UDK 323.28:004(100)

ВИРТУЕЛНА ЗАКАНА ИЛИ РЕАЛНА ОПАСНОСТ-САЈБЕР ТЕРОРИЗМОТ НИЗ ПРИЗМАТА НА НАЈЕКСПОНИРАНИТЕ CASE STUDIES

М-р Наташа Донева
Асистент на Правен факултет, Универзитет "Гоце Делчев"-Штип
E-mail: natedoneva3@gmail.com

Апстракт
Мистеријата наречена сајбер тероризам и те како е интересна за следење со оглед на фактот дека е динамична, постојано се модифицира, се менуваат појавните облици, се менува modus operandi, се продира во сфери и области кои се од круцијално значење за опстанокот на самите држави... Се злоупотребува информатичкиот изум за започнување на нови бескрупулозни војни, за ширење ксенофобични пораки, за крадење парични средстава, за крадење на берзанските тајни, за инсајдерски информации.... Речиси и да нема крај на енормната листа на полиња на продор, проблеми кои не се започнати токму со овој вид модерен криминал. Потребата од негово сузбивање и те како е алармантна и бара меѓународна соработка и помош, за резултати кои иако нема да бидат утописти чки, барем ќе се задоволителни.
Чудно но материјата за сајбер криминалот и тероризмот иако присутна во сите држави, сепак различно е регулирана. Што значи различни држави имаат различен систем на регулирање и справување со оваа материја, но и различни законски инкриминаации. Затоа се донесени плејада на меѓународни документи преку кои светот се обидува да се заштити од сајбер криминалот и сајбер тероризмот. Но дали нивната имплементација на државно ниво е толку успешна колку што се очекува. Дали постои документ со интернационална сила и глобално значење, на кој сите држави би му се "покориле" за да се заштитат од дигиталниот тероризам?
Овој труд ќе ги спомене најекспонираните сајбер напади, анализирајќи ги преку case studies, но неминовно мора да ја отвориме темата за (не)постоењето на адекватна законска регулатива која сеопфатно ќе ја инкриминира новата глобална виртуелна проблематика. Дали е потребна Дигитална Женевска Конвенција, и што всушност би претставувала истата?

Клучни зборови: *меѓународен криминал, законски инкриминации, хакери, сајбер напади, ...*

VIRTUAL THREAT OR REAL DANGER - CYBER TERRORISM THROUGH THE PRISM OF THE MOST EXPOSED CASE STUDIES

Natasa Doneva, MA
Assistant at the Faculty of Law, University "Goce Delcev" - Stip
E-mail: natedoneva3@gmail.com

Abstract:
The mystery called cyber terrorism is far than just interesting to follow given the fact that it is dynamic, constantly modifies, changes the appearance forms, changes modus operandi, penetrates into areas that are crucial for the survival of the states themselves. The

information invention is being abused for launching new unscrupulous wars, spreading xenophobic messages, stealing money, stealing stock exchanges, insider information ... Almost no end to the enormous list of fields of penetration, problems started right with this kind of modern crime. The need for its prevention and the requirement of international cooperation and assistance, is more than alarming and needet for results that, although not utopian, will at least be satisfactory.

Strangely, the issue of cyber crime and terrorism, although present in all countries, is still regulated differently. Which means different countries have a different system of regulation for dealing with this matter, as well as different legal incriminations. That's why a significant number of international documents had been adopted, and through them the world is trying to protect itself from cybercrime and cyber terrorism. But is their implementation at the state level as successful as expected? Is there a document with international force and global significance, in which all states would "be subdued" to protect themselves from digital terrorism?

This paper will mention the most exposed cyber attacks, analyzing them through case studies, but inevitably we must open the topic of the (non) existence of adequate legislation that will incriminate the new global virtual problem. Do we need a Digital Geneva Convention, and what would it actually mean?
Keywords: international crime, legal incriminations, hackers, cyber attacks, conventions ...

Вовед

Кога се споменува терминот “сајбер”-дијапазонот на работи на коишто може да се однесува е енормен. Така може да зборуваме за сајбер криминал, сајбер тероризам, сајбер уценување[1], сајбер простор...Најчести дилеми разбрануваат сајбер криминалот и сајбер тероризмот[2]. Иако голем број на автори ги сместуваат во исти кош овие два поима, сепак има огромна разлика меѓу нив. Истите имаат една работа што ги поврзува – компјутер претставен како оружје за извршување на кривичните дела. Додека сајбер криминалот најчесто хакерите го прават заради финансиска корист, забава, или меѓусебен натпревар, сајбер тероризмот е секогаш политички мотивиран. Сајбер криминалот се однесува на online или нелегални активности на интернет, додека сајбер терористите маркираат мети како нафтени, електрични компании, транспортни инфраструктури и нивните системи...Најчесто сајбер терористите имаат тим од компјутерски гении, години поминати во планирање на напади, финансии со кои ги реализираат нападите.

