УНИВЕРЗИТЕТ У БЕОГРАДУ

ФАКУЛТЕТ БЕЗБЕДНОСТИ

КАТЕДРА СТУДИЈА БЕЗБЕДНОСТИ

АНАЛИЗА ДРУШТВЕНИХ МРЕЖА И ПОДИЗАЊЕ СВЕСТИ МЛАДИХ О САЈБЕР БЕЗБЕДНОСТИ

– ДИПЛОМСКИ РАД –

Ментор:
Ана Ковачевић
Ван. Проф. др.

Студент:
Мина Петровић
262/17

Београд, 2022

САДРЖАЈ

1. Увод

Поседовање стабилне интернет конекције више није упитно. Међусобно повезивање никада није било толико приступачно свим друштвеним слојевима. Овакав феномен довео је до општег побољшања свакодневног живота, али и увео нове претње на које раније нису постојала. Баш ово повезивање примарно се врши преко друштвених мрежа. Оне, као бесплатан онлајн сервис, омогућавају људима да се групишу и пронађу заједнички језик и начин изражавња који њима највише одговара. У последње три деценије интересовање јавности и научно стручних заједница за друштвене мреже је порасло и оне су постале предмет свакодневне расправе. Анализа друштвеног умрежавање је *интердисциплинарна* област и обухвата истраживања у различитим областима као што су социологија, антропологија, психологија, економија, рачунарство, менаџмент, маркетинг, биологија, организационе науке и медицина. Велика интересовања доводе и до великих проблема. Данас често можемо да налетимо на различите онлајн претње, биле оне у социјалном или материјалном смислу. Постојање свести да проблем постоји је први корак ка дијагностиковању и суочавању са проблемом. Уколико не постоји перцепција да проблем постоји, неће постојати ни методи заштите од истих. Овај рад се фокусира на процес анализе друштвених мрежа. Друштвена мрежа је друштвена структура која је састављена од људи, компанија, предузећа који су повезани различитим односима или интеракцијама, који се у контексту социјалне анализе мрежа називају **чвор и ивица**. Да би извршили анализу користимо се алатима за визуелизацију и анализу. Два алата која ћу ја користити су Гефи (енг. Gephi) и Нетлитик (енг. Netlytic). Користећи приложене алате желим да на визуелан начин користећи се методана анализе мрежа прикажем да ли се у заједницама младих води разговор о сајбер безбедности, ко су актери који га покрећу, и да социјалном анализом прикажем колика је свест младих о актуелним сајбер проблемима.

2. Интернет-основни појмови

Како бисмо лакше успели да разумемо негативне и позитивне стране друштвених мрежа у данашњем друштву потребно је да се пре свега осврнемо на настанак и пролиферацију истих. Двадесет и први век се сматра веком информација и самим тим и нове ере информационог друштва. Лака повезаност и остваривање контакта једним кликом омогућио нам је Интернет.

Интернет је системска архитектура која је револуционирала комуникације и методе трговине дозвољавајући различитим рачунарским мрежама широм света да се међусобно повежу. Понекад се назива „мрежом мрежа". Интернет се појавио у Сједињеним Државама 1970-их, али није постао видљив широј јавности све до раних 1990-их. Процењује се да ће до краја 2022. године приближно 4,5 милијарди људи, или више од половине светске популације, имати приступ интернету. (Dennis, 2022).

Даљим развијањем долазимо до модерних друштвених мрежа које су нама познате и потпадају под кишобран WEB-а 2.0 док се ми данас налазимо на прагу WEB-а 3.0. Када бисмо поредили **WEB-1.0, WEB-2.0 и WEB-а 3.0.** најлакше би било искористити аналогију еволуције телевизора (Team, 2022):

- **WEB-1.0-** Представља доба првобитне појаве телевизора, црно беле боје који приказују огроман потенцијал који носи будућност. Повезују мали број људи и сматра се да је потребна велика вештина да бисмо га користили.

- **WEB-2.0**- Осликава нагли скок у еволуцији технологије, ЛЦД телевизори, 3Д пројекције и слика која изгледа као да можете у њу закорачити.

- **WEB-3.0**- Најлакше је описати као садашњост и будућност у једном, искуство унутар метауниверзума. Стварност у виртуелној реалности и танка граница између мета и стварног света. Промена имена Фејсбука у Мета 28. октобра 2021. могла би се показати као рани знак да прелазак на Веб 3.0 узима маха (Meta,2021).

Са сигурношћу можемо закључити да је интернет саставни део наших живота, а друштвене мреже примаран израз комуникације. Цена изражавања је приступачнаа могућност широка. Јаз између људи је смањен и свака особа добија осећај припадности одређеним подгрупама и тиме сазнаје више о колективу и себи.

Битна ствар за поменути је ИОТ (енг. Internet of Things). Термин Интернет ствари се генерално односи на сценарије у којима се мрежно повезивање и рачунарске способности проширују на објекте, сензоре и свакодневне предмете који се обично не сматрају компјутерима, омогућавајући овим уређајима да генеришу, размењују и троше податке уз минималну људску интервенцију (Williams & McCauley, 2016).

Нико од нас не помишља када купује паметан усисивач или аутомобил о томе које опасности постоје. Корисници морају да верују да су ИоТ уређаји и сродни сервиси података заштићени од рањивости, посебно пошто ова технологија постаје све присутнија и уплетена у наш свакодневни живот. Лоше обезбеђени ИоТ уређаји и услуге могу послужити као потенцијалне улазне тачке за сајбер нападе и изложити корисничке податке крађи остављајући токове података неадекватно заштићеним.

Истраживања рађена од стране Републичког завода за статистику 2020. године налазе да **98,3**% домаћинстава поседује ТВ, а **94,1**% домаћинстава поседује мобилни телефон. Лаптоп поседује **52,3**% домаћинстава (Ковачевић et al., 2020). Наредне године тај проценат повећан је на **53,9**% домаћинстава, што представља повећање од **1,6**% у односу на 2020. годину, а **4,9**% у односу на 2019. Годину (Ковачевић et al., 2021). Према извештају Ратела у Србији, 99,2% старости између 16 и 24 године користи рачунар и 98,2% користи Интернет сваки дан или скоро сваки дан (CERT, 2022).

3. Сајбер безбедност

Сајбер безбедност је примена технологија, процеса и контрола за заштиту система, мрежа, програма, уређаја и података од сајбер напада. Циљ му је да смањи ризик од сајбер напада и заштити од неовлашћене експлоатације система, мрежа и технологија (IT Governance, 2022).

Интернет је самостално постигао револуцију начина на који се управља животом, омогућавајући људима да се повежу на друштвене мреже отварајући нове економске хоризонте било то употреба ради вршења трансакција за појединце и организације, или укључивање великих промена у то како се врши настава у школама и на факултетима. Упркос томе, многи људи се и даље суочавају са ризицима по безбедност информација због великог броја претњи. Ове претње се крећу од једноставних до катастрофалних напада. Први се може састојати од примитивних нежељених е-порука, док други може укључивати организоване групе за сајбер криминал који користе злонамерни софтвер за крађу, корумпираност и уништавање података у значајном обиму (Lehto, 2018). Главни фактор ризика за безбедност информација је ниво индивидуалне свести о сајбер безбедности, који се може корисно описати као (Zwilling et al., 2020):

- **Низак-** Понашање ниске свести укључује необраћање пажње или занемаривање безбедносних упозорења, које у већини случајева аутоматски обезбеђују апликације и је приступ бесплатним отвореним мрежама (као што је Ви-Фи) са мобилних уређаја и лаптопова.
- **Средњи-** Средњи ниво свести може се окарактерисати немаром израженом у неправилном раду технологије.
- **Висок-** Коначно, висока свест укључује познавање сајбер претњи и способност предузимања акције у њиховој превенцији.

Јасно је да је свакодневница професионалног живота зависна од употребе интернета за чак и најосновније задатке. Масовност присуства на интернету не

одликује и спремност људи да се информишу о употреби потребних алата који би им омогућили безбедно сурфовање и уопште заштиту од било којих сајбер претњи. Као што смо предходно навели, данас се налазимо у периоду WEB-а 2.0 и основни ниво познавања сајбер окружења није више довољан.

Рансомваре је једна од малициознијих сајбер претња у дигиталној инфраструктури. Нападачи који покрећу нападе рансомваре-а користе различите технике да отму датотеке и ресурсе корисника или организација како би тражили откуп у замену за ослобађање шифрованих/ухваћених података или ресурса. Иако постоји много напада злонамерног софтвера, рансомваре се сматра најопаснијим јер намеће велико финансијско оптерећење организацији. **Криптовалута** је начин плаћања којем се не можеући у траг који нападач користи да би добио откупнину од жртава како би прикрио свој идентитет и локацију. Ово и даље ствара изазове за праћење нападача или мрежа нападача. Предложена су многа решења за анализу и динамичко реаговање на откривене аномалије које штите кориснике и организације од тога да буду жртве напада рансомвера. Криптографски алгоритам који се користи у сваком рансомваре-у је другачији и било би веома корисно погледати извршне датотеке и лоцирати ове крипто модуле. Најчешће се то врши статичком или динамичном анализом. Статичка анализа се користи за откривање крипто-бинарних функција пре њиховог извршења. Динамичка анализа покушава да научи крипто алгоритме током рада (Reshmi, 2021).

Откупни софтвер извршава и понаша се као праве апликације за очување приватности и указује на присуство злонамерних кодова и у сумњивим ситуацијама често даје лажне позитивне резултате и узрокује озбиљне проблеме са техникама откривања заснованим на аномалијама. Потребан је напредак у алатима и техникама јер се рансомваре брзо развија. Постоји много индустријских и академских предлога који раде на локалним хостовима, серверима, облаку итд.

да би се открили и спречили ови напади. Многи предлози сугерисали су анализу дневника понашања система датотека, мрежних пакета, меморијских депонија, који би довели до лакшег и бржег препознавања (Reshmi, 2021).

Потребно је увести знатно повећање знања о сајбер безбедности кроз програме обуке, користећи теоријска предавања и симулаторе (нпр. **Фишинг симулатор**) како би се пружила изложеност алатима за заштиту сајбер безбедности. Они би се фокусирали на оперативне, употребне и процесне аспекте побољшања знања корисника који би се спровели у ефикасно ублажавања претњи у сајбер безбедности. Претње константо еволуирају и човечанство каска за компијутерима. До које границе је могуће постићи оптималну заштиту и указати на њену важност, а притом не уништити доживљај откривања различитих могућности истог? Једном када наше друштво призна да су претње сајбер безбедности штетне не само за једног корисника паметног телефона, већ и за друштво у целини; тада може да почне зачетак решења. Вредност података стално расте, вероватно чак и више од стварног новца. Императив је успоставити културу сајбер безбедности јер је ово питање вишеструко и технологија се стално развија (Bubukayr & Almaiah, 2021).

4. Позиивни и негативни аспекти интернета

Сајбер простор је бесконачан и шири се великом брзином. Можемо га поистоветити са бескрајним црнилом свемира у којем не можемо увек знати шта се налази. Неке од позитивних страна интернета су (Hashem, 2021):

1. Изградња веза и одржавање контакта са породицом и пријатељима
2. Проналажење себе, подстицање креативности и инспирације
3. Показивање емпатије и своје нежности
4. Боља комуникација са људима у стварном животу
5. Ширење битних вести и информација
6. Подршка људима у невољи и самом себи која је најчешће потребна тинејџерима
7. Стварање и креирање сопственог бизниса
8. Мотивација младих људи
9. Образовање о занимљивим темама
10. Проналажење нових хобија и група људи који су уживаоци истих

Негативне стране укључују (Siddiqui & Singh, 2016):

1. Проблем приватности и свести о томе колико је просечна особа заштићена у онлине сфери
2. Проблеми се суочавањем људи лице у лице
3. Онлине малтретирање и злостављање које може довести до незамисливих последица
4. Лажне вести које најчешће постављају инфлуенцери. Иако су често безболне оне некада могу да имају разарајуће ефекте
5. Крађа идентитета и злоупотреба туђих фотографија и снимака које лако могу довести до фаталних последица
6. Интернет изазива зависност

7. Приказивање нереалистичних стандарда лепоте и живота доводи младе често до стања депресије
8. Данас се тешко повлачи линија између тога ко је заиста странац, а ко је особа са интернета што доводи корисника до дилеме коме треба да верује
9. Постоји велик проблем продаје илегалних супстанци и оружја
10. Сексуални злочини су далеко већи поготово они почињени над малолетницима

4.1. Онлајна и офлајн

Стављање линије између реаланог света и интернета је врло тежак. Један од догађаја који је потресао Србију десио се 8. Децембра 2021. године када је на друштвеној мрежи твитер објављено да је двадесетогодишња девојка по имену **Кристина Ђурић** познатија по својој онлине персони Кика извршила самоубиство (Mijušković, 2021).

