference (ASWEC).* IEEE, 2010.
403. Sullivan, Michael J. *Joint Strike Fighter: Restrucuring Added Resources and Reduced Risk, but Concurrency is Still a Major Concern.* (GAO-12-525T) Washington, DC: U.S. Government Accountability Office, 2012. http://www.gao.gov/assets/590/589454.pdf (preuzeto 19. oktobra 2014).
404. Sundberg, Ralph, Kristine Eck and Joakim Kreutz. "Introducing the UCDP Non-State Conflict Dataset." *Journal of Peace Research*, 49 (2012): 351-362.
405. Surowiecki, James. *The Wisdom of Crowds.* New York, NY: Anchor, 2005.
406. Šušnjić, Đuro. *Ribari ljudskih duša.* Beograd: Čigoja, 2008.
407. Switzerland, Federal Department of Defence, Civil Protection and Sport DDPS. *National Strategy for the Protection of Switzerland Against Cyber Risks*, 2012. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/National_strategy_for_the_protection_of_Switzerland_against_cyber_risksEN.pdf (preuzeto 12. januara 2016).
408. Talbot, David „Why We’re So Vulnerable.“ *MIT Technology Review*, January 25, 2016. https://www.technologyreview.com/s/545621/why-were-so-vulnerable/ (preuzeto 28. januara 2016).
409. Taylor, Adam. „These are America’s 9 Longest Foreign Wars.“ *The Washington Post*, May 29, 2014. https://www.washingtonpost.com/news/worldviews/wp/2014/05/29/these-are-americas-9-longest-foreign-wars/ (preuzeto 12. januara 2016).
410. The Carlyle Group. *Portfolio Company Highlights: Booz Alen Hamilton.* https://www.carlyle.com/our-business/portfolio-of-investments/booz-allen-hamilton-inc (preuzeto 20. novembra 2015).
411. *The EU's Common Security and Defence Policy*. *EUR-Lex.* http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Aai0026 (preuzeto 22. decembra 2015).
412. The Garrett Hardin Society, http://www.garretthardinsociety.org/info/quotes.html (preuzeto 28. avgusta 2015).

413. The Global Innovation Index. *2015 Country Rankings.* https://www.globalinnovationindex.org/content/page/data-analysis/ (preuzeto 21. februara 2016).
414. The ICTY Committee Established to Review the NATO Bombing Campaign Against the Federal Republic of Yugoslavia. *Final Report to the Prosecutor*. Press release, June 13, 2000.
415. The International Peace Research Institute Sweden, Centre for the Study of Civil War. *CSCW Annual Reports.* https://www.prio.org/Programmes/Extensions/Centre-for-the-Study-of-Civil-War/Annual-Reports/?xitem=4&handler=Programme (preuzeto 3. avgusta 2015).
416. *The Iran Hostage Crisis: A Chronology of Daily Developments, Report Prepared for the Committee on Foreign Affairs U.S. House of Representatives,* 97th Congress 1st Session. Washington DC: Foreign Affairs and National Defense Division Congressional Research Service Library of Congress, 1981. https://www.ncjrs.gov/pdffiles1/Digitization/77922NCJRS.pdf.
417. The Reut Institute. *Israel 15 Vision: Principles and Guidelines for Achieving a Socioeconomic Leapfrog, Version B* (2009). http://www.reut-institute.org/data/uploads/Articles%20and%20Reports%20from%20other%20organizations/20090913%20-%20ISRAEL%2015%20Version%20B.pdf (preuzeto 12. septembra 2015).
418. The White House, George Bush. *National Security Presidential Directive/NSPD-54 / Homeland Security Presidential Directive/HSPD-23.* January 8, 2008. https://fas.org/irp/offdocs/nspd/nspd-54.pdf (preuzeto 15. novembra 2015).
419. The White House, Office of the Press Secretary. „Fact Sheet: Cybersecurity National Action Plan," press release, February 09, 2016. https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan (preuzeto 20. februara 2016).
420. Thill, Scott. "March 17, 1948: William Gibson, Father of Cyberspace." *Wired*, March 17, 2009. http://archive.wired.com/science/discoveries/news/2009/03/dayintech_0317 (preuzeto 9. novembra 2015).
421. Shanker, Thom. "Cyberwar Nominee Sees Gaps in Law." *New York Times,* April 14, 2010. http://www.nytimes.com/2010/04/15/world/15military.html (preuzeto 22. februara 2016).
422. Thompson, Mark „The $5 Trillion War on Terror." *Time*, June 29, 2011. http://nation.time.com/2011/06/29/the-5-trillion-war-on-terror/ (preuzeto 23. marta 2016).
423. Toffler Alvin and Heidi Toffler. *War and Anti-war: Survival at the Dawn of 21st Century.* New York, NY: Warner Books, 1995.
424. Treaty Between The United States of America and The Russian Federation on Measures for the Further Reduction and Limitation of Strategic Offensive Arms (New START), U.S. – Rus., April 8, 2010, https://www.whitehouse.gov/blog/2010/04/08/new-start-treaty-and-protocol (preuzeto 22. avgusta 2015).