“Терористот е благороден, страшен, неодоливо фасинантен бидејќи во себе тој ги комбинира двата недостижни врва на човековата големина-маченикот и јунакот. Од денот кога се заколнал, од се срце да го ослободи својот народ и татковина, знае дека смртта му е судбина”- Сергеј Степњак Кравчински/ Илегалната Русија (1863).

[1] https://anydifferencebetween.com/difference-between-cyberterrorism-and-cyberextortion/. Сајбер уценувањето се врши преку е маил пораки во кој криминалците се заканuваат дека ќе објават, уништат доверливи информации, доколку жртвите не платата одредена сума на пари.

[2] https://anydifferencebetween.com/difference-between-cybercrime-and-cyberterrorism/ .

Terrere на латински растреперува. Корените на тероризмот[3] потекнуваат токму од тука. Се вели теророт, тероризмот во првобитна форма, датира од праисторијата. Дури и првата империја во Месопотамија се темелела на истиот. А во денешен облик , и во мирновременски услови е меч кој виси над секоја глава која ќе се крене.Тероризмот е најнасилниот облик на психолошка војна . Ако се погледне ретроактивно ќе се примети широкиот спектар на облици и трансформации што истиот ги прави. Сепак идеологијата е онаа што останало исто. Ако и примарните форми на тероризмот предизвикуваа катастрофални последици и репрекусии, тогаш што се предвидува со доаѓањето на сајбер тероризмот?

Сајбер просторот всушност не е природна туку човечка креација,кој иако своевремено бил осмислен за подобрување на животниот стандарт на човекот и ширење на милионски опции за искористување на технологијата како алатка за подобро живеење, сепак доживува илузорност. Парадоксот се состои во Тоа што човечки изум, се искористи и злоупотреби како оружје против човечноста. Можеби изгледа како преувеличување, но таргетот и позадината при употреба на сајбер тероризмот, имаат мошне немилосрдни цели кои повлекуваат невини жртви.

Денеска често ќе се сретнат полемики, несогласувања, контрадикторни ставови поврзани токму со овој стар феномен, кој добива ново руво. Имено низа автори сметаа дека доаѓа до "преувеличување" на стравот од сајбер тероризмот, дека медиумите и научната фантастика придонесуваат во обликување на погрешна претстава за истиот. За среќа многу е поголема редицата на експерти кои приложуваат издржани факти и аргументи против сајбер тероризмот. Не е воопшто наивна игра користењето на компјутер за да се навлезе во компјутерски системи, безбедносни мрежи, државни инфраструктуи, персонални компјутери, за да се изврши кражба или модификација на податоци, 'инкогнито" да се следи нечија активност, да се шпионира или саботира... Без разлика дали нападот е проследен од организација, група хакери, државни/владини структури-последиците сепак ќе бидат исти, катастрофални за сите. Директно или индиректно репрекусии ќе претрпат дузина различни профили на стопански организации, финансиски институции, безбедносни државни сегменти и што е најважно човечки жртви...

Доколку досега се војуваше но доменот на воздухот, копното, водата и вселената, сега војната се прошири и во сајбер просторот. Сајбер нападите од година во година стануваат се пософистицирани и поспецифични. Пример во 2008 година сајбер нападите од персоналните компјутери се префрлија на државните институции. НАСА потврдила откривање на црв помеѓу лаптопите на интернационалната вселенска станица, а подоцна биле хакирани и компјутерите на Пентагон. Понатаму на ред биле и фаинансиски институции како The state bank of India- која 2008 година била мета на хакери лоцирани во Пакистан.

Примери:

- Во 1997 година ИРА ја фрапирала јавноста со транспарентното упатување закани дека ќе почне да користи електронски напади на службените и владини компјутерски системи.

[3] Подетално за историјата на тероризмот: Шалијан Ж, Блин А, Историја на тероризмот,Табернакул 2009

- Во 1988 година, терористичката герилска организација ги преплавила амбасадите на Шри Ланка со 800 e-mail-ови на ден. Пораката била "Ние сме Интернет" "Црни тигри" и ова е се со цел да ги попречиме вашите комуникации.
- Интернет саботери, 1998 година ја обезличија Web-страната на индискиот "Bhabha" центар за атомско истражување, при што украле електронска пошта.
- Палестинско-иразелската сајбер војна од 2000 година искористиле DoS алатки за да го нападнат најголемиот снабдувач на Интернет услуги "Netvision".

Во следнава табела се прикажани едни од поекспонираните и познати напади врз националната инфраструктура и безбедност[4].