Наиме, након своје јутјуб и гејмерске каријере, у којој је била веома успешта сакупивши стотине хиљада претплатника, Кика је доживљавала свакодневно онлајн злостављање. Вид малретирања који је она доживела често се састојао из групног малтретирања и вређања онлајн. Овакви догађаји су постали све учесталији и говоре нам о томе колико заправо не постоји свест о томе шта се дешава иза екрана нечијег компјутера. Трагедије које се превасходно дешавају у контексу онлајн сфере бивају закопане мноштвом других информација и заборављене у року од недељу дана.

Камфекција у области рачунарске безбедности је процес покушаја хаковања веб камере особе и њеног активирања без дозволе власника веб камере (Conyers & Kiyuna, 2015). Један од најпознатијих случаја је 32-годишњи софтверски инжењер који је осуђен на две године и два месеца затвора због даљинског приступа дневницима ћаскања, фотографијама, видео снимцима и веб камерама својих женских жртава (FBI, 2014). У периоду од девет година **Роберт Дејвис** је,

користећи се злонамерним софтвером за инфилтрирање, приступао веб камерама девојчица посматрајући их током својих приватних свакодневних активности (FBI, 2014).

Полиција је **11. септембра 2014.** године саопштила да су два мушкарца од 20 година тешко претучена након што је непозната група људи викала омаловажавајуће опаске о њиховој сексуалној оријентацији у Филаделфији (Jitchotvisut, 2018). Како би лакше ушли у траг нападачима, власти су објавиле видео снимак инцидента и није прошло много времена пре него што су твитер детективи у Филаделфији почели да идентификују вероватне починиоце путем провера на друштвеним мрежама користећи идентификацију лица. Након што су твитер истражитељи прикупили довољно доказа, обавестили су полицијску управу Филаделфије и предали случај властима. Ово је такође један од многих случајева у којем се интернет показао као одличан алат у решавању злочина (Jitchotvisut, 2018).

Дана 13. септембра 2005, Близард-ова невероватно популарна масовна онлајн игра **Ворлд оф Воркрефт** (енг.World of Warcraft) доживела је случајан догађај који је имитирао ширење вирусне инфекције широм њене базе играча. Штетни ефекат, назван Корумпирана крв, похарао је хиљаде играча и оставио ликове нижег нивоа у неизбежној смртној петљи. Како је овај вирус напредовао, натерао је своје играче да се карантирају и понашају у складу са правилима како се он не би више проширио. Ширење Корумпиране крви и промене понашања играча у вези са тим привукле су пажњу епидемиолога др Нине Феферман, која је била једна од играча Ворлд оф Воркрефта у време инцидента. Феферман се обратила свом колеги др Ерику Лофгрену. Године 2007. њих двоје су објавили рад у којем су детаљно описани њихови налази, укључујући сложене моделе људског понашања током пандемије. Феферман каже да је инцидент помогао да се информише о тренутном истраживању предиктивног моделирања око Ковид-19 (Elker, 2021).

5. Друштвене мреже

Најпопуларније платформе друштвених мрежа у 2022. години је **Јутјуб** (енг. YouTube), затим **Фејзбук** (енг. Facebook), **Вацап** (енг. Whatsapp), и тик иза њега **Инстаграм** (енг. Instagram) (McCormick, 2022).

Концепт претраживања интернета данас се своди на конзумацију информација, догађаја или људи. Пре само мање од двадесет година овако нешто било је незамисливо. Интерент простор најбоље се могао описати стањем анархије у којој су најискуснији они који испливају на површину. Наш свет се сада мери, мапира и снима дигиталним битовима. Читави животи, од рођења до смрти, сада су каталогизовани у дигиталном царству. Ови подаци, који потичу из тако различитих извора као што су паметна возила, подводне микроскопске камере и фотографије које објављујемо на друштвеним мрежама, довели су нас до највећег доба открића које је човечанство икада спознало. Кроз науку о подацима откључавамо скривене тајне података. Правимо открића која ће заувек променити начин на који живимо и комуницирамо са светом око нас (Cukierski et al., 2015).

Најпознатији веб портал у Србији који популаризује чет собе и полако уводи нашу земљу у свет друштвених мрежа је **Крстарица.** Након Крстарице, пажњу почиње да привлачи и форум **Ана.рс,** познатији и као први женски форум који је активан до данашњег дана.

- **Крстарица**-Настала је 26. марта 1996. године када ју је основао Иван Петровић, који је за непуних годину дана довео Крстарицу до најпосећенијег сајта у земљи. Основне студије завршио је на Факултету организационих наука Универзитета у Београду. Као пројекат из области информационих система одлучио је да креира Крстарицу и самим тим себи упише име у веб историји (Крстарица, 2018).
- Широко познат модел друштвених мрежа није се појавио до 1997.-2000 године са појавом прве модернije друштвене мреже **Sixdeegrees.com** која је

име добила по идеји да су две особе удаљене највише шест конекција. Ова друштвена мрежа настала је свега 5 година пре Фејзбука и није доживела ни приближно велики успех. Највећи проблем ове апликације био је пребрзи излазак из домена локалног и покушај да се оствари глобално. Мала густоћа мреже учинила је да ова друштвена мрежа никада не достигне критичну масу (Kopal et al., 2020).

- **Myspace** (енг. Myspace)- Покренут 1. августа 2003. године. Овај сајт је био прва друштвена мрежа која је досегла глобалну публику и имала је значајан утицај на технологију, поп културу и музику (Molloy, 2008). Појавио се као ривал Friendster-у, али у 2006. години доживео је исту судбину са порастом популарности апликације коју сматрамо синонимом друштвених мрежа.
- **Фејзбук** (енг. Facebook) је америчка друштвена мрежа основана 2004. године од стране Марка Зукерберга и Едуарда Саверина као пројекат повезивања студента који похађају престижне универзитете у Америци, а 2006. године достигли су врхунац обухвативши целокупан свет.
- Синергија структуре блога и друштвене мреже остварио је **Твитер** (енг. Twitter) својом појавом 2006. године када је добио популаран назив СМС интернета. О овој друшвеној мрежи ће бити речи у даљем тексту.
- Година 2010. је упечатљива у том смислу да је интернет почаствован тренутно најпопуларнијиом стриминг платформом **Твич** (енг. Twitch) која има доста елемената друштвене мреже, иако се не сматра друштвеном мрежом. Поред Твича исте године на интернет сцену ступа **Инстаграм** (енг. Instagram) апликација која омогућава кориснику да поставља своје слике, видео записе или приче које нестају након 24 сата. Тренутно се налази у топ 5 најпосећенијих и коришћенијих апликација, поготово њена мобилна верзија. Ова апликација је достигла 2020. године милијарду корисника (Constine, 2018).

- Стабилно издање апликације **ТикТок** (енг. TikTok) је преузело цео свет за секунд. ТикТок, познат у Кини као Дојин (енг. Doyiin), налази се у власнишву компаније БитДенс. Формат је врло једноставан и адиктиван. Корисници могу постављати своје видее у трајању до 3 минута који потом заједно излазе на почетној страници. Логаритам је толико персонализован да теме за које нисте заинтересовани неће вам никада излазити.
- **Јутјуб (енг. YouTube**)- *„Наша мисија је да свима дамо глас и покажемо им свет. Верујемо да свако заслужује да има глас и да је свет боље место када слушамо, делимо и градимо заједницу кроз наше приче.*“ (Youtube, 2022). Америчка платформа за дељење видеа на интернету и друштвена мрежа са седиштем у Сан Бруну, Калифорнија. Покренули су га 14. фебруара 2005. Стив Чен, Чед Хурли и Џевед Карим. У власништву Гугла, то је други најпосећенији сајт ако не рачунамо Гугл ретраживач (Goodrow, 2017).
- **Дискорд** (енг. Discord) је платформа за размену инстант порука (чет соба). Корисници имају могућност да комуницирају гласовним позивима, видео позивима, разменом текстуалних порука, медијима и датотекама у приватним четовима или у оквиру заједница које се називају „сервери“, уколико корисници имају преко 13 година. Сервер је колекција соба за ћаскање путем текстуалних порука и канала за гласовно комуницирање који се користе за разговоре. Може им се приступити преко позива у виду линка. Постоје јавни или приватни сервери. У данашњем окружењу дискорд користе многе модерне фирме као пословну апликацију с обзиром на велики број опција, одличну прегледност и организацију, и могућност додељивања улога различитим корисницима (Discord, 2022).
- **Тумблр (енг. Tumblr)** је амерички веб-сајт за микроблоговање и друштвена мрежа основана 2007. године тренутно у власништву компаније Аутоматик. Омогућава корисницима да објављују мултимедијалне и друге садржаје на кратком блогу. Корисници могу

пратити блогове других корисника. Блогери такође могу учинити своје блогове приватним или јавним. Многим функцијама вебсајта се може приступити преко „контролне табле“. Од јула 2021. Тумблр је домаћин више од 529 милиона блогова. Своју популарност достигао је раних 2010-их година (Boutin, 2009).

- **ЛинкедИн** (енг. LinkedIn) је америчка онлајн услуга оријентисана на пословање и запошљавање која ради преко веб-сајта и мобилне апликације. Покренута 5. маја 2003. године, платформа се првенствено користи за професионално умрежавање и развој каријере и омогућава особама које траже посао да објављују своје биографије, а послодавцима да објављују послове (LinkedIn, 2022).

5.1. Друштвене мреже забавног карактера

5.1.1. Фејзбук-Facebook

Са преко 2,32 милијарде активних месечних корисника, Фејзбук остаје најраспрострањенија платформа друштвених медија, са процењених 13 милиона интеракција у секунди (Juma & Shaalan, 2020). Један је од најизазовнијих артефаката рачунарске науке, који поставља неколико изазова оптимизације и робусности. Да бисте креирали свој налог потребне су вам следеће информације: име, презиме, важећи имејл. Прављење јединственог налога траје свега пар секунди. Можете поставити своју профилну слику и насловну слику, делити на свом зиду линкове, фотографије и кратке снимкове које могу гледати лајковати и коментарисати ваши пријатељи. Осећај инклузивности на Фејзбуку се добија учествовањем у групама и страницама које можете правити или се већ придружити постојећима. Раније су људи бирали ресторане гледајући колико је купаца већ било тамо. У доба друштвених медија, утицај других је јачи: људи могу да посматрају чекирања својих пријатеља на Фејзбуку преко мобилних телефона и да тиме донесу одлуку о одабиру ресторана без потребе да их посећују физички, већ да то посматрањем својих пријатеља учине онлајн (Kumar & Qiu, 2021). Пријатељство на Фејсбуку је неусмерена веза. Ако је корисник некоме пријатељ, онда је њихово пријатељство узајамно. Сматра се да је Фејзбук друштвена мрежа која је највише интегрисана у животе група без обзира на пол и године. Могућност повезивања свог Фејзбук налога са другим апликацијама омогућава Фејзбуку далеко лакши начин сакупљања потребних информација. На пример, Амазон је дао корисницима могућност да не поделе свој идентитет приликом објављивања рецензија, док су Јелп и ТрипАдвисор интегрисали корисничке налоге са личним Фејзбук налозима. Када нас трећа апликација пита да ли желимо да је повежемо са Фејзбуком и тиме уштедимо време како не бисмо морали да креирамо налог, пружамо личне податке трећим аплацијама и тиме доводимо себе у опасност која надилази корист.