425. Treaty Between The United States of America and The Union of Soviet Socialist Republics on the Limitation of Strategic Offensive Arms (SALT I), U.S. – USSR, May 26, 1972, T.I.A.S. No. 7503.
426. Treaty Between The United States of America and The Union of Soviet Socialist Republics on the Limitation of Strategic Offensive Arms, Together With Agreed Statements and Common Understandings Regarding the Treaty (SALT II), Hearings Before the Senate Committee on Foreign Relations, 96th Cong., 1sr Sess. Part II, 7), (signed, not ratified), U.S.– USSR, June 18, 1979.
427. Treaty Between The United States of America and The Union of Soviet Socialist Republics on the Reduction and Limitation of Strategic Offensive Arms (START 1), U.S. – USSR, July 21, 1999, http://www.state.gov/www/global/arms/starthtm/start/start1.html (preuzeto 22. avgusta 2015).
428. Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community, signed at Lisbon, 13 December 2007, OJ C 306. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12007L%2FTXT (preuzeto 15. novembra 2015).
429. Treaty of Westphalia, Peace Treaty between the Holy Roman Emperor and the King of France and their respective Allies, 1648. http://avalon.law.yale.edu/17th_century/westphal.asp (preuzeto 2. septembra 2015).
430. Turing, Alan Mathison. "The Chemical Basis of Morphogenesis." *Philosophical Transactions of the Royal Society of London B: Biological Sciences* 237, no. 641 (1952): 37-72.
431. Turse, Nick. „America's Secret Empire of Drone Bases." *The World Can't Wait,* http://www.worldcantwait.net/index.php/features/covert-drone-war/7447-americas-secret-empire-of-drone-bases (preuzeto 3. septembra 2015).
432. Tzu, Sun, General Carl von Clausewitz, Niccolo Machiavelli, and Baron De Jomini. *The Complete Art of War*. New York: Start Publishing LLC, 2012.
433. Tzu, Sun. *The Art of War*. Translated by Lionel Giles. http://classics.mit.edu/Tzu/artwar.html.
434. U.S. Air Force, „F-16 Fighting Falcon," 23 September 2015. http://www.af.mil/AboutUs/FactSheets/Display/tabid/224/Article/104505/f-16-fighting-falcon.aspx (preuzeto 14. marta 2016).
435. U.S. Department of Defense. *Cyber Strategy*, April 2015. http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf (preuzeto 15. decembra 2015)
436. U.S. Department of Defense. *Department of Defense for Operating in Cyberspace*, July 2011. http://www.defense.gov/news/d20110714cyber.pdf (preuzeto 15. decembra 2015).
437. U.S. Office of Management and Budget *Fiscal Year 2016, Budget of the U.S. Government.* https://www.whitehouse.gov/sites/default/files/omb/budget/fy2016/assets/budget.pdf (preuzeto 1. marta 2016).
438. United Kingdom of Great Britain and Northern Ireland Ministry of Defence. *Joint Doctrine Publication 0-01, UK Defence Doctrine*, Fifth Edition, (2014),

Annex 2A, The UK principles of war and the principles of Allied joint and multinational Operations, 50, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/389755/20141208-JDP_0_01_Ed_5_UK_Defence_Doctrine.pdf (preuzeto 11. septembra 2015).