Година	Напаѓач	Цел	Последици
1982	САД-ЦИА	Логичка бомба насочена кон гасоводот на СССР во Сибир	Деструкција
1999/2000	Русија	Пентагон, НАСА, Национална лабораторија	Крадење информации и шпионажа
2007	Кина	Компјутерска мрежа на САД	Одбивање на услуга
2008	Непознато	Воена мрежа на САД	Злонамерен код/зомби машина
2008	Русија	Веб сајтови на Владата и др институции во Грузија	Одбивање на услуга
2010/2011	Непознато	Иранski објект за збогатување на ураниум	Саботажа

2001 та година меѓудругото ја одбележало и тензичната сајбер војна помеѓу Кина и САД . Причината била судирот на кинески авион со американски шпионски авион. Првите напади ги упатиле кинеските хакери, кои не направиле значителни штети, но настрадала страницата на Американскиот конгрес. Додека американските хакери ги таргетирале веб страните на властите во покраини во КИна, но и оние на корејските компании Samsung I Daewoo Telecoma.

Во 2008 година група хакери наречени "Greek Security Team" упаднале во компјутерите на CERN – Европскиот центар за нуклеарни истражувања, што за малку не ја презеле контролата врз еден од детекторите LHC – најголемиот ахцелератор на честици. Уште пострашно е што хакерите во системот провалиле уште првиот ден од експерментот и поставиле лажна страница на сајтот на CERN. Со што иако не предизвикале енорми штети, доволно било што покажеле дека електронската заштитата на институциите од ваков калибар е на "стаклени нозе".

[4] Повеќе: М.Богданоски, М.Богданоски, Е.Николов, Д.Петревски, Сајбер нападите како најсовремена закана за воените операции и критичната инфраструктура, MILCON, Скопје, 2012

Во 2010 година била создадена малициозната програма Stuxnet која ги заразила SCADA апарати на Сименс кои ги контролираат нафтоводите, електричната, нуклеарната и другите индустриски потенцијали во Иран, преку инфицирање на најмалку 30.000 компјутери ширум светот.

2. "Интерна" класификација на сајбер нападите

Честопати се врши еден вид "интерна" класификација на сајбер нападите:

- ✓ **Неселективни напади-Indiscriminate attacks**- овие напади се на глобално ниво и се напади кои не бираат дали метата е држава или компанија. Пример за ваков напад е Operation Shady RAT[5] , Red October[6], 2017 Petya cyber attack[7]…
- ✓ **Деструктивни напади-Destructive attacks-** се напади кои имаат за цел да нанесат штета. Пример за овој тип напад се LulzRaft, TV5Monde[8], Stuxnet, Operation Ababil, Shamoon…
- ✓ **Cyberwarfare** –се политички мотивирани напади кои целат меѓудругото и за саботажа и шпионажа. Пример за овој вид напади се: нападот во Естонија-2007 година, нападот во Бурма-2010 година[9], сајбер војна помеѓу Јапонија/Јужна Кореја[10], нападите во текот на Руско-Грузиска војна, Opeartion Olympic Games, Opisrael, Singapore cyberattacks...
- ✓ **Државна шпионажа-Government espionage-** овие напади се насочени за кражба на информации од државни организации. Пример за овие напади се: GhostNet[11], Operation Newscaster[12], Titan Rain, Cyber attack during the G20 Summit , Operation Cleaver…
- ✓ **Корпоративна шпионажа-Corporate espionage-** овие напади целат на кражба од корпорации поврзани со права од индустриска сопственост. Пример за овие напади се: Operation Aurora[13], Operation Socialist, Sony Pictures Entertainment hack,IEEE…
- ✓ **Кражба на e-mail адреси –**овие напади се однесуваат на кражба на e mail адреси на специфични веб сајтови. Пример за овие напади се: RockYou, Adobe[14], Yahoo…

[5] Operation Shady RAT-серија на сајбер напади започнати 2006 година.Од овој напад погодени биле најмалку 71 организација, ОН и Интернационалниот Олимписки комитет.

[6] Подетално: https://www.computerworld.com/article/2474163/cybercrime-hacking/red-october-5-year-cyber-espionage-attack--malware-resurrects-itself.html

[7] Petya е фамилија на енкриптирани малциозни софтвери, откриени 2016 година.

[8] Овие напади се случиле 2015 година кога бил нападнат францускиот сервис TV5Monde од малциозен софтвер.

[9] Сајбер нападите во Бурма се одвивале пред изборите во 2010 година, преку користење DDoS напади.

[10] Војната инволвирала јапонски интернет форум (2channel) и корејски веб сајт. Истата се одвивала во 2010 година.