5.1.2. Твитер-Twitter

Твитер је платформа друштвених медија заснована на микроблоговању. Корисници који прате аутора могу читати његове објаве, које су ограничене на 280 карактера и свака таква написана порука окачена на наш зид назива се твит. Пријатељства се не стварају као на Фејсбуку. Уколико некога запратити он није дужан да запрати вас чиме се даје осећај хијерархије и појаве инфлуенцера. Сваки твит који корисник објави је апсолутно јаван за разлику од објава на Фејзбук профилу који су откључани под условом пријатељства. Корисници не морају да се региструју да би читали постове, али се морају регистровати да би их објавили. Опис вашег Твитер профила укључују основне информације о вама као што су: име, презиме, број твитова, када сте се придржили твитеру, колико корисника ви пратите и колико корисника прати вас. Иако Твитер спада у друштвене мреже које превасходно служе за забаву, Твитер помоћу својих хештегова привлачи велике групе маркетиншких стручњака и продавца који лако могу да пронађу тип публике у ком усмеравају свој производ.

5.1.3. Инстаграм-Instagram

Купљена од стране Фејзбука 2010. године, Инстаграм је друштвена мрежа креирана по принципу дељења искључиво слика или видео снимака које се сортирају по хештеговима или локацијама на којима се налазе корисници. Популарност је задобила могућношћу да корисници преко својих слика стављају филтере које је Инстаграм дизајнирао. Предходно поменут термин инфлуенцера је настао на овој друштвеној мрежи. Проводећи свакодневницу на овој апликацији стичемо осећај да је ово једина платформа која пружа осећај емотивне повезаности између корисника и производа. Била и Каркуш 2016. пронашли су доказе да корисници Инстаграма показују теже облике симптома депресије, анксиозности и стреса, од оних који га не користе (Bilal et al., 2016). Ипак, ова апликације има највећи домен међу младима и поспешује осећај инклузивности, активизма и покретања разговора о темама које су се често сматрале табу.

5.1.4. Јутјуб-Youtube

Откад је купљен од стране компаније Гугл, Јутјуб се проширио ван основног веб сајта на мобилне апликације, мрежну телевизију и могућност повезивања са другим платформама (NBC, 2006). Видео категорије обухватају музичке спотове, видео клипове, вести, кратке филмове, игране филмове, документарне филмове, аудио снимке, трејлере филмова, тизере, стримове уживо, влогове и још много тога. Већину садржаја генеришу појединци, укључујући сарадњу између Јутјубера и корпоративних спонзора тј. утемељених медијских корпорација као што су Дизни, Парамоунт и Варнер Брос. Дискавери телевизија је такође креирале и проширили своје корпоративне канале како би се оглашавале широј публици. Јутјуб је прва платформа на којој су креатори бивали плаћени од компаније директно тако што би скупљали претпланике.

5.2. Друштвене мреже пословног карактера

5.2.1. Линкд ин-LinkedIn

ЛинкедИн омогућава члановима (радницима и послодавцима) да креирају профиле и повезују се једни са другима у онлајн друштвеној сфери која може представљати професионалне односе у стварном свету. Чланови могу позвати било кога (било постојећег члана или не) да постане линкед ин тј. умрежен. Такође, може се користити за организовање офлајн догађаја, придруживање групама, писање чланака, објављивање огласа за посао, објављивање фотографија и видео записа и још много тога (LinkedIn, 2022).

5.2.2. Митап-MeetUp

Митап је платформа друштвених медија за хостовање и организовање личних и виртуелних активности, скупова и догађаја за људе и заједнице сличних интересовања, хобија и професија. Основали су га 2002. Скот Хејферман и још четворица сарадника. Дефиниција „професионалног умрежавања“ је синоним за семинаре, конвенције и било коју врсту такозваних састајања. Преко Митап

платформе можете пронаћи заједнице људи који имају заједничке интересе. Догађаји су груписани у различите категорије као што су професионални догађаји, категорисани под: *каријера и посао*. Обично је то мешавина семинара и умрежавања након посла (Norton, 2021).

5.2.3. Ксинг-Xing

Ксинг платформа је еквивалентна ЛинкедИну за говорнике немачког (Xing, 2022). То је један од најпопуларнијих сајтова у Немачкој (10,1 милион корисника), Швајцарској (900.000 корисника) и Аустрији (800.000 корисника). У Европи има око 12 милиона регистрованих чланова. Међутим, говорници немачког нису једина циљна група платформе. Постоје чланови из целог света који говоре низ различитих језика. Преко Ксинг-а можете се умрежити са другим пословним професионалцима, пронаћи прилике за посао, информације о конвенцијама, семинарима, курсевима обуке и још много тога. То је одлична алтернативна платформи ЛинкедИн (Norton, 2021).

5.3. Врсте узнемиравања на друштвеним мрежама

Растућа популарност друштвених мрежа произилази из великог броја корисника стечених за кратко време; неки сервиси друштвених мрежа већ сада су окупили стотине милиона корисника. Повећање доступности интернета, подстиче кориснике да 24/7 на различите начине граде поуздане односе на мрежи без икакве опрезности или свести о последицама које их могу затећи. Преливање сајбер света у реалност свакодневнице препушта омладину и наше најмлађе чланове да се боре са сасвим новим претњама као што су:

1. **Узнемиравање**- То укључује слање увредљивих и злонамерних порука појединцу или групи насилника и често се понавља више пута. Сајбер ухођење је један од облика узнемиравања који укључује сталне претње и непристојне поруке, и може довести до физичког узнемиравања у стварном, офлајн свету.
2. **Флејминг (енг. Flaming)** је сличан узнемиравању, али се односи на препирку на мрежи која се размењује путем е-поште, тренутних порука или соба за ћаскање. То је врста јавног малтретирања која често упућује грубо ословљавање, вређање или непримерене слике ка одређеној особи. Овакав тип малтертирања се често налази у четовима MOBA (eng. Multiplayer online battle arena) игара.
3. **Изостављање**- Искључивање је чин намерног издвајања и изостављања особе из онлајн група и сајтова за ћаскање. Група потом оставља злонамерне коментаре и малтретира онога кога је изоставила (Kim, 2013).
4. **Доксовање (енг. Doxing)**- Односи се на чин отвореног откривања осетљивих или личних података о некоме без њиховог пристанка у сврху њиховог срамоћења или понижавања. Ово може да варира од ширења личних фотографија или докумената јавних личности до дељења сачуваних личних порука појединца у онлајн приватној групи. Кључан је недостатак пристанка жртве. Превара слична доксовању са додатним елементом обмане је

ситуација у којој се насилник спријатељује са својом метом и уљуљкава је у лажни осећај сигурности. Када насилник задобије поверење своје мете, злоупотребљава то поверење и дели тајне и приватне информације жртве трећој страни или више трећих лица (Securly, 2019).

5. **Тролovање-** Тролovање је појава када насилник жели да намерно узнемири друге објављивањем запаљивих коментара на мрежи. Тролovање можда није увек облик малтретирања путем интернета, али се може користити као алат за сајбер малтретирање када се ради са злонамерном и штетном намером. Ови насилници имају тенденцију да буду одвојенији од својих жртава и немају лични однос.
6. **Маскирање-** Маскирање се дешава када насилник креира измишљени профил или идентитет на мрежи са једином сврхом да некога малтретира путем интернета. То би могло укључивати креирање лажног налога е-поште, лажног профила на друштвеним мрежама и одабир новог идентитета и фотографија како би се преварила жртва. У овим случајевима, насилник обично буде неко кога жртва прилично добро познаје.

Са појавом корона вируса и померања школовања у онлајн сферу, наилазимо на пораст злостављања и малтретирања не само од стране вршњака већ и од стране наставника и професора алудирајући на то да онлајн дискурс није довољно валидан и да жртве не доживљавају заправо неку врсту злостављања. Самим тим починиоци неће бити пријављени и њихово понашање неће бити санкционисано. У недостатку адекватне дефиниције онлајн академског малтретирања као претње која се појављује, његове мете не могу лако да процене његову озбиљност или са сигурношћу пријаве да су жртве (Noakes & Noakes, 2021).

7. Анализа друштвених мрежа

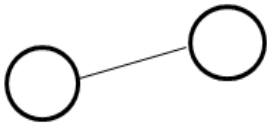
Када бисмо се удаљили од релности и сагледали свет око нас дошли бисмо до увида да се цео свет може перцепирати као мрежа или шаблон. Жене, мушкарци, деца, животиње, биљке; од ланца исхране до нагона живота и смрти, преко хемијских реакција које се дешавају у нашим телима.

Термин социјлна мрежа је први сковао Роџер Браун који је утврдио да је социјална структура слична мрежи и како комуникација међу појединцима личи на однос између чворишта и другог угњежђења у мрежи (Zhang, 2010). О овим појмовима ће бити више речи у наредном поглављу. Један аутор га је дефинисао као Уметност и науку извлачења вредних скривених увида из огромне количине полуструктурираних и неструктурираних података друштвених медија како би се омогућило информисано и проницљиво доношење одлука (Sponder & Khan, 2018).

Био чвор или комадић свако живо биће је део веће слике на платну живота. Присуство претходно поменутих друштвених мрежа ствара велике потребе за анализом огромне количине података било ради статистичке евиденције или ради увида у популарне трендове и пласирања одређених производа. Сваки корисник је чвор у неком графу и уколико не постоји производ који се пласира онда је корисник сам производ. Наука о подацима има карактеристике сличне ДНК. Попут ДНК, наука о подацима се састоји од основних грађевних блокова који су уткани у ствар велике лепоте и сложености. Грађевински блокови стварају темељ, али успешна репликација такође захтева пажљиво избалансиране процесе и идеалне услове околине. На крају, сваки пример може изгледати површно, али сировине остају исте (Boozo Allen Hamilton Inc., 2015).

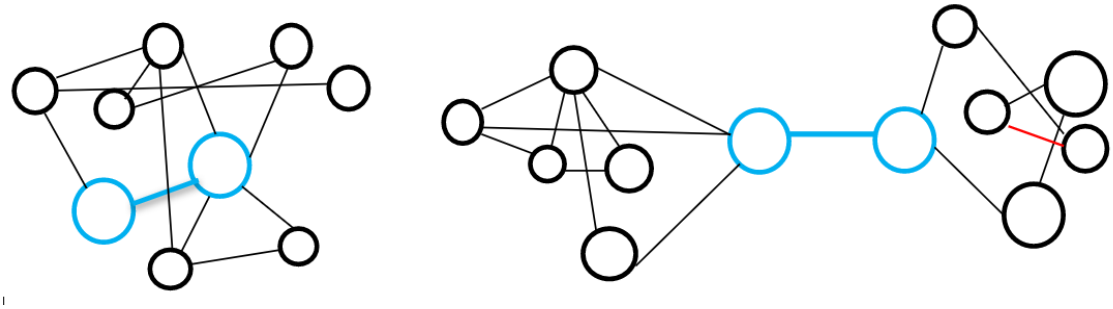
7.1 Терминологија анализе друштвених мрежа

Основни концепт анализе мрежа можемо замислити као релацију између двоје људи који један другом шаљу СМС поруке. Скуп ових појединаца анализира се помоћу **графова**. Кружне сфере у графу представљају особе и називају се **чворови** (енг. Node, Vertex) док линију која их повезује називамо **ивица** (енг. edge, link) као што видимо на слици број 1 (Grandjean, 2021).



Слика бр 1: Неусмерен приказ два чвора (Граф са 1 ивицом)

Интерес највише пада на **ивице**, тј. интеракцију између чворова. Када бисмо у додали и све остале чланове који се дописују са чворовима са слике број 1, дошли бисмо до сазнања да између неких од њих такође постоји веза. Шта више, постоји могућност да је неко од њих и део примарне везе као на слици број 2 (Grandjean, 2021).