439. United Kingdom of Great Britain and Northern Ireland Ministry of Defence. *AJP-01(D), Allied Joint Publication 01(D), Alied Joint Doctrine*, (2010), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/33694/AJP01D.pdf (preuzeto 11. septembra 2015).
440. United Kingdom. *The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World*. United Kingdom, UK Cabinet Office, 2011. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf (preuzeto 5. januara 2016).
441. United Nations Development Programme. *Human Development Report 2015.* http://report.hdr.undp.org/ (preuzeto 21. februara 2016).
442. United Nations Security Council Resolution 1244, S.C. Res. 1244. U.N. Doc. S/RES/1244 (June 10, 1999). https://documents-dds-ny.un.org/doc/UNDOC/GEN/N99/172/89/PDF/N9917289.pdf?OpenElement (preuzeto 13. februara 2016).
443. United Nations, Department of Economics and Social Affairs *World Urbanization Prospects, 2014 Revision.* http://esa.un.org/unpd/wup/Publications/Files/WUP2014-Report.pdf (preuzeto 15. septembra 2015).
444. United Nations, Department of Economics and Social Affairs. *Population Division, World Population Prospects, the 2015 Revision.* http://esa.un.org/unpd/wpp/Graphs/Probabilistic/POP/TOT/ (preuzeto 12. septembra 2015).
445. United States Department of Defense, Joint Chiefs of Staff. *National Military Strategy for Cyberspace Operations*, ix. http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-023.pdf (preuzeto 14. decembra 2013).
446. United States Department of Homeland Security. *Risk Management Fundamentals,* April 2011. https://www.dhs.gov/xlibrary/assets/rma-risk-management-fundamentals.pdf (preuzeto 28. februara 2016).
447. United States Department of State. *Treaties in Force:, A List of Treaties and Other International Agreeements of the United States in Force on January 1, 2013*. http://www.state.gov/documents/organization/218912.pdf (preuzeto 21. februara 2016).
448. United States Depeartment of Defense Office of General Counsel. *An Assessment of International Legal Issues in Information Operations*, 1999. http://www.au.af.mil/au/awc/awcgate/dod-io-legal/dod-io-legal.pdf (preuzeto 8. jula 2015).
449. *United States Diplomatic and Consular Staff in Tehran,* Judgment, I. C. J. Reports 1980, p. 3.
450. United States General Accounting Office (GAO). B-247094. The Honorable Howard Wolpe Chairman, Subcommittee on Investigations and Oversight Committee on Science, Space, and Technology House of Representatives,

February 4, 1992. http://fas.org/spp/starwars/gao/im92026.htm (preuzeto 26. januara 2015).
451. United States Government Accountability Office (GAO). *F-35 Joint Strike Fighter: Problems Completing Software Testing May Hinder Deliver of Expected Warfighting Capabilities.* (GAO-14-322), Washington, DC: U.S. Government Accountability Office, 2014. http://www.gao.gov/assets/670/661842.pdf (preuzeto 27. marta 2016).
452. United States Government Accountability Office (GAO). *Navy Aircraft Carriers: Cost-Effectiveness of Conventionally and Nuclear-Powered Aircraft Carriers* (GAO/NSIAD-98-1). Washington, DC: U.S. Government Accountability Office, *1998.* http://fas.org/man/gao/nsiad98001/c3.htm (preuzeto 18. januara 2016).
453. United States of America, Department of Homeland Security, National Initiative for Cybersecurity Careers and Studies. "Explore Terms: A Glossary of Common Cybersecurity Terminology." http://niccs.us-cert.gov/glossary.
454. United States of America. *Department of Defense Instruction, 8500.01,* March 14, 2014.
455. United States Securities and Exchange Commission. *Form 10-K, XNYS:BAH Booz Allen Hamilton Holding Corp Annual Report*, 2012. http://quote.morningstar.com/stock-filing/Annual-Report/2012/3/31/t.aspx?t=XNYS:BAH&ft=10-K&d=64ece737bbfff1deaf0c6b79fafe3153, (preuzeto 20. novembra 2015).
456. United States, Department of the Army, Military Operations. *TRADOC Pamphlet 525-7-8, Cyberspace Operations Concept Capability Plan 2016-2028,* February 22, 2010. http://www.fas.org/irp/doddir/army/pam525-7-8.pdf (preuzeto 11. avgusta 2015).
457. Uppsala Universitet, Department of Peace and Conflict Research. *UCDP Datasets*. http://www.pcr.uu.se/research/ucdp/datasets/ i http://www.ucdp.uu.se/ged/ (preuzeto 3. avgusta 2015).
458. Urquhart, Conal. "Project Loon: Google Plans Balloon Network to Extend Internet Reach." *The Guardian,* 15 June 2013. http://www.theguardian.com/technology/2013/jun/15/project-loon-google-balloon-internet (preuzeto 22. oktobra 2015).
459. US DoD Joint Chiefs of Staff. *Joint Information Environment*, White Paper, January 22, 2013. http://www.jcs.mil/Portals/36/Documents/Publications/environmentalwhitepaper.pdf.
460. Valentino-Devries, Jennifer and Danny Yadron. „Cataloging the World's Cyberforces." *The Wall Street Journal*," October 11, 2015. http://www.wsj.com/articles/cataloging-the-worlds-cyberforces-1444610710 (preuzeto 22. decembra 2015).
461. Van Creveld, Martin. *Technology and War: From 2000 B.C. to the Present*, A Revised and Expanded Edition. New York, NY: The Free Press, 1991.
462. Van Creveld, Martin. *The Rise and Decline of the State.* Cambidge, UK: Cambridge University Press, 1999.
463. Van Creveld, Martin. *The Transformation of War.* New York, NY: The Free Press, 1991.