[11] GhostNet -е името на една од најголемите операции за сајбер шпионажа откриена во 2009 година.

[12] Operation Newscaster- сајбер шпионажа која користи социјално вмрежување.

[13] Operation Aurora- серија сајбер напади, прво јавно објавени од Google, а започнати 2009 година. Нападите биле наменети за десетици организации.

[14] Во 2013 година хакери влегле во мрежата на Adobe украле информации за корисниците, со што биле оштетени над 150 милиони потрошувачи.

- ✓ **<u>Кражба на кредитни картички и финансиски податоци-</u>** Пример за овие напади се: 2017 Equifax data breach[15], Goodwill Industries, Subway[16]…

Сајбер тероризмот поради неговата мултидимензионалност, метаморфози, и те како ја отежнува унитарноста при неговото дефинирање. Имено не може да се пронајде само една единствена дефиниција која ќе го постави овој поим во правна рамка.

Иако постојат низа на "мети" на кој тактизираат и играат сајбер терористите, сепак една слаба точка, или "ахиловата пета" е токму националната инфраструктура на државите. На оваа поле не постои разлика меѓу економски развиени/неразвиени држави, земји во транзиција, општествено моќни/слаби... Сите подеднакво "себично" ја чуваат својата инфраструктура, потенцирајќи ја енормната важност што истата ја има за целокупниот опстаок и нормалното функционирање на земјите. Истата е еквилибриум помеѓу националната безбедност, економијата, индустријата, здравјето на граѓаните... За граѓаните тоа е синоним за водата, електричната енергија, транспортот, комуникациските системи... За државите тоа е еквивалент на средствата, системите и мрежите, било да се физички или виртуелни, кои се од витално значење за државата (производство, пренос и дистрибуција на електрична енергија, гасот, нафтата и нафтените производи, водоводната мрежа, насипи, брани, замјоделството, производство и дистрибуција на храна, владините институции, транспортен систем, финансиските институции, телекомуникациите, јавното здравје, одбранбените механизми, хардвер, софтвер...).Нарушеното делување на само еден од овие сектори, влијае директно и индиректно на речиси сите останати, доведувајќи до колапс, или дестабилизирање на самата држава. Така само еден компјутерски вирус може да ја прекине дистрибуцијата на природен гас во целиот регион. Последователно оваа влијае врз намалувањето на електричната енергија, што пак своето влијание го пренесува врз престанок на компјутеризираните контролни единици и комуникации. Свои репрекусии ќе претрпат и патниот, воздушен и железнички сообраќај, како и работата на службите за итна помош.

Затоа секоја држава мора да ја штити својата национална критична инфраструктура. Потребно е да се поседува стратешки план за превенција, брзо реагирање и отстранување на последиците од евентуален напад, и "back up" план за враќање во нормален тек на нападнатата инфраструктура. Сето тоа значи добра проценка на реалната слика на сите недостатоци што ги има државата, не само од виртуелен туку посебно од сајбер напад, понатаму редуцирање или целосно анулирање на таквите недостатоци, развивање и етаблирање на системи на идентификација и спречување на потенцијалните напади, оспособување на посебни системи за навремена сигнализација, алармирање за веќе нападнат систем, "отстранување" на нападот и санирање на нанесените последици. Оваа комплицирана, испреплетена мрежа на одбрана, како што изгледа на прв поглед, всушност е нужна потреба во денешно време. Финансиските средства и времето потрошени за создавање на ваква ефикасна мрежа не може да се

[15] Equifax во 2017 година објавиле дека биле жртви на сајбер напади, каде што сајбер криминалците добиле пристап на над 140 милиони клиенти, на кои им биле откриени и социјални броеви, броеви на кредитни картички.

[16] Во 2012 година, во интернационален заговор биле хакирани терминали за плаќање на над 150 франшизи за Subway ресторани.

компарираат со вредноста на доброто што се штити. Бидејќи опстанокот на државата, нејзините витални органи, и безбедноста на граѓаните нема цена.
Овој вид на заштита ја карактеризира сајбер безбедноста, каде се обезбедува заштита на средствата што вклучуваат податоци, компјутерите, серверите, зградите, објектите, но пред се луѓето.
Сајбер тероризмот е многу тежок за детектирање, пред се затоа што е речиси невозможно да се одреди почитичката пропадност или спонзорите на неговите извршители. Постои само невидлив непријател кој е навидум слабо наоружан, само со еден персонален компјутер. Но еден гениј на компјутер е посилен од многубројните армии на државите. Истиот со дигитални кодови, "информатички јазик", електронски новини атакува државни информациски мрежи, менува цели национални државни заштитени програми, инфилтрира штетни "црви" кој ја уништуваат унитарноста и ја слабеат целата држава.
Според ФБИ овој феномен наречен сајбер тероризам кој зазема инвазија со рапидна брзина е: "***предумислени, политички мотивирани напди против информации, компјутерските системи, компјутерските програми и податоци што резултираат со насилство против цели кои не се воени од стана на суб националните групи или тајни агенти."*** Според истите, сајбер нападите се трети по ред најопасни закани, кои следат веднаш по нуклеарната војна и оружјето за масовно уништување.