Слика бр. 2: Приказ проширеног неусмереног графа

Наравно, споредни чворови такође могу имати релације тј. односе једни са другима без обзира на одабране чворове. Сагледајући ову велику мрежу схватамо да чворови са Слике број 1 нису једини фактор у њиховом односу, нити су по сваку цену центар истог. Додавањем додатних нивоа овој интеракцији приказује

се степен децентрализације који се шири докле год постоје ивице и чворови. Ширина мреже зависи од количине информација којом располажемо и колики је домен нашег интересовања. Два чвора могу бити центар збивања, и у исто време имати различит контекст. Граф сагледамо као математички концепт који нам на апстрактан начин поједностављује односе људи у њему.

Односи ивица унутар графа могу бити (Grandjean, 2021):

- **Неусмерени** (енг. Undirected)- Два чвора која су повезана једном ивицом
- **Усмерени** (енг. Directed)- Два чвора која су повезана луком, у којем се ставља акценат на реципрочност у којем долазимо до сазнања ко је прималац а ко пошиљалац
- **Реципрочни** (енг. Reciprocal) Два чвора повезана луком где су пошињаоц и примаоц у реципрочном контакту

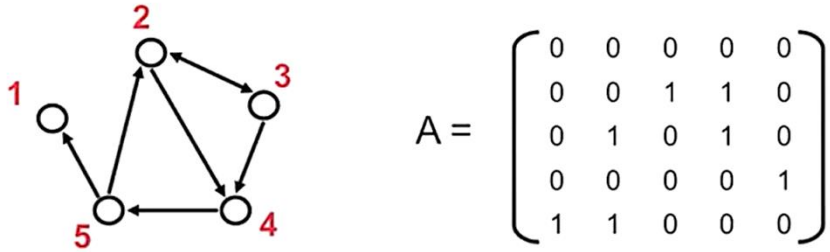
Слика бр. 3: Приказ различитих врста ивица унутар графа

Поред односа потребно је поменути и **атрибуте ивица** (Adamic, 2012):

- Први који ћемо поменути је **степен пондерисаности** (енг. Weight) који нам укратко показује фреквентност комуникације. Ивица може имати бесконачну вредност и даје нам више информација о томе колико је однос интензиван и колики је степен појављивања тог односа (Слика бр 3.4.). Додавањем веће тежине ивицама долазимо до ужих сазнања.
- Са друге стране се налази и **степен непондерисаности** (енг. Unweighted) где не постоји однос тј ивица између два чвора.
- **Тип** (енг. Type) , представља особу која се налази иза чвора.

- **Ранг** (енг. Ranking), означава ближе ко је особа која представља дат чвор. Да ли је то наш пријатељ, познаник или на пример члан породице. Рангира учеснике графа на основу улоге.
- Својства у зависности од остале структуре графа

Како софтвер представља нашу мрежу? Најједноставнији начин је кроз матрицу суседности (енг. adjacency matrix), као штоо је приказано на слици број 4, али такође се користи и листа суседности (енг. edge list) и листа ивица (енг. adjacency list) (Adamic, 2012).



Слика бр. 4: Приказ усмереног графа (лево) и матрице суседности (десно) (Adamic, 2012)

Скуп А представља **матрицу суседности**. Први ред представља први чвор који не поседује ни једну одлазећу ивицу, ипак, како се виид на усмереном графу, има једну ивицу које се креће ка њему која је обележена бројем 1 у првој колони (Adamic, 2012).

- А**ij**= 1 ако чвор и има ивицу ка чвору j (**И<=>J**), или је =0 уколико чвор и нема ивицу ка **J**
- А**ij**= 0 осим ако мрежа не иде сама око себе
- А**ij**= А**ij** ако је мрежа неусмерена или ако и или **J** деле заједничку реципрочну ивицу **(И<=> J)**

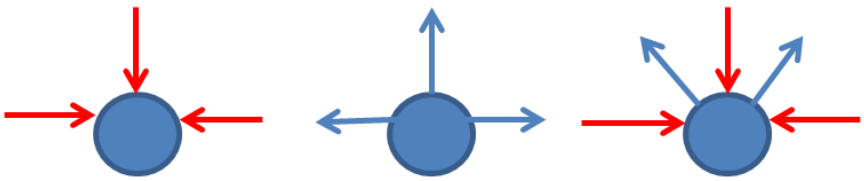
Листу суседности се користи за лакшу и крађу анализу, тако да уместо гомиле нула пишу се ствари које се налазе на графу (нпр. 2,3;2,4;3,2;3,4...).

Листу ивица се користи када граф има велики број интеракција и када постоји превише атрибута на једној мрежи. Као и у предходном примеру (Слика бр. 4), уместо писања много нула за први чвор довољно је написати 1 за други 3,4; за трећи 2,4...(Adamic, 2012).

Централност се концентрише на одређеног појединца као тачку фокуса. Мери степен до којег појединац комуницира са другим појединцима у мрежи. Што се појединац више повезује са другима у мрежи, то је већа њихова централност у мрежи (de Laat et al., 2007).

Ивична својства најближих конекција могу бити (Adamic, 2012):

- **Централност у степену** (енг. indegree) се концентрише на одређеног појединца као тачку фокуса. Централност свих других појединаца заснива се на њиховом односу према фокусној тачки појединца „У степену". (Слика бр. 5.1.)
- **Спољни степен** (енг. outdegree) је мера централности која се још увек фокусира на једну индивидуу, али се аналитика бави излазним интеракцијама појединца. Мера ванстепене централности је колико пута фокусна тачка појединца ступа у интеракцију са другима. (Слика бр. 5.2.)
- **Комбиновани степен** обухвата број директних ивица које се крећу ка чвору и из њега (Слика бр. 5.3.)



Слика бр. 5: Са лева на десно, 1) Чвор приказан са централношћу у степенеу, 2) Чвор приказан са спољашњим степеном 3) Чвор приказан са комбинованим степеном

Да ли је сваки чвор повезан један са другим? То можемо изразити на следећи начин (Adamic, 2012):

1. **Снажно повезане компоненте** означавају могућност сваког чвора да у одређеном графу достигне било који други тако да су повезани директном ивицом
2. **Слабо повезане компоненте** означавају хипотетичку могућност да се сваки чвор може достићи од стране било ког другог пратећи ивицу у било ком смеру
3. За сада, можемо само поменути и **гигантску компоненту**

Када се говори о мери централности, она даје могућност лакшег уочавања кључних актере. Она се изражава кроз следеће мере (Adamic, 2012):

- **Степен централности** (енг. degree centrality)-Представља појединца обележеног чвором на графу који има највише конекција са осталим појединцима.
- **Централност блискости** (енг. closeness centrality)-Састоји се у мерењу удаљености врхова графова. Онај који има најмању просечну удаљеност у односу на остале је, дакле, онај који је у просеку најближи свим осталима.
- Својства која додељујемо ивицама зависе од остатка мреже. Неке ивице могу се налазити између два подручја мреже и тиме могу да играју улогу моста. То је својство које називамо **степен међусобности** (енг. betweenness centrality). Рачунамо удаљеност између два чвора тако што бројимо на колико њих наилазимо док не дођемо до жељене тачке.
- **Својствена централност** (енг. eigenvector centrality)-Када се одмакнемо и погледамо у граф уочићемо чвор са највише конекција. Издвајање тог примера чинимо помоћу овог алата.

Овакав концепт не можемо применити на стваран живот ако не платимо цену екстремног поједностављивања људских односа и свођења интеракција на чворове.

То је изузетно једноставан начин да се представи однос између два елемента, који садржи веома висок ниво апстракције.

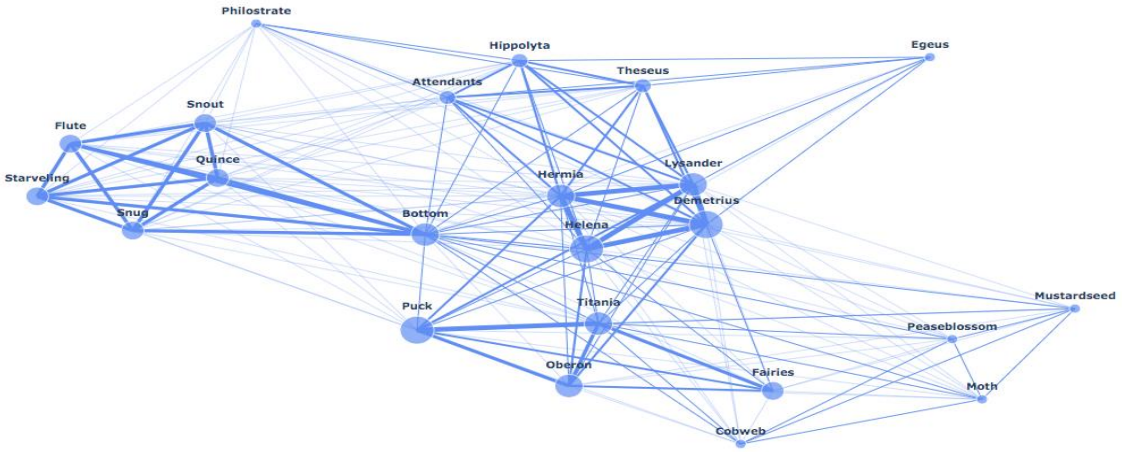
7.2. Алати за анализу

Приказ следећих алата односи се на програмске, хибридне и алате који се користе за визуелизацију. Велике мреже је веома тешко представити и самим тим визуелизовати тако да информације које су добијене могу бити искоришћене на користан начин.

У даљем тексту ћу представити оне које су најпопуларније и на које се најчешће наилази приликом визуализације података у сфери анализе мрежа. **Гефи** (енг. Gephi) је алат који је намењен истраживачкој анализи података. Реч је о хибридном алату који може поднети рад на малим, средњим и средње великим мрежама. Ово је алат који ћемо користити приликом анализе у даљем тексту.

Нетворк Екс (енг. Network X) је Пајтон (енг. Pyton) библиотека која омогућава стварање и манипулацију мрежама. Програм ову библиотеку такође користи ради визуелизације. Процес учења овог алата у данашњем времену није превише захтеван и нашао би се при врху лествице као погодан за почетнике, иако је неопходно познавање Пајтона.

Долази са великим бројем алгоритама за анализу мрежа. Форма датотека које прима су GLM, GraphML,GEXF, Pajek, Graph 6... (Kopal et al., 2020). На слици испод (Слика бр. 6) можемо видети приказ односа у једној од најпознатијих представа Вилијама Шекспира Сан летње ноћи.

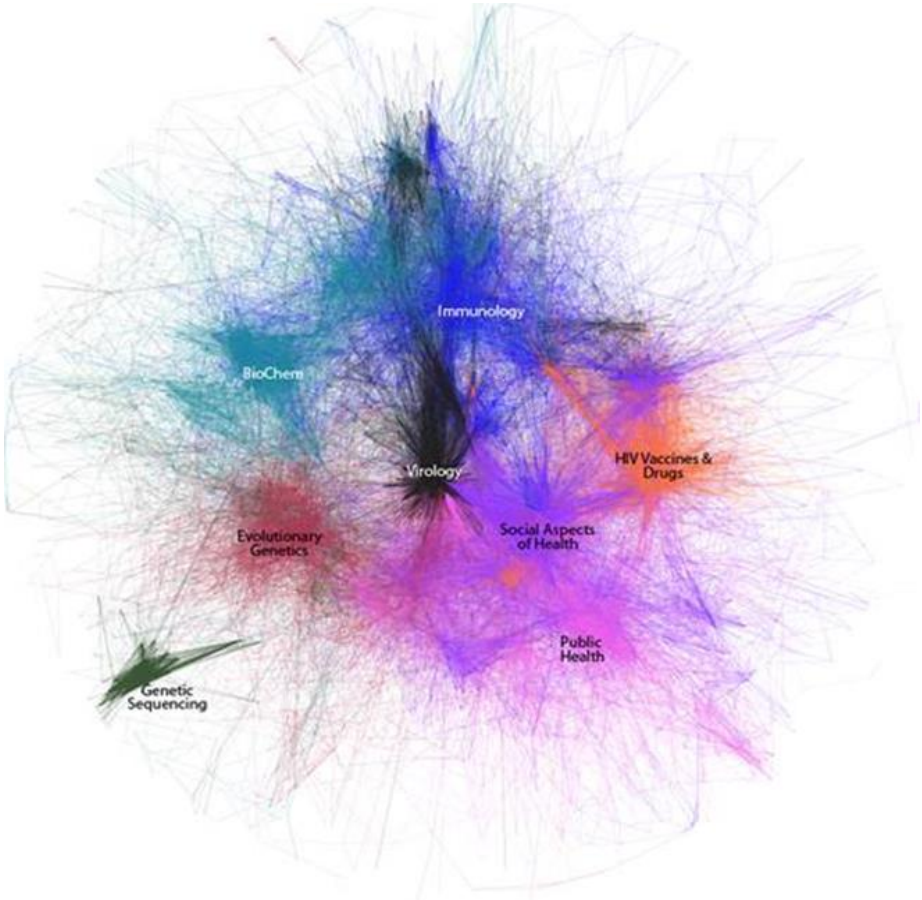


Слика бр. 6: Приказ графа коришћењем Неворк Икс-а, Однос ликова у делу Сан Летње ноћи В. Шекспира (Weng, 2020)

Пајек (енг. Pajek), или у преводу на српски језик паук. Као алат за анализу најчешће се користи за анализу великих мрежа. Писан је у Делфију и долази у различитим варијантама као што су Пајек и Пајек икс ел (енг. Pajek XL), при чему други користи далеко мање меморије и ради са лакоћом на још већим мрежама. Пајек има уграђене најчешће коришћене алате за анализу мрежа.