464. Veracode. „State of Software Security Report Supplement to Vol 6, Fall 2015: Application Development Landscape,“ 2015.
465. Vienna Convention on the Law of Treaties, May 23, 1969. 1155 U.N.T.S. 331, 8 I.L.M. 679.
466. Vinge, Vernor. „What is Singularity?“ *Department of Mathematical Sciences, San Diego State University*, 1993. http://mindstalk.net/vinge/vinge-sing.html (preuzeto 23. marta 2016).
467. Virillio, Paul. *Information Bomb.* London, UK: Sage, 2000.
468. Virillio, Paul. *Speed and Politics.* New York, NY: Semiotext(e), 1977 [2006].
469. Von Clausewitz, Carl. *On War*. Translated by J.J. Graham. http://www.gutenberg.org/files/1946/1946-h/1946-h.htm#link2HCH0001.
470. Von Solms, Rossouw and Johan van Niekerk. "From Information Security to Cyber Security." *Computers and Security* 38, (October 2013): 97-102.
471. Vujaklija, Milan. *Leksikon stranih reči i izraza*, treće izdanje. Beograd, Prosveta, 1980.
472. Wang, Yu. „A New CVE-2015-0057 Exploit Technology,“ September 2015. https://www.exploit-db.com/docs/39660.pdf (preuzeto 18. novembra 2015).
473. Warden, John A. III. „The Enemy as a System.“ *Airpower Journal* (Spring 1995), http://www.airpower.maxwell.af.mil/airchronicles/apj/apj95/spr95_files/warden.htm (preuzeto 5. septembra 2015).
474. Warden, John A., III. „The Enemy as a System.“ *Airpower Journal* (Spring 1995), http://www.airpower.maxwell.af.mil/airchronicles/apj/apj95/spr95_files/warden.htm (preuzeto 16. avgusta 2015).
475. Warner, Jon S. and Roger G. Johnston. „GPS Spoofing Countermeasures.“ *Homeland Security Journal* (December 12, 2003).
476. Warrick, Joby. "CIA Hired Blackwater for Kill Program, Sources Say." *Los Angeles Times,* August 20, 2009, http://search.proquest.com.nduezproxy.idm.oclc.org/docview/422237061?accountid=12686 (preuzeto 22. januara 2016);
477. Watson Institute, International & Public Affairs, Brown University, *Cost of War,* http://watson.brown.edu/costsofwar/ (preuzeto 23. marta 2016);
478. Weaver, Matthew. „Angela Merkel: German Multiculturalism has 'Utterly Failed.“ *The Guardian*, October 17, 2010. http://www.theguardian.com/world/2010/oct/17/angela-merkel-german-multiculturalism-failed (preuzeto 23. februara 2016).
479. Webster, Frank. *Theories of the Information Society.* Abingdon, UK: Routledge, 2006. https://cryptome.org/2013/01/aaron-swartz/Information-Society-Theories.pdf.
480. White House. *Administration Strategy on Mitigating the Theft of U.S. Trade Secrets,* 20 February 2013. https://www.whitehouse.gov/sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf (preuzeto 15. avgusta 2015).
481. White House. *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, May 8, 2009. https://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf (preuzeto 2. septembra 2015).