Еден од повпечатливите и експонирани сајбер напади се случил во 1999 година за време на интервенцијата на НАТО и бомбандирањето на Србија. Бројни просрпски хакерски групи реагирале врз интервенцијата на алијансата , при што ја нападнале интернет-инфраструктурата на НАТО. По бомбандирањето на кинеската амбасада во Белград од старана на САД и кинеските хакери се вклучиле во конфликтот. Бројните хакерски напади создале море од испратени "мејлови" кои ја парализирале секојдневната комуникација на НАТО, по што неколку дена не можела ниту да се користи нивната официјалната веб страница. Истовремено на неколку веб страници на земјите членки на НАТО биле нападнати со пораки за прекин на воената операција.Целта на хакерите за прекин на војната не успеала, но им се дало до знаење на големите воени сили дека не се безбедни, ниту електронски добро покриени.

2.1 Сајбер напад врз информациско –комуникациската инфраструктура на Естонија.[17]

Овој случај вклучува серија сајбер напади кои започнале во 2007 година. Истите ги таргетирале информацико комуникациските системи на Естонскиот Парламент, банките, министерствата,медиумите... со што се атакувало врз речиси сите витални институции во државата и се обезбедило нејзино дестабилизирање. НАТО застанал во поддршка на Естонија и затоа токму во Талин се наоѓа НАТО Кооперативниот центар за сајбер одбрана, која е најистакната институција за истражување и обука, која се занимава со образование, консултации, размена на лекции и развој во врска со сајбер одбраната. Од 2008 година НАТО ја објавиле својата прва политика за одбрана од сајбер

[17] Повеќе: Ј Ачкоски, Сигурноста на компјутерските системи, компјутерски криминал и компјутерски тероризам, Скопје, 2012.

нападите. Меѓудругото алијансата ја донела контроверзната повелба од Талин[18], напишана од интернционална група од околу дваесетина експерти и публикувана во 2013 година од Cambridge University Press, со која се наметнува прашањето дали и врз сајбер криминалот важат одредбите за меѓународното химанитарно и воено право? Кои сајбер операции можат да се квалификуваат како вооружен напад, кога државите можат да реагираат во самоодбрана? Потоа во 2017 година била донесена Tallinn 2.0[19] повелбата.

Всушност сајбер нападите, можат да се појават како резултат на веќе постоечки физички напад/ војна/ конфликт, или пак да се одвиваат паралелно со истиот.

Така во 2008 година се појави **Руско-Грузискиот конфликт.** Имено регионот Абхазија и Јужна Осетија меѓународно правно и припаѓаат на Грузија, но де факто се самостојни и под заштита на Русија[20]. Откако ескалираа односите помеѓу овие две држави, на сцената настапи и сајбер војната, која се одвиваше паралелно со физичката. Имено Грузиската влада ја обвинувала Русија за неовластено навлегување во компјутерските системи на витални владини сајтови и нивно исклучување. Исто така обвинението се однесуваа на руските хакери кои наводно ја "заземале" страната на Министерството за надворешни работи и други круцијални институционални страни, со што Грузија била оневозможена да го известува светот за кулминацијата на војната. Поради тоа Грузиската влада била принудена да почне да го користи јавниот сервис на Google , за да може да создаде свој блог, преку кој ќе ја известува јавноста и медиумите.

Иако кај сајбер тероризмот нема класични напади како кај "стариот тероризам", сепак последиците од новиот тероризам се можеби далеку поопасни и безмилосни, бидејќи индиректно се врши експанзија на штетите. Така напад на компјутерскиот систем на аеродром ќе направи огромни последици во управувањето на летовите, неправилно давање команди за слетување, што пак може да предизвика пад на авиони и големи материјални и човечки жртви. Се калкулира дека се повеќе напади во иднина ќе го имаат обележјето токму на сајбер тероризмот.