Један занимљив пример овога је то да ако пошаљете граф у Ексел, Пајек ће отворити нови документ и у њега записати матрицу суседства. Поред тога нуди могућност 3Д приказа и оптимизован је да ради са сопственим форматом улазних дадотека (Kopal et al., 2020).

На слици испод (Слика бр. 7) је визуелни приказ преклапања заједница које учествују у напретку медицине.

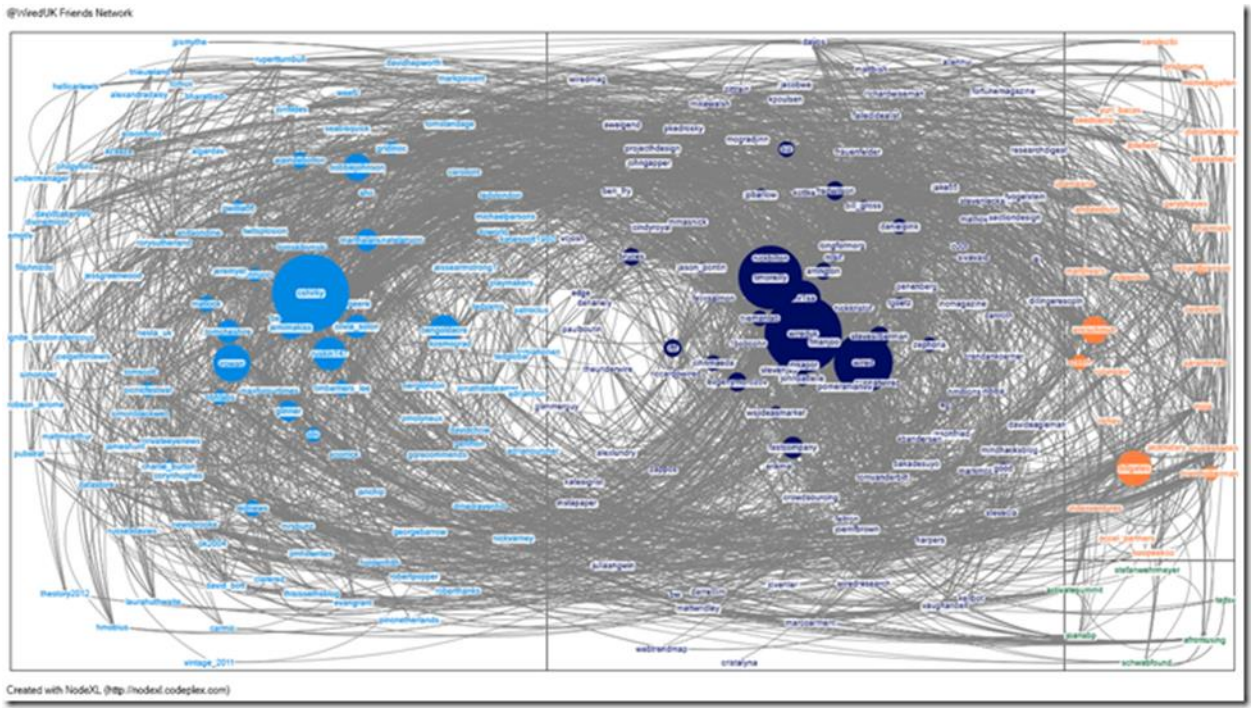


Слика бр. 7: Приказ преклапања научних заједница у медицини користећи визуализацију Пајек програма (Moody, 2018)

Ноде икс-ел (енг. Node XL) је алат Мајкрософт Ексела (енг. Microsoft Exel) из 2007. године који функционише као додатак и служи за анализу и визуелизацију података. Он може користити дадотеке Пајек, GraphML, UCINet, а такође може и да анализира податке са друштвених мрежа као што су фејзбук, твитер или јутјуб. Нуди основне могућности визуелизације мреже са доста понуђених шаблона за једноставнији рад.

Овај алат је добар за почетнике и такође даје могућност лаког прелажења са Ноде икс ел-а на Гефи и самим тим Ноде икс ел може да извози фајлове који су компатибилни са Гефијем (Kopal et al., 2020). Слика број 8 нам показује

визуелизацију и анализу твитер група и њихову интеракцију, користећи Ноде икс ел.



Слика бр. 8: Интеракција различитих твитер група визуализовано помоћу програма Ноде икс ел-а (Hawksey, 2011)

Одабир алата највише зависи од одговора на следећа питања:

- Да ли је потребно анализирати веће количине података? Да ли је потребно израчунати у стварном времену?
- Да ли је мрежа која се анализира гушћа и већа и да ли је битно време за које ће се извршити израчунавање?

Након одговора на ова питања долази се до најадекватнијег алата у односу на потребе анализе.

8. Анализа друштвених мрежа и подизање свести младих о сајбер безбедности користећи Гефи и Нетлитик

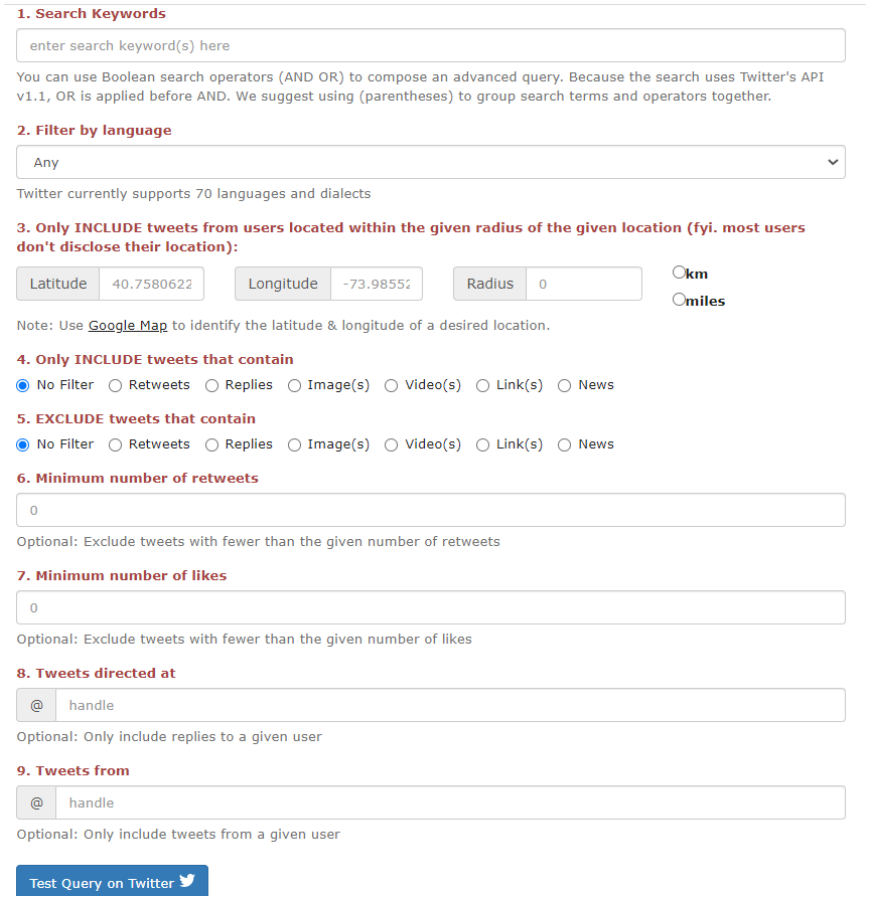
Успех визуелизације заснива се на дубоком познавању и бризи о суштини, квалитету, релевантности и интегритету садржаја. Визуелизација података је одувек имала значај у друштвеним наукама и она има неколико предности, укључујући, али не ограничавајући се на, давање смисла сложеним питањима на лакши и привлачнији начин. У даљем тексту ћу приказати анализу друштвених мрежа помоћу алата Гефи и Нетлитика. Као што је у предходном делу текста већ поменуто, Гефи је алат који омогућава лаку манипулацију и визуелизацију графа. Могућности које поседује су широке, а постоји могућност њиховог проширења користећи плагинове које му додају на функционалности и начину визуелизације мреже (Gephi, 2022).

Нетлитик је програм који на једноставан начин нуди прикупљање и визуелизацију података преко неколико платформи друштвених мрежа. Он је бесплатан и врло једноставан за коришћење. Потребно је имати валидну Гугл адресу и лични профил на Твитеру. Ради на неколико популарних друштвених мрежа као што су Твитер, Фејсбук, Јутјуб и Инстаграм. Такође подржава текстуалне датотеке и табеле за анализу података. Подаци добијени преко Нетлитик-а могу се користити у већини других платформи за анализу мреже (Netlytic, 2022).

8.1. Репрезентативност узорка

Пре него што почнем са анализом потребно је да то урадим на валидном узорку. Друштвену мрежу на којој ћу вршити анализу је Твитер. Често је коришћена за вођење разговора о озбиљнијим темама и брзом ширењу вести из целог света. Самим тим Твитер је добар избор за ову анализу. Када отворим прву страницу Нетлитика и улогујем се потребно је да се пријавим на ниво два. Важно је имати налог на нивоу два, зато што већина тема на Твитеру почиње са 50.000 твитова, а

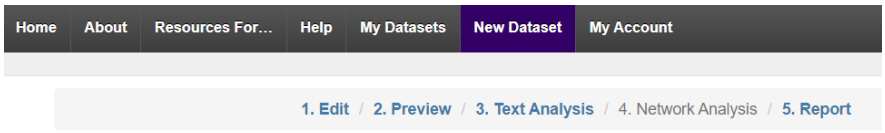
најпопуларније теме обично имају неколико стотина хиљада твитова. Скуп података који се састоји од 10.000–50.000 твитова о актуелној теми је статистички репрезентативан. Кликнућу на поље на коме пише нови сет података (енг. New dataset) означено тегет бојом на слици број 10, где ће се приказати да сам повезана са својим Твитер налогом и у првом реду уписујем назив сета, укуцавам кључне речи и кликћем на (енг. Test Query) тј. тестирање упита (Слика бр. 9).