482. White House. *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, May 16, 2011. https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (preuzeto 2. septembra 2015).
483. WhiteHat Security. „2014 Website Security Statistics Report.“ http://info.whitehatsec.com/rs/whitehatsecurity/images/statsreport2014-20140410.pdf (preuzeto 22. marta 2016).
484. Whitlock, Craig. “Remote U.S. Base at Core of Secret Operations." *The Washington Post*, October 25, 2012. https://www.washingtonpost.com/world/national-security/remote-us-base-at-core-of-secret-operations/2012/10/25/a26a9392-197a-11e2-bd10-5ff056538b7c_story.html (preuzeto 4. septembra 2015).
485. Wilde, Oscar, Jules Barbey d'Aurevilly, and Lady Wilde. *Epigrams: Phrases and Philosophies for the Use of the Young*, Vol. 10. London, New York: AR Keller & Company, Incorporated, 1907.
486. Williams, Michael R. *A history of Computing Technology*. Wiley-IEEE Computer Society Press, 1997.
487. Yavo, Udi. „CVE-2015-0057: The 1-Bit that Eill Bring Windows Down.“ *Ensilo Blog*, entry posted February 15, 2015. http://blog.ensilo.com/one-bit-rule-compromising-windows-single-bit (preuzeto 28. marta 2016).
488. Zegart, Amy B. "September 11 and the Adaptation Failure of US Intelligence Agencies." *International Security* 29, no. 4 (2005): 78-111.
489. Zetter, Kim. „Hacker Lexicon: What is a Zero Day?“ *Wired*, November 11, 2014. http://www.wired.com/2014/11/what-is-a-zero-day/ (preuzeto 12. aprila 2016).
490. Zetter, Kim. „Obama: NSA Must Reveal Bugs Like Heartbleed, Unless they Help the NSA.“ *Wired*, April 15, 2014. http://www.wired.com/2014/04/obama-zero-day/ (preuzeto 18. aprila 2016).
491. Zetter, Kim. “An Unprecedented Look at Stuxnet, the World’s First Digital Weapon.” *Wired*, November 3, 2014, http://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/ (preuzeto 12. Decembra 2015).
492. Zhaohui, Dong, ed. „China Upgrades Missile Force, Adds Space and Cyber War Forces.“ *China Military News*, January 1, 2016, http://english.chinamil.com.cn/news-channels/china-military-news/2016-01/01/content_6840089.htm (preuzeto 20. februara 2016).
493. Ziolkowski, Katharina. "Ius ad bellum in Cyberspace – Some Thoughts on the "Schmitt–Criteria*”* for Use of Force.” In *4th International Conference on Cyber Conflict,* edited by Christian Czosseck, Rain Ottis and Katharina Ziolkowski. Tallinn, Estonia: NATO CCD COE Publications, 2012.
494. Zucchino, David. „Drone Pilots Have a Front-row Seat on War, from Half a World Away.“ *Los Angeles Times*, February 21, 2010, http://articles.latimes.com/2010/feb/21/world/la-fg-drone-crews21-2010feb21 (preuzeto 3. septembra 2015).
495. Герасимов, Валерий. „Ценность Науки в Педвидении.“ *Военно-Промишлений Куриер*, 8 (476), 27 февраля 2013. http://www.vpk-news.ru/articles/14632 (preuzeto 23. februara 2016).