Центарот за стратегиски и меѓународни студии го дефинира овој поим како " ***употреба на компјутерски мрежни средства за напад или уништување на националните инфраструктури (пример: енергетски, транспортни владини капацитети) или да ја принудат и заплашат владата или цивилното население***", или "***сајбер тероризам е криминален акт извршен врз компјутер пришто е предизвикано насилство, смрт и/ или деструкција, создавајќи терор поради убедување на Владата да ја промени политиката.***

Идеално би било на одреден временски период да се прават истражувања кои ќе покажат како еволуираат сајбер таргетите. Дали остануваат исти, или пак со текот на времето, се појавуваат нови области, кои стануваат поинтересни за таргетирање. Секако клучни секогаш биле и ќе останат финансиските и државни институции-бидејќи се ризница на национални, безбедносни и материјални податоци. На ранг листата веднаш потоа би ги сместиле институциите/објектите за нафта, гас, водоснабдување,електрична

[18] Повеќе: https://ccdcoe.org/tallinn-manual.html

[19] Повеќе: https://ccdcoe.org/tallinn-manual-20-international-law-applicable-cyber-operations-be-launched.html

[20] Абхазија и Јужна Осетија и припаѓаа на Грузија, но по распадот на Советскиот Сојуз, и по граѓанските војни , тие се отцепија од Грузија. Русија ја признала независноста на Абхазија и Јужна Осетија во август 2008 година.

енергија-бидејќи без нивно функционирање државата ќе стане аномична и дисфункционална.

3. Case studies

3.1 CASE STUDY: PETYA / NOTPETYA

Petya е рансомер т.е уценувачки софтвер или еден од многуте видови на штетен софтвер, кој го инфицира таргетираниот компјутер, енкриптира податоци, притоа и дава на жртвата порака објаснувајќи и како може да плате на Bitcoin[21] за да го добие клучот за рекуперација, т.е враќање на хакираните податоци. Името Petya е добиено од култниот серијал за тајниот агент Џејмс Бонд-"GoldenEye" , каде Petya е еден од двата советски оружја-сателити кои носат GoldenEye – атомска бомба. Оваа семејство на штетен енкриптиран софтвер прв пат бил нотиран во 2016 година, како малциозен софтвер кој ги напаѓа само и исклучиво системите на Microsoft Windows.

Патот до целосна имплементација на Petya се одвива низ неколку фази. Прво овој софтвер се прикачувал зад наводен е маил за аплиакција за работа и pdf документ на кој откако жртвата ќе кликне се активира и почнува "операцијата" на штетниот софтвер. Истиот го окупира хардискот и сите информации на него а за понатамошно негово "ослободување" и декриптирање бара плаќање на биткоин.

Во 2017 година се појавила нова верзија на Petya, која брзо го добила името NotPetya . Првите мети биле стационирани во Украина, но за кратко време ја зазеле речиси цела Европа. Се проценува дека биле инфицирани 12.500 машини во над 64 држави само во првиот ден на детектирање. Рапидно и сигурно биле нападнати компании и институции во Источна Европа, како банки и финансиски центри, областите на енергијата...Притоа оваа нова верзија рапидно ги инфицирала и заземала компјуерите и мрежите без "класичните методи на старата Petya". Така новиот малциозен софтвер се ширел без барање и е маилови. Поради тоа постојат неколку парметри кој помагаат за дистинцирање на овие фракции од ист штетен софтвер.

- Not Petya се шири самостојно, за разлика од Petya која бара "одобрување" преку кликање на емаил со инфициран софтвер.
- NotPetya енкриптира се, за разлика од Petya кој претежно енкриптира првично само одреден дел од хардискот.
- NotPetya иако многу сличен сепак не е класичен малциозен софтвер, што можеби е најилузорната, контрадикторна информација. Имено иако и овде пристигнува порака за плаќање бикоин, за декрипција на податоците, сепак постои разлика. Така кај Petya постои посебен код благодарение на кои се дознава која жртва платила биткоин. Додека кај NotPetya овој код е речиси ирелевантен при понатамошна идентификација. Затоа многумина претпоставуваат дека целта на NotPetya е многу посложена од очекуваното. Наводната интенција е да собере информации од сајбер агенции и релевантни институции слични на нив.

[21] Bitcoin е платежен систем кој се појавува во 2009 година. Уште е познат како дигитална/виртуелна/криптовалута или електронски пари. Биткоинот не е регулиран од никаков ентитет-како Централна Банка или слично и затоа е синоним за децентрализирана валута.

3.2 CASE STUDY: WANNA CRY ATTACK

Wanna Cry е малциозен црв кој делува многу слично на штетниот софтвер Petya. Идентичноста е во тоа што и wanna cry ги напаѓа windows системите, ги енкриптира податоците и за нивно декриптирање бара плаќање биткоин. Но сепак овде станува збор за мрежен црв бидејќи вклучува транспортен механизам кој му овозможува сам да се репродуцира и самостојно да се шири. Овие напади започнале во 2017 година, каде првата "зараза" е маркирана во Азија.За само еден ден се проценува дека биле инфицирани на над 230.000 компјутери во 150 држави.