Слика бр. 9: Приказ екрана који користимо ради претражавања упита на друштвеној мрежи Твитер, Преузето са: https://netlytic.org/?do_addDataset

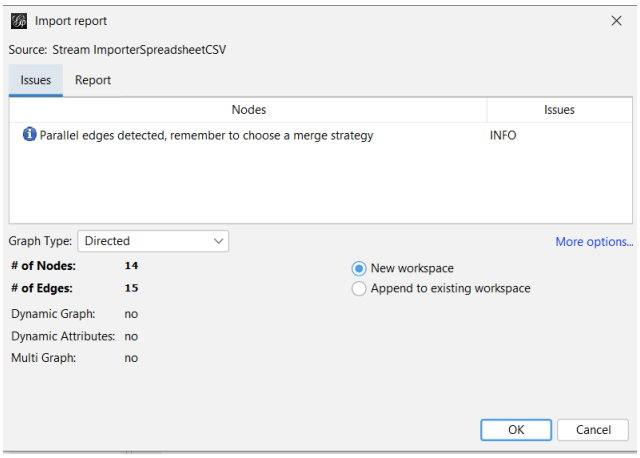
Упите које ћу креирати су: *Сајбер безбедност, Сајбер безбедност (млади), Cyber Security, Cyber Security (youth).*Употребом терминологије на енглеском језику добија се већа количина података за анализу. Након тестирања термина сајбер безбедност,

програм ће га обрадити. Након тога кликом на поље Анализа мреже (енг. Network Analysis) генерише се фајл спреман за преузимање.



Слика бр. 10: Приказ интерфејса Нетлитика, Преузето са: https://netlytic.org/?do_addDataset

Отварам апликацију Гефи и убацујем фајл. Прва страница која се појављује има приказ колико ивица и чворова се састоји у овом графу (Слика бр. 11), и служи као одличан индикатор тога колико је конкретно интеракција извршено по питању овог термина.



Слика бр. 11: Приказ броја ивица и чворова приликом убацивања фајла у апликацију Гефи

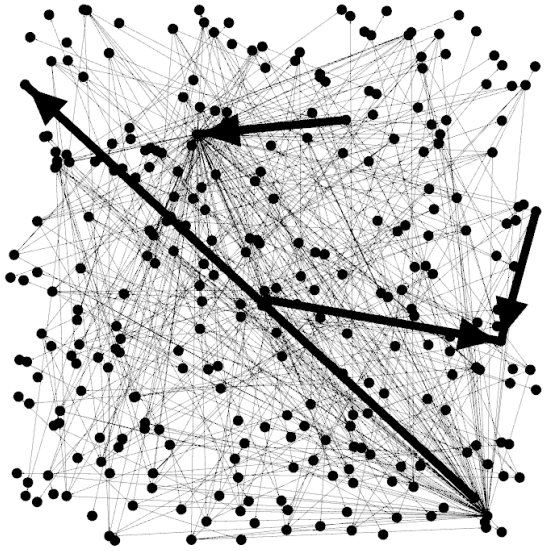
Видимо да је број чворова 14 а број ивица 15, закључујемо да се на Твитеру у контексу термина сајбер безбедност не води толико опширан разговор. Када поновимо овај исти процес долазим до:

- **Сајбер безбедност**: Чворова:**14;** Ивица: **15**
- **Сајбер безбедност (млади):** Чворова:**1**; Ивица**: 0**
- **Cyber Security**: Чворова**: 20 328**; Ивица**: 37 140**
- **Cyber Security (youth):** Чворова: **295**; Ивица: **495**

Најрепрезентативнији узорак је последњи који није ни превелик ни премали и то га чини подобним за вршење анализе приликом које могу добити валидан резултат.

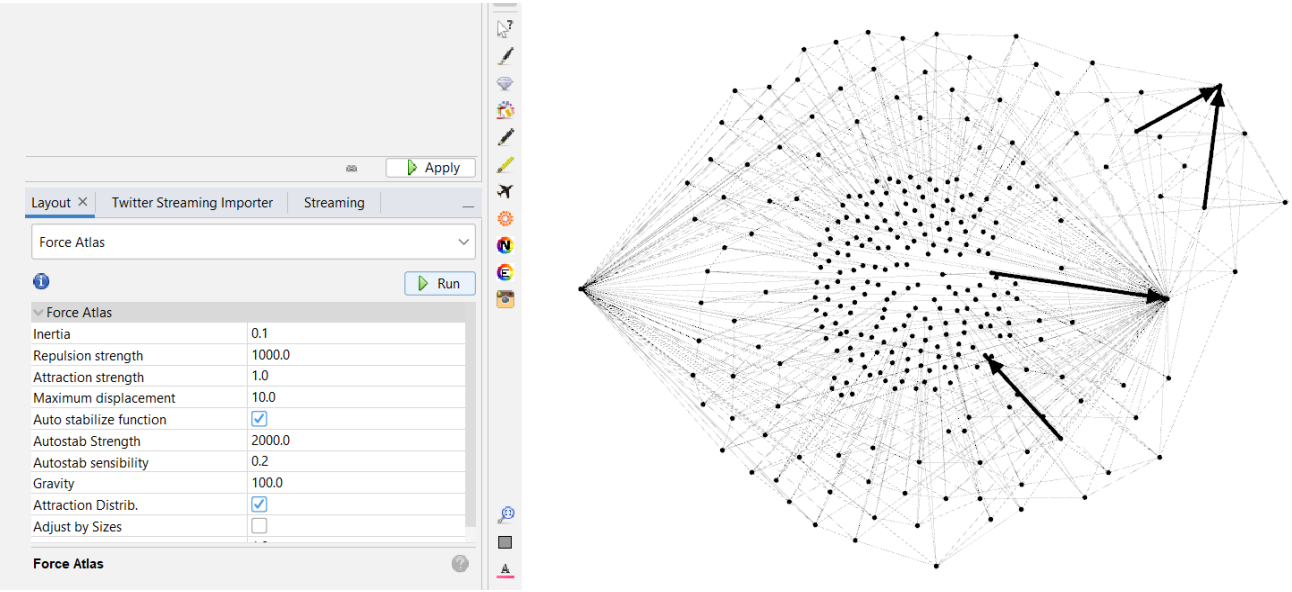
8.2. Анализа узорка коришћењем Гефија

Први корак: Убацујем узорак у Гефи који потом генерише извештај (Слика бр. 11), притискам дугме OK и тада нам се по први пут на екрану појављује граф који у овом моменту изгледна хаотично и врло несређено (Слика бр. 12). Он је увек црних ивица и чворова. Користећи точкић на мишу можемо га увећавати и смањивати на екрану.



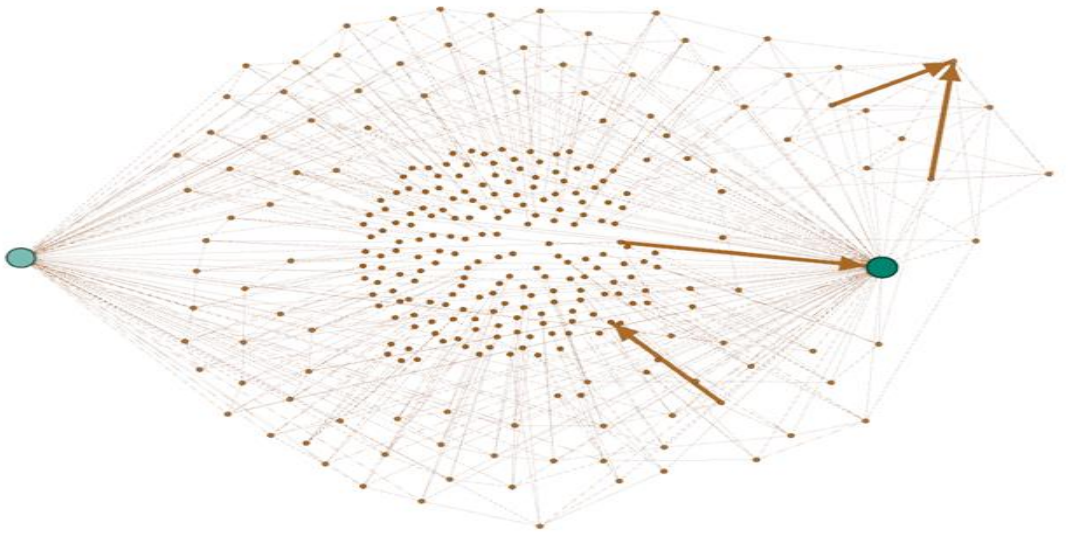
Слика бр. 12: Приказ несређеног графа у Гефију

Други корак: Алгоритми распореда одређују облик графикона. То је уједно и најважнија операција. Поставка (енг. Layout) у себи садржи различите опције, а из падајућег менија бирам опцију *Force Atlas,* и тако покрећем програм и постављам параметре (како је приказано на слици бр. 13 са доње леве стране) тако да добијем бољи изглед графа. Када сам задовољна изгледом графа заустављам функцију.



Слика бр. 13: Приказ графа приликом коришћења Форс Атласа

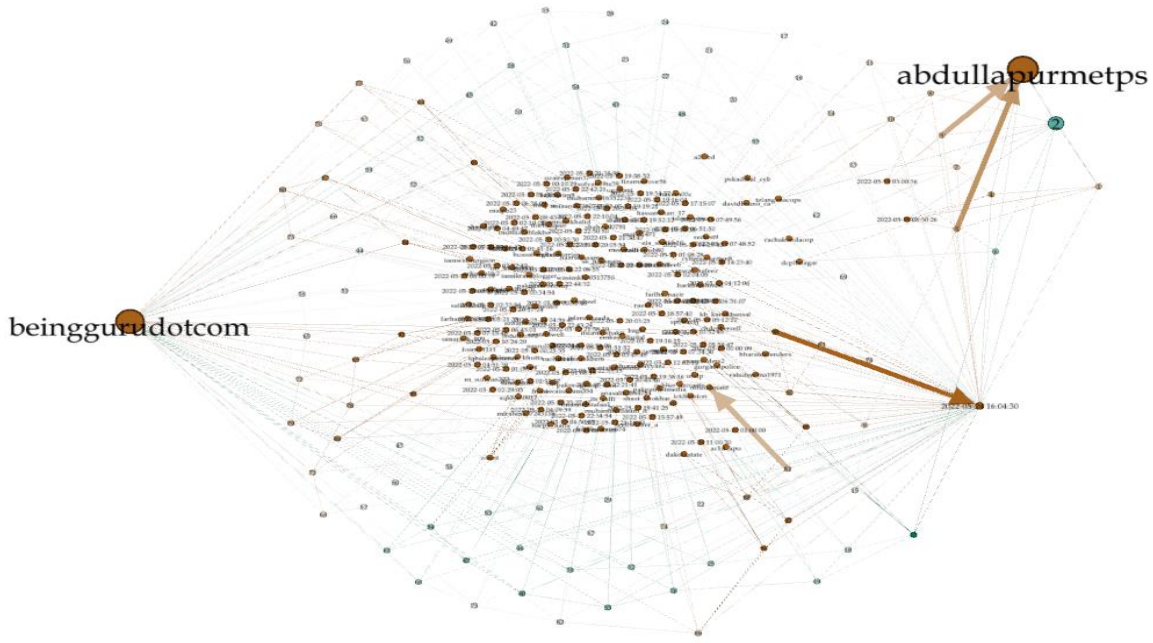
Трећи корак: У горњем левом углу кликом на картицу Ranking->Degree->Nodes и одаберем боју, и преко градијента ћу моћи да видим да зелени чворови имају највише ивица а браон најмање. Да би граф био прегледнији притиснућу на дугме које изгледа исто као дијамант и вертикално ћу повући курсором и повећати чворове који ме занимају (Слика бр. 14).



Слика бр 14: Сортиран граф у односу на степен

Док се ова радња извршава, са десне стране у прозору статистика ћу покренути команду под именом *Avg. Path Length*. тј. просечну дужину пута, која ће потом избацити два прозора у којима ћу добити увид у број чворова између којих се посматрани чвор налази (енг. betweennes centrality), и у близину два чвора (енг. closeness centrality). **Просечна дужина пута је 5,506,** док је **дијаметар 16** што значи да мрежа мора прећи **16 скокова** да би дошла од једног до другог чвора.