496. Министерство обороны Российской Федерации (Минобороны России). *Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве* (2011). http://ens.mil.ru/science/publications/more.htm?id=10845074@cmsArticle (preuzeto 18. marta 2015).
497. Соглашение между правительствами государств—членов шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности. Екатеринбург, 16 июня 2009 года, (вступило в силу с 5 января 2012 года), 81-е пленарное заседание 2 декабря 2008. https://ccdcoe.org/sites/default/files/documents/sco-090616-iisagreementrussian.pdf (preuzeto 26.marta 2016).
498. Совет Федерации, Федералыного Собрания Российской Федерации. *Концепция стратегии кибербезопасности Российской Федерации – Проект*, 10 января 2014. http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf (preuzeto 5. januara 2016).
499. "Echelon: Big Brother without a Cause." *BBC News*, July 6, 2000. http://news.bbc.co.uk/2/hi/europe/820758.stm (preuzeto 12. avgusta 2015).
500. "The Law That's Not a Law." *IEEE Spectrum* 52, no. 4 (April 2015): 38-57.
501. "Russian Military Unveils Revolutionary Electronic Warfare System." *Sputnik News,* March 4, 2015. http://sputniknews.com/military/20150304/1019042643.html (preuzeto 5. novembra 2015).
502. "Selecting Security Monitoring Approaches by Using the Attack Chain Model." *Gartner*, https://www.gartner.com/doc/2816617?ref=clientFriendlyURL (preuzeto 18. marta 2016).
503. "Strategic Culture: The Impact of Technology on the Military", *7th International Security Forum (ISF),* Panel chaired by Stephanie Neuman, speakers Stephen Biddle, Jack Treddenick, Kenneth W. Estes, Center for Security Studies (CSS), (Zurich, Switzerland: April 2007), http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?id=30882.
504. „42 Years for Snowden Docs Release, Free All Now." *Cryptome.* https://cryptome.org/2013/11/snowden-tally.htm (preuzeto 13. decembra 2015).
505. „Belgacom Attack: Britain's GCHQ Hacked Belgian Telecoms Firm." *Spiegel Online International,* September 20, 2013. http://www.spiegel.de/international/europe/british-spy-agency-gchq-hacked-belgian-telecoms-firm-a-923406.html (preuzeto 12. avgusta 2015).
506. „Blog: Leonie Awarded Afghanistan Information Support Contract." *Signal*, May 15, 2014. http://www.afcea.org/content/?q=leonie-awarded-afghanistan-information-support-contract (preuzeto 20. februra 2016).
507. „Bright Lights, Big Cities." *The Economist*, February 4, 2015, http://www.economist.com/node/21642053 (preuzeto 15. septembra 2015).
508. „Checkpoints, Physical Obstructions, and Forbidden Roads." *B'Tselem*, January 16, 2011, updated May 20, 2015, http://www.btselem.org/freedom_of_movement/checkpoints_and_forbidden_roads (preuzeto 23. februara 2016).
509. „China Military Seeks to Bring Cyber Warfare Units Under One Roof." *Bloomberg*, October 23, 2015. http://www.bloomberg.com/news/articles/2015-