3.3 CASE STUDY: UKRENEGRO/ UKRAINIAN BLACKOUT

Во декември 2016 година Украинскиот дистрибутер на енергија Ukrenergo претрпел сајбер напад кој довел до краток прекин на енергија во Киев и блиските реони. Им било потребно еден час за да се врати енергијата во нормала.овој напад бил изведен со помош на сајбер влијанието, т.е штетен софтвер кој ја презел контролата врз системите.

3.4 CASE STUDY: STUXNET

Stuxnet е штетен компјутерски црв откриен 2010 година, со презумпција дека е развиван од 2005 година наводно од страна на Америка и Израел, со примарна цел и таргет-Иранската нуклеарна програма[22]. Повеќе медиумски извештаии сугерираат дека Staxnet бил наменет да го саботира објектот за збогатување на ураниум во Натанз[23]. Штетите настанати во Нантанз во почетокот не можеле да укажат на вистинскиот проблем, се додека не била побарана помош од експерти кои го детектирале вирусот Stuxnet во иранската нуклеарна мрежа.

3.5 CASE STUDY: OPERATION BUGDROP

Операцијата BugDrop е сајбер напад кој има за цел да навлезе во критичната инфраструктура, медиумите и научните истражувања. Интенцијата е да се соберат чувствителни информации од "метите" вклучувајќи снимени разговори, screen shots, документи, пасворди... Поголемиот дел од таргетите се сместени во Украина, Русија, помал број во Австрија и Саудиска Арабија.

Метите на оваа операција пред се се компании за нафта и гас,интернационални организации кои вршат надзор на човековите права, тероризам и сајбер нападите, инжинерски компании кои дизајнираат електрани, дистрибуција на гас, снабдување на вода, научните истражувачки центри... Операцијата ги заразува жртвите преку т.н phishing напад.

[22] http://large.stanford.edu/courses/2015/ph241/holloway1/

[23] Натанз е град во Иран,најпознат по неговото обележје-индустриски комплекс за преработка т.е збогатување на ураниум. Според Меѓународната агенција за атомска енергија од 2012 година збогатено е вкупно 6876 кг ураниум хексафлуороид.

3.6 CASE STUDY: TV5 MONDE CYBER ATTACK

TV5 Monde е глобална телевизиска мрежа, која во 2015 година беше жртва на сајбер напад, изведен од хакерска група позната како CyberCaliphate. Истите успеале да навлезат во внатрешните системи, со што три часа целосно ги превземале. Дури ни наредниот ден TV5 Monde не успеале целосно да ги вратат работите во свои раце.Хакирани биле и "Facebook" и " Twitter" мрежите на телевизијата. За француските власти сајбер нападот бил напад врз слободата на изразување и слободата на информирање.

3.7 CASE STUDY: SHAMOON

Shamoon уште попознат како W32.DisTrack е компјутерски вирус откриен 2012 година. Истиот отстапува од "класичните" однесувања на останатите вируси поради неговата унишsувачка природа, времетрањето и цената потребни за рекуперација на оштетениот и нападнат компјутер. Вирусот се шири многу брзо, окупирајќи го целиот систем и крадејќи специфични информации кои ги дава на напаѓачите а потоа ги брише. Со овој вирус се нападнати националните нафтени компании на Саудиска Арабија-Saudi Aramco и Катарскиот RasGAs.

3.8 CASE STUDY: LULZRAFT

LulzRaft е името на хакерска група која во 2011 година проследија серија напади врз веб страните на Канадската конзервативна партија и Канадската енергетска компанија Husky Energy. Првиот напад врз конзервативната партија се однесувал на лажна вест за здравјето на канадскиот министер, која ја постирале на веб страната откако ја хакирале. Вториот напад врз оваа конзервативна партија се однесува на хакирање и разоткривање на личните информации на донаторите на партијата. Притоа хакерската група се исмејала на безбедносната заштита, потенцирајчи дека ја уништиле користејќи базични, лесни методи. Исто така ја хакирале,окупирале страната на Husky Energy,објавувајќи дека одреден број корисници ќе добијат бесплатен гас, доколку користат одреден код...

3.9 CASE STUDY: RED OCTOBER

Red October е малциозен програм за сајбер шпионажа откриен во Октомври 2012 година, но со претпоставка дека неколку години наназад успешно ја вршел својата задача незабележано. Целта на операцијата била снимање на дипломатски тајни па дури и лични информации, кои се добивале од сите уреди, па и од мобилните телефони.