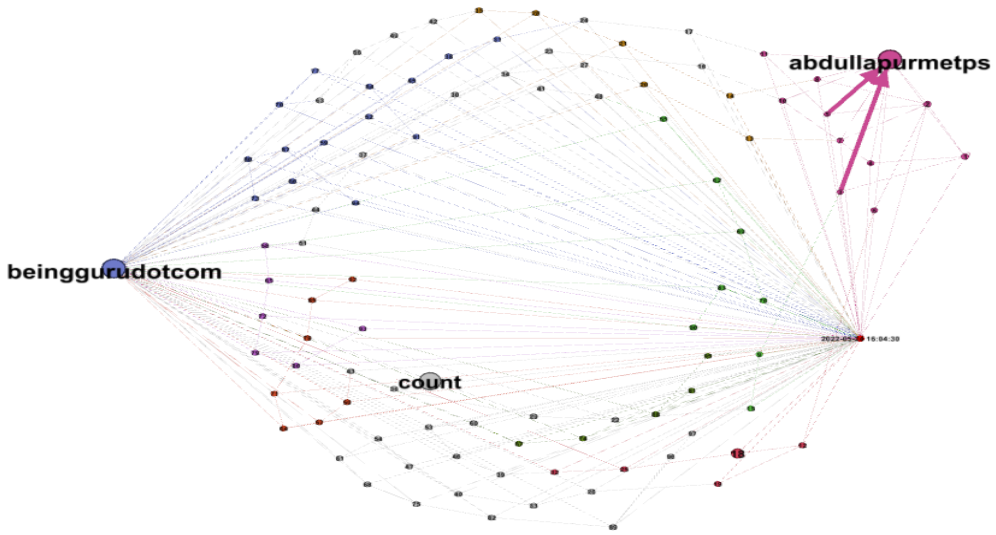
Четврти корак: Appearance->Nodes->Ranking->Betweeness-centrality->Apply, потом кликом на *Layout* и бирам опцију *No overlap* да се чворови не би преклапали, затим притискам покрени и стоп када добијем жељени изглед графа. Затим притискам болдовано слово **T** да би се на графу приказала имена, и слово A да би та имена подесила по величини тако да буду лакши за посматрање (Слика бр. 15). Тренутно се два чвора највише истичу на овом графу а то су: **abdullapurmetps, beinggrudotcom**



Слика бр 15: Граф са примењеним степеном међусобности и приказаним корисницима без преклапања чворова

Да бих истражила конкретно о чему је реч довољно је да у Твитер претраживач укуцам њихова имена. **@abdullapurmetps** је Abdullapurmet Police Station полицијска станица у Индији која већину својих твитова базира на безбедности својих младих у сајбер и стварном свету, фокусирајући се превасходно на превенцију малолетничког криминала и смањењење конзумирања наркотика. Друга особа је инфлуенцер који је такође из Индије, Hisham Sarwar, који свој садржај пласира младима како би се заштитили у сајбер свету. Половина садржаја ова два налога је на енглеском а друга на хинду језику, што не чини њихову поруку толико лаком за пренети.

Пети корак: Са десне стране на контролној траци бирам: Statistics–>Modularity->Run, да бих могла да добијемо увид у број заједница на који је подељен граф и колика је модуларност у питању. Отвара се прозор који је **Modularity Report**, који указује на то да модуларност износи **0.562** и да је граф подељен у 18 заједница. Затим, са леве стране кликћем на: Partition->Modularity class->Бирам које боје желим-> Apply, ово омогућава да различите групације обојим различитим бојама.



Слика бр. 16: Приказ графа након уклањања чворорова који нису повезани са много других

Затим, опет се враћамо на десну траку и бирамо: Filters -> Topology Folder->Degree range-> превучемо је у оквир испод-> Parameters (Парамтери) и потом нам се појави слајдер. На слајдеру нулу променимо на мало већу вредност, у нашем случају 5. Као резултат можемо приметити да су обрисани они чворови који нису повезани са много других и добијамо чистији изглед графа на којим можемо јасно прочитати доминантне актере тј. чворове у нашем графу (Слика бр. 16).

Шести корак: У горњем десном углу нам се налази *Data Laboratory*. Кликом на тај одељак појавиће се 18 колона, неке од тих колона су Id, Label, User ID, Follower count, User created at, User bio, User location… Ово су све карактеристике одређеног профила на твитеру који анализирам. Од основног идентификационог броја, до тога када су креирали свој твитер профил. У *Data Laboratory* поред дугмета *Nodes* се налази и дугме *Edges* (Слика бр. 17). Кликом на њега показаће се листа ивица. Листа ивица се састоји од извора (енг. Source), назива циљног чвора (енг. Target), типа графа (енг. Type) и идентификационог броја (енг. Id).

Nodes Edges Configuration Add node Add edge Search/Replace Import Spreadsheet Export table More actions Filter: Id

Id	Label	user_id	user_stat...	user_friends_c...	user_followers_...	user_created...	user_bio	user_loca...	user_verified	pr_indegr...	pr_indegree_no...	pr_domain	pr_proximity	pr_rank	pr_rank_min-ma...	In-Degree
n11	a2i_bd	249130848...	5406	4993	19873	2014-05-12 ...	#Banglades...	Dhaka, B...	1	2.0	0.019417	0.019417	0.019417	2.0	0.027027	2
n2	abdullapurmetps	945914862...	2335	77	936	2017-12-27 ...	V.Swamy, In...	Abdullap...		1.0	0.009709	0.009709	0.009709	1.0	0.013514	2
n14	ac1d_apu	290543792...	2887	30	132	2014-11-20 ...	Bangladeshi...	Banglade...		0.0	0.0	0.0	0.0	0.0	0.0	0
n28	anasali62864754	116320820...	2474	180	9	2019-08-18 ...	Data Scienc...			0.0	0.0	0.0	0.0	0.0	0.0	0
n34	aniaani87380741	109979340...	26626	1302	169	2019-02-24 ...	RTs not nec...			0.0	0.0	0.0	0.0	0.0	0.0	0
n88	ansa_zanjbeel	147406922...	290	33	30	2021-12-23 ...				0.0	0.0	0.0	0.0	0.0	0.0	0
n57	aqkhan0012	137253617...	471	53	16	2021-03-18 ...	We are a co...	Sargodha		0.0	0.0	0.0	0.0	0.0	0.0	0
n69	arhamalik2	135902716...	265	240	22	2021-02-09 ...	Student of ...			0.0	0.0	0.0	0.0	0.0	0.0	0
n101	att									1.0	0.009709	0.009709	0.009709	1.0	0.013514	1
n43	awaisaslam354	105640451...	2668	241	321	2018-10-28 ...	loyal to soul.	Pakistan		0.0	0.0	0.0	0.0	0.0	0.0	0
n89	azharmayo3a	151470124...	815	69	5	2022-04-14 ...	Senior Soft...	Wiesbad...		0.0	0.0	0.0	0.0	0.0	0.0	0
n18	baghi__	135040029...	1191	763	808	2021-01-16 ...	CA to be...	Rawalpin...		0.0	0.0	0.0	0.0	0.0	0.0	0
n65	barkhiaahmad	114512932...	96	69	3	2019-06-29 ...	OWNER OF...	Pakistan		0.0	0.0	0.0	0.0	0.0	0.0	0
n15	beinggurudotco...	305180975	17800	945	30689	2011-05-25 ...	Forget who ...	Islamabad		74.0	0.718447	0.718447	0.718447	74.0	1.0	74
n104	bharatdefenders									1.0	0.009709	0.009709	0.009709	1.0	0.013514	1
n78	bilalhussain674	134249107...	52	152	5	2020-12-25 ...	want peace	Punjab, P...		0.0	0.0	0.0	0.0	0.0	0.0	0
n45	bukharim9	109775883...	9469	828	831	2019-02-19 ...	Trying to Pu...	space		0.0	0.0	0.0	0.0	0.0	0.0	0
n103	chdcybercell									1.0	0.009709	0.009709	0.009709	1.0	0.013514	1
n5	crazycoders2	151659613...	1	3		2022-04-19 ...				0.0	0.0	0.0	0.0	0.0	0.0	0
n9	cybersecurityn8	114242403...	1236614	2	27071	2019-06-22 ...	The place f...			0.0	0.0	0.0	0.0	0.0	0.0	0
n102	cybher_security									1.0	0.009709	0.009709	0.009709	1.0	0.013514	1
n93	dakotastate	19363913	5259	300	4172	2009-01-22 ...	Official Twi...	Madison, ...		0.0	0.0	0.0	0.0	0.0	0.0	0
n8	davidbruno_ca	228148440...	8818	478	640	2014-01-07 ...	Cyber Secur...	Canada • ...		2.0	0.019417	0.019417	0.019417	2.0	0.027027	2
n95	dcplbnagar									1.0	0.009709	0.019417	0.012945	1.0	0.013514	1
n25	emkay_digital	142396223...	355	65	15	2021-08-07 ...	Digital Mar...	Pakistan		0.0	0.0	0.0	0.0	0.0	0.0	0
n68	farhanh72634885	142079574	28	16	10	2021-07-29 ...	Graphic des...			0.0	0.0	0.0	0.0	0.0	0.0	0

Слика бр. 17: Приказ Свих података из графа у виду табеле

Седми корак: На врху као трећа картица налази се дугме Preview (енг. Преглед). Кликом на њега појављује се нова картица са менијем где се могу користити све озамишљене опције ради испробавања различитих верзија графа. На самом крају

потребно је да из падајућег менија кликне на сачувај, уколико је потребна промена формата то се може учинити из SVG-а u PDF, и тиме је анализа графа завршена.

Након анализе термина *Сајбер безбедност, Сајбер безбедност (млади)* увиђам да скоро па не постоји разговор о заштити младих на интернету. Коришћењем истих термина на енглеском језику ситуација делује наизлед боља, али не и драстично боља када се узме у обзир број говорника овог језика. Охрабрујућа чињеница након ове анализе јесте појачан дискурс о безбедности на интернету у једном од најбрже растућих технолошких земаља тј. Индији.

Једини помак у Републици Србији када се ради о сајбер безбедности је ационални центар за превенцију безбедносних ризика у ИКТ (информационо-комуникациони систему) системима Републике Србије. Основан је у оквиру Регулаторне агенције за електронске комуникације и поштанске услуге, у складу са Законом о информационој безбедности ("Службени гласник Републике Србије ", број 6/2016, 94/2017и 77/2019). Примарна задужења Националног ЦЕРТ-а су координација превенције и заштите од безбедносних ризика у информационо-комуникационим системима (ИКТ системима) на националном нивоу. На сајту ЦЕРТ-а је могуће пријавити инцидент и попунити формулар. Овакав начин функционисања им је донео доста успеха.

9. Закључак

Друштвене мреже су данас постале нешто сасвим ново и иновативно, сваког трена се мењају и сваке године појављују се нове апликације на нашим мобилним телефонима. Велика опасност на њима изазива различите врсте проблема, од сајбер напада који могу оштетити корисника материјално, до психичког злостављања, крађе идентита и мучења људи понекад и за нешто мало као што је видео или лајк. Држава не ради на томе да законе које поставља у сајбер простору води ка адекватном одговарању на изазове ризика и претње са којима се просечан корисник суочава на дневном нивоу. Овим путем се свако ко крочи на интернет осећа као да је на непознатој територији и што је та особа млађа, то је мање упозната са својим правима и могућностима које може остварити како би се обезбедила онлајн.

Социјалне мреже су моћне по броју корисника који постоје. Но, без обзира на то, истраживање које сам спровела не указује на њихову свемоћ. Анализом друштвених мрежа коришћењем Гефија и Нетлитика дошла сам до закључка да у погледу термина *Сајбер безбедност* разговор није на нивоу на којем се очекује. Постизање промене у добром правцу врши се стављањем акцента на теме сајбер безбедности код младих стварајући свест о реалном проблему данашњице. Подизањем свести код најмлађих постављамо услов за технолошки освешћене генерације које тек треба да дођу.

Дискурс о сајбер безбедности мора да се води у свим правцима, тако што ћемо примарно увести методе образовања деце и младих у школе и тиме побољшати општу свест и безбедност на интернету. Неће постојати дијалога нити побољшања уколико се не призна постојање објективног проблема и легитимне опасности света који се налази иза малих и великих екрана.