10-22/china-military-chiefs-seek-to-unify-cyber-warfare-operations (preuzeto 20. februara 2016).
510. „Cyberpunk as a Science Fiction Genre.“ *Information Database, The Cyberpunk Project*, stranica poslednji put modifikovana 12. jula 2004. http://project.cyberpunk.ru/idb/scifi.html (preuzeto 8. novembra 2015).
511. „F-22 Squadron Shot Down by the International Date Line.“ *Defense Industry Daily*, March 1, 2007. http://www.defenseindustrydaily.com/f22-squadron-shot-down-by-the-international-date-line-03087/ (preuzeto 12. aprila 2015).
512. „France to Invest 1 Billion Euros to Update Cyber Defences.“ *Reuters*, February 7, 2014, http://www.reuters.com/article/france-cyberdefence-idUSL5N0LC21G20140207 (preuzeto 20. februara 2016).
513. „GCHQ Broke the Law by Spying on UK Citizens.“ Channel 4, February, 6, 2015. http://www.channel4.com/news/gchq-nsa-broke-law-surveillance-prism-snowdown (preuzeto 12. avgusta 2015).
514. „Gen. Dempsey's Remarks and Q&A on Cyber Security at the Brookings Institute.“ *Joint Chiefs of Staff*, July 27, 2013. http://www.jcs.mil/Media/Speeches/tabid/3890/Article/571864/gen-dempseys-remarks-and-qa-on-cyber-security-at-the-brookings-institute.aspx (preuzeto 14. januara 2016).
515. „Get the Data: Drone Wars.“ *The Bureau of Investigative Journalism*, https://www.thebureauinvestigates.com/category/projects/drones/drones-graphs/ (preuzeto 3. septembar 2015).
516. „Growing Number of EU States Say They Prefer Non-Muslim Refugees.“ *Times of Israel*, September 8, 2015, http://www.timesofisrael.com/eu-states-increasingly-say-they-prefer-non-muslim-refugees/ (preuzeto 23. februara 2016).
517. „Is India’s $3.60 Smartphone Too Good to Be True?“ *BBC News*, 18 February 2016. http://www.bbc.com/news/world-asia-india-35601544 (preuzeto 22. februara 2016).
518. „Jam. Bomb. Hack? New U.S. Cyber Capabilities and the Suppression of Enemy Air Defenses.“ *Georgetown Security Studies Review*, April 07, 2014. http://georgetownsecuritystudiesreview.org/2014/04/07/jam-bomb-hack-new-u-s-cyber-capabilities-and-the-suppression-of-enemy-air-defenses/ (preuzeto 23. marta 2015).
519. „Migrants Crisis: Slovakia 'Will Only Accept Christians'.“ *BBC News*, August 19, 2015, http://www.bbc.com/news/world-europe-33986738 (preuzeto 23. februara 2016).
520. „Prosecutor: Most Cologne New Year's Suspects are Refugees." *Associated Press*, February 15, 2016, http://news.yahoo.com/cologne-prosecutor-majority-suspects-asylum-seekers-135156726.html (preuzeto 23. februara 2016).
521. „Rulling Illustrates World Court’s Lack of Real Jurisdiction.“ *Times Daily*, May 13, 1984, 5D. https://news.google.com/newspapers?nid=1842&dat=19840513&id=e5UpAAAAIBAJ&sjid=tccEAAAAIBAJ&pg=2188,2978824&hl=en (preuzeto 08. januara 2015).
522. „Snowden Downloaded NSA Secrets While Working for Dell, Sources Say.“ *Reuters*, August 15, 2013. http://www.reuters.com/article/usa-security-snowden-dell-idUSL2N0GF11220130815, (preuzeto 22. novembra 2015).

523. „The Advantage of ADA 95.“ *AdaIC.* http://archive.adaic.com/intro/ada-vs-c/ada-vs-c.html (preuzeto 22. marta 2016).
524. „US ‘Spied on French Presidents’ – Wikileaks.“ *BBC News*, June 24, 2015. http://www.bbc.com/news/33248484 (preuzeto 12. avgusta 2015).
525. „US military and intelligence computer networks,“ *Electrospaces.net*, March 11, 2015, http://electrospaces.blogspot.rs/2015/03/us-military-and-intelligence-computer.html, (preuzeto 22. decembra 2015).
526. „War in the Fifth Domain.“ *The Economist*, July 1, 2010. http://www.economist.com/node/16478792 (preuzeto 12. oktobra 2015).

BIOGRAFIJA AUTORA

Dragan Mladenović je rođen 13.05.1972. godine u Doboju. Osnovnu školu i Vojnu gimnaziju završio je u Beogradu sa odličnim uspehom. Zvanje diplomiranog inženjera mašinstva je stekao 1995. godine na Vojnotehničkoj akademiji u Beogradu. Zvanje magistra tehničkih nauka - područje organizacionih nauka za elektronsko poslovanje je stekao na Fakultetu organizacionih nauka u Beogradu 2011. godine odbranom magistarske teze *Međunarodni aspekt cyber ratovanja*, koja od strane Privredne komore Beograda proglašena za najbolju magistarsku tezu u 2011. godini. Zvanje mastera nauka u oblasti sajber bezbednosti je stekao 2016. godine na Nacionalnom univerzitetu odbrane u Vašingtonu, SAD, kao istaknuti student i prvi strani student master studija na Koledžu za upravljanje informacionim resursima Ministarstva odbrane SAD.

Od 1995. godine do danas je zaposlen u Vojsci Srbije kao profesionalni oficir. Pripadnik je Uprave za telekomunikacije i informatiku (J-6) Generalštaba Vojske Srbije, u činu potpukovnika. U toku profesionalne karijere je obavljao više dužnosti u oblasti tehničke službe i logistike u Gardi Vojske Srbije. U toku profesionalne službe je odlično ocenjivan i više puta je nagrađivan i pohvaljivan za izuzetne profesionalne i akademske rezultate. Odlikovan je ordenom za zasluge u oblastima odbrane i bezbednosti trećeg stepena.