10. Литература

1. McCormick, K. (2022, April 23). 6 most popular social media platforms 2022 - unobvious Intel! WordStream. Retrieved May 5, 2022, from https://www.wordstream.com/blog/ws/2022/01/11/most-popular-social-media-platforms
2. Adamic, L. (2012). 1 3 1C Degree and Connected Components 2032. YouTube. YouTube. Retrieved April 15, 2022, from https://www.youtube.com/watch?v=VInwAJ3S44Q&list=LL&index=7&t=586s&ab_channel=OsirisSalazar .
3. Adamic, L. (2012). 3 1 3A degree betweenness closeness 2641. YouTube. YouTube. Retrieved April 10, 2022, from https://www.youtube.com/watch?v=RXohUeNCJiU&list=LL&index=4&ab_channel=OsirisSalazar.
4. Bilal, N., Karakus, M., Varkal, M. D., Boztepe, O., Bilal, B., & Sarica, S. (2016). An assessment of the levels of anxiety and depression in patients with recurrent aphthous stomatitis. Archives of Otolaryngology and Rhinology, 001–005. https://doi.org/10.17352/2455-1759.000011
5. Bilal, N., Karakus, M., Varkal, M. D., Boztepe, O., Bilal, B., & Sarica, S. (2016). An assessment of the levels of anxiety and depression in patients with recurrent aphthous stomatitis. Archives of Otolaryngology and Rhinology, 001–005. https://doi.org/10.17352/2455-1759.000011
6. Boozo Allen Hamilton Inc. (2015). (PDF) The Field Guide to data science - researchgate. Research Gate. Retrieved June 2, 2022, from https://www.researchgate.net/publication/258698880_The_Field_Guide_to_Data_Science
7. Boutin, P. (2009, March 13). Tumblr makes blogging blissfully easy. The New York Times. Retrieved May 20, 2022, from

https://gadgetwise.blogs.nytimes.com/2009/03/13/tumblr-makes-blogging-blissfully-easy/

8. Bubukayr, M. A., & Almaiah, M. A. (2021). Cybersecurity concerns in smart-phones and applications: A survey. 2021 International Conference on Information Technology (ICIT). https://doi.org/10.1109/icit52682.2021.9491691
9. CERT. (2022). Nacionalni Cert Republike Srbije. CERT.RS. Retrieved May 31, 2022, from https://www.cert.rs/
10. Constine, J. (2018, June 21). Instagram hits 1 billion monthly users, up from 800m in September. TechCrunch. Retrieved May 10, 2022, from https://techcrunch.com/2018/06/20/instagram-1-billion-users/
11. Conyers, L., & Kiyuna, A. (2015). Cyberwarfare sourcebook 2015. Lulu.com.
12. Cukierski, W., Herman, M., Kohlwey, E., & Kherloplan, A. (2015). The Field Guide to Data Science. Booz Allen Hamilton.
13. de Laat, M., Lally, V., Lipponen, L., & Simons, R.-J. (2007). Investigating patterns of interaction in networked learning and computer-supported Collaborative Learning: A Role for social network analysis. International Journal of Computer-Supported Collaborative Learning, 2(1), 87–103. https://doi.org/10.1007/s11412-007-9006-4
14. Dennis, M. A. (2022, April 7). Internet. Encyclopædia Britannica. Retrieved April 10, 2022, from https://www.britannica.com/technology/Internet
15. Discord. (2022). What is discord: A guide for parents and educators. Discord. Retrieved May 31, 2022, from https://discord.com/safety/360044149331-What-is-Discord#:~:text=Discord%20is%20a%20free%20voice,homework%20and%20mental%20health%20support.
16. Elker, J. (2021, January 4). World of warcraft experienced a pandemic in 2005. that experience may help coronavirus researchers. The Washington Post. Retrieved May 14, 2022, from https://www.washingtonpost.com/video-

games/2020/04/09/world-warcraft-experienced-pandemic-2005-that-experience-may-help-coronavirus-researchers/

17. FBI. (2014, December 18). Man sentenced to 17 years in federal prison for trying to get teen to perform sexual act over webcam. FBI. Retrieved May 30, 2022, from https://www.fbi.gov/contact-us/field-offices/memphis/news/press-releases/man-sentenced-to-17-years-in-federal-prison-for-trying-to-get-teen-to-perform-sexual-act-over-webcam
18. Fruhlinger, J. (2020, June 19). Ransomware explained: How it works and how to remove it. CSO Online. Retrieved May 30, 2022, from https://www.csoonline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remove-it.html
19. Gephi. (2022). Learn how to use Gephi. graph exploration and manipulation. Retrieved June 2, 2022, from https://gephi.org/users/
20. Goodrow, C. (2017, February 27). You know what's cool? A billion hours. blog.youtube. Retrieved May 31, 2022, from https://blog.youtube/news-and-events/you-know-whats-cool-billion-hours/
21. Governance, I. T. (2022). Cyber security. IT Governance. Retrieved May 15, 2022, from https://www.itgovernance.co.uk/what-is-cybersecurity
22. Hashem, H. (2021, November 8). 13 positive effects of social media on our society today. Kubbco. Retrieved May 30, 2022, from https://www.kubbco.com/13-positive-effects-of-social-media-on-our-society-today/
23. Hawksey, M. (2011). Twitter network analysis and visualisation Ii: NodeXL . hawksey.info/blog. Retrieved June 12, 2022, from https://hawksey.info/blog/2011/09/twitter-network-analysis-and-visualisation-ii-nodexl/.
24. Jitchotvisut, J. (2018, May 11). 8 times crimes were solved by the internet. Insider. Retrieved May 14, 2022, from https://www.insider.com/crimes-solved-by-people-online-2018-5

25. Juma, M., & Shaalan, K. (2020). Online social network analysis for cybersecurity awareness. Studies in Systems, Decision and Control, 585–614. https://doi.org/10.1007/978-3-030-47411-9_32
26. Kim, T. H., & *, N. (2013, December 13). 5 different types of cyberbullying. End Cyber Bullying. Retrieved May 31, 2022, from https://endcyberbullying.org/5-different-types-of-cyberbullying/
27. Kopal, R., Korkut, D., & Krnjašić Saša. (2020). SNA Programska Rješenja. In Analiza (socijalnih) mreža: Praktična Primjena (3rd ed., Vol. 1, pp. 342–353). essay, Algebra.
28. Kumar, S., & Qiu, L. (2021). Social Media Analytics and practical applications, 15–25. https://doi.org/10.1201/9781003196198
29. Lehto, M. (2018). Cyber Security Education and research in the Finland's universities and universities of Applied Sciences. Cyber Security and Threats, 88–179. https://doi.org/10.4018/978-1-5225-5634-3.ch015
30. LinkedIn. (2022). About linkedin. About LinkedIn. Retrieved May 31, 2022, from https://about.linkedin.com/
31. Martin Grandjean. Introduction to Social Network Analysis: Basics and Historical Specificities. HNR+ResHist Conference 2021, Historical Network Research, 2021, Luxembourg, Luxembourg. ff10.5281/zenodo.5083036ff. ffhalshs-03351755f
32. MeetUp. (2022). About. Meetup. Retrieved May 5, 2022, from https://www.meetup.com/about/
33. Meta. (2021, November 23). The Facebook Company is now Meta. Meta. Retrieved May 30, 2022, from https://about.fb.com/news/2021/10/facebook-company-is-now-meta/
34. Mijušković, N. (2021, December 9). Ko Je Jutjuberka Kika (21) Koja Je Izvršila Samoubistvo: Poznata je i Po Skandalu sa Bakom Prasetom (video). 24sedam. Retrieved May 5, 2022, from https://24sedam.rs/showbiz/vesti/96192/ko-je-

jutjuberka-kika-21-koja-je-izvrsila-samoubistvo-poznata-je-i-po-skandalu-sa-bakom-prasetom-video/vest

35. Moody, J. (2018). Example of visualizing communities in collaboration network . mrvar.fdv.uni-lj.si. Retrieved June 12, 2022, from http://mrvar.fdv.uni-lj.si/pajek/be3.htm.
36. Molloy, F. (2008, March 27). Internet connectivity. ABC (Australian Broadcasting Corporation). Retrieved May 15, 2022, from https://www.abc.net.au/science/articles/2008/03/27/2199691.htm
37. NBC. (2006, October 9). Google buys YouTube for $1.65 billion. NBCNews.com. Retrieved May 31, 2022, from https://www.nbcnews.com/id/wbna15196982
38. Netlytic. (2022). About. Netlyticorg. Retrieved June 2, 2022, from https://netlytic.org/home/?page_id=10834
39. Noakes, T., & Noakes, T. (2021, February 24). Distinguishing online academic bullying: Identifying new forms of harassment in a dissenting emeritus professor's case. Heliyon. Retrieved May 31, 2022, from https://www.sciencedirect.com/science/article/pii/S240584402100431X
40. Norton, C. (2021, December 16). 7 professional networking alternatives to linkedin. PR Daily. Retrieved May 8, 2022, from https://www.prdaily.com/7-professional-networking-alternatives-to-linkedin/
41. Reshmi, T. R. (2021). Information security breaches due to ransomware attacks - A systematic literature review. International Journal of Information Management Data Insights, 1(2), 100013. https://doi.org/10.1016/j.jjimei.2021.100013
42. Reshmi, T. R. (2021). Information security breaches due to ransomware attacks - A systematic literature review. International Journal of Information Management Data Insights, 1(2), 1–8. https://doi.org/10.1016/j.jjimei.2021.100013
43. Securly, /. (2019, December 4). The 10 types of cyberbullying. Blog. Retrieved May 31, 2022, from https://blog.securly.com/10/04/2018/the-10-types-of-cyberbullying/

44. Siddiqui, S., & Singh, T. (2016). Social media its impact with positive and negative aspects. International Journal of Computer Applications Technology and Research, 5(2), 71–75. https://doi.org/10.7753/ijcatr0502.1006
45. Sponder, M., & Khan, G. F. (2018). Digital Analytics for marketing. Routledge.
46. Team, T. I. (2022, May 21). Web 2.0 and web 3.0 definitions. Investopedia. Retrieved May 30, 2022, from https://www.investopedia.com/web-20-web-30-5208698#toc-the-bottom-line
47. Weng, R. (2020). Network graph of characters in A Midsummer Night's Dream. Retrieved June 12, 2022, from https://towardsdatascience.com/tutorial-network-visualization-basics-with-networkx-and-plotly-and-a-little-nlp-57c9bbb55bb9.
48. Williams, P. A., & McCauley, V. (2016). Always connected: The security challenges of the Healthcare Internet of Things. 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT). https://doi.org/10.1109/wf-iot.2016.7845455
49. Xing. (2022). Impressum. Zur XING Startseite. Retrieved May 31, 2022, from https://www.xing.com/legalnotice
50. Youtube. (2022). About YouTube. YouTube. Retrieved May 31, 2022, from https://about.youtube/
51. Zhang, M. (2010). Social network analysis: History, concepts, and research. In Handbook of social network technologies and applications (pp. 3-21). Springer, Boston, MA.
52. Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2020). Cyber Security Awareness, knowledge and behavior: A comparative study. Journal of Computer Information Systems, 62(1), 82–97. https://doi.org/10.1080/08874417.2020.1712269
53. Ковачевић, др М., Шутић, В., Рајчевић, У., & Миланковић, А. (2020, September 22). Употреба информационо–комуникационих технологија у

Републици Србији, 2020. Република Србија Републички завод за статистику. Retrieved April 10, 2022, from https://www.stat.gov.rs/publikacije/

54. Ковачевић, др. М., Шутић, В., & Рајчевић, У. (2021, October 22). Употреба информационо-комуникационих технологија у Републици Србији, 2021. Публикације | Републички завод за статистику Србије. Retrieved May 1, 2022, from https://www.stat.gov.rs/publikacije/
55. Крстарица. (2018, July 2). Menadžment. Krstarica. Retrieved May 10, 2022, from https://www.krstarica.com/info/menadzment/