Kao student poslediplomskih studija na Fakultetu organizacionih nauka u Beogradu i na Nacionalnom univerzitetu odbrane u Vašingtonu, i kao samostalni istraživač, duži niz godina se bavi istraživanjem sukoba i ratovanja u sajber prostoru, informacione bezbednosti, međunarodnog prava oružanih sukoba i informacionih tehnologija. Učestovovao je kao predavač na više naučnih i stručnih skupova, a 2015. godine je bio govornik na javnom slušanju u Narodnoj skupštini Republike Srbije na temu „Sajber bezbednost u Republici Srbiji“. Objavio je više naučnih i stručnih radova o području sajber sukoba, ratovanja, informacione bezbednosti i informacionih tehnologija, kao i knjigu pod nazivom *Međunarodni aspekt sajber ratovanja*, 2013. godine, u izdanju Medija centra Odbrana.

Poseduje napredno znanje engleskog jezika, a pasivno ruskog.

Oženjen je, ima sina i živi u Beogradu.

Прилог 1.

Изјава о ауторству

Име и презиме аутора Драган Младеновић

Број индекса 90/2004

Изјављујем

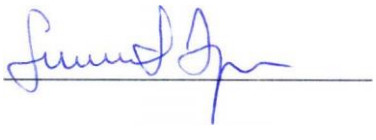
да је докторска дисертација под насловом

Мултидисциплинарни аспекти сајбер ратовања

- резултат сопственог истраживачког рада;
- да дисертација у целини ни у деловима није била предложена за стицање друге дипломе према студијским програмима других високошколских установа;
- да су резултати коректно наведени и
- да нисам кршио/ла ауторска права и користио/ла интелектуалну својину других лица.

Потпис аутора

У Београду, 13. јула 2016. године



Прилог 2.

Изјава о истоветности штампане и електронске верзије докторског рада

Име и презиме аутора Драган Младеновић

Број индекса 90/2004

Студијски програм

Наслов рада Мултидисциплинарни аспекти сајбер ратовања

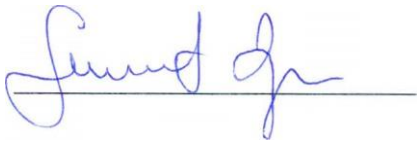
Ментор проф. др Мирјана Дракулић

Изјављујем да је штампана верзија мог докторског рада истоветна електронској верзији коју сам предао/ла ради похрањења у **Дигиталном репозиторијуму Универзитета у Београду.**

Дозвољавам да се објаве моји лични подаци везани за добијање академског назива доктора наука, као што су име и презиме, година и место рођења и датум одбране рада.

Ови лични подаци могу се објавити на мрежним страницама дигиталне библиотеке, у електронском каталогу и у публикацијама Универзитета у Београду.

Потпис аутора



У Београду, 13. јула 2016. године

Прилог 3.

Изјава о коришћењу

Овлашћујем Универзитетску библиотеку „Светозар Марковић” да у Дигитални репозиторијум Универзитета у Београду унесе моју докторску дисертацију под насловом:

Мултидисциплинарни аспекти сајбер ратовања

која је моје ауторско дело.

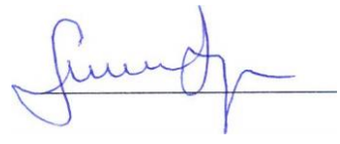
Дисертацију са свим прилозима предао/ла сам у електронском формату погодном за трајно архивирање.

Моју докторску дисертацију похрањену у Дигиталном репозиторијуму Универзитета у Београду и доступну у отвореном приступу могу да користе сви који поштују одредбе садржане у одабраном типу лиценце Креативне заједнице (Creative Commons) за коју сам се одлучио/ла.

1. уторство (CC BY)
2. Ауторство — некомерцијално (CC BY-NC)
3. Ауторство — некомерцијално — без прерада (CC BY-NC-ND)
4. Ауторство — некомерцијално — делити под истим условима (CC BY-NC-SA)
5. Ауторство — без прерада (CC BY-ND)
6. Ауторство — делити под истим условима (CC BY-SA)

(Молимо да заокружите само једну од шест понуђених лиценци. Кратак опис лиценци је саставни део ове изјаве).

Потпис аутора



У Београду, 13. јула 2016. године