3.10 CASE STUDY: SONY PICTURES HACK

Guardian of peace е псевдоминот под кои група хакери објавиле низа заштитени податоци од познатото филмско студио Sony pictures[24]. Помеѓу хакираните информаци се објавиле податоци за вработените, нивните семејства, е маилови, копии од необјавени филмови на Sony. Оваа хакерска група барала од компанијата да не го репродуцира

[24] https://oag.ca.gov/system/files/12%2008%2014%20letter_0.pdf

филмот the interview комедија за атентат над северно корејскиот лидер. Оваа барање се третирало многу сериозно бидејќи заканите се однесувале на терористички напад во кината каде евентуално би се прикажувал филмот[25]. Sony ја откажала премиерата на овој филм и дозволила само негов dounload. Иако многумина хакерската група ја поврзале со Северна Кореја истата целосно негирала било каква инволвираност во овој сајбер напад. Меѓутоа овој сајбер напад повлече низа политички ескалации помеѓу САД и Северна Кореја[26].

3.11 CASE STUDY: OPERATION CLEAVER

Американската софтверската фирма Cylance во 2014 година на извештај од 86 страни[27] објавила две годишна истрага за операција наречена Operation Cleaver, т.е сајбер напад кој целел на клучни инфраструктури, како војската, нафтената и енергетската индустрија, транспортот, болници лоцирани ширум светот. Името cleaver го добила благодарение на истоименот терминот "cleaver" кој многу често бил користен во малциозниот код. Всушност овој сајбер напад таргетирал над 50 ентитети во повеќе од 16 држави.

3.12 CASE STUDY: CYBERATTACK DURING THE PARIS G20 SUMMIT

Овој сајбер напад се одвивал пред почнувањето на G20 самитот во Париз,Франција во 2011 година. Самитот бил наменет за шефовите на финансиските институции и централните банки. Нападот започнал во Декември со еден пратен е маил. Атачментот на емаило бил тројански коњ кој бил замаскиран со pdf документ инфициран со малциозен вирус. Поради фактот дека истиот се ширел со енормна брзина, за кратко време заразил значителна бројка на компјутери на финансиските министри. Според подоцнежните изешати овој напад тагирал само G20 документи, оставајќи ги останатите финасики чувствителни податоци нехакирани.

3.13 CASE STUDY: OPERATION SHADY RAT

Operation Shady Rat серија на сајбер напади кои започнале 2006 година. Објавена од страна на Dmitri Alperovitch, истата претставува напад на најмалку 71 организација, вклучувајќи ги и ОН и Интернационалниот Олимписки Комитет. Се шпекулира дека зад истата стои Народна Република Кина.

Овие case studies само уште еднаш ја покажуваат на тежината и комплексноста на сајбер нападите. Уште еднаш се покажа дивертификацијата на метите но и на начините/методите на напад. Секако клучни мети биле и ќе останат исти а тоа се есенцијанлните-витални "органи" на една држава како електрани, објекти за снабдување и обезбедување вода, електрична енергија, транспотниот сообраќај, научно истражувачките центри, здравствените и финансиските објекти... Проблемот е "оружјето" , бидејќи нападот може да е преку вируси, софтвери, спамизи... прикриени но сигурни виновници за енормните штети.

[25] https://www.rollingstone.com/movies/movie-news/sony-cancels-interview-new-york-premiere-amid-terror-threats-194486/,https://variety.com/2014/film/news/sony-has-no-further-release-plans-for-the-interview-1201382167/

[26] https://www.bbc.com/news/world-asia-30608179

[27] https://www.cylance.com/content/dam/cylance/pdfs/reports/Cylance_Operation_Cleaver_Report.pdf

Кембрицкиот центар за истражуавње на ризици[28] потенцијалните извршители ги класифицираат на три групи:

- ✓ Организиран криминал-Organised criminals – организираниот сајбер криминал веќе се трансформира во индустрија.
- ✓ Хактивисти- Hacktivists- се организирани кадри на активисти кои хакираат за политички причини. Тие се пронаоѓаат поради нивната мисија и затоа често не ги знаат меѓусебните вистински имиња.
- ✓ Осамени волци- Lone wolf – се индивидуалци кои работат сами, не во група.

4. New Health care cyber attacks?

Здравствената индустрија се базира на технологија која е конектирана на Интернет: од записи за пациенти и лабараториски резултати, до радиолошка опрема и болнички лифтови... Овие сегменти претставуваат одлична грижа на пациентите, но од друга страна истите се ранливи и подложни на сајбер напади, кој ги хакираат записите на пациентите, инфузиите, блокади на повеќе болнички сегменти додека не се плати биткоин.. Ова ги стави во прашање експертите кои бараа да се прогласи црвен аларм во здравствениит систем, бидејќи за разлика од нападите во финансикиот сектор, нападите од здравствената сфера може да резултираат со сериозни повреди, дури и смрт.

Во "одбрана" на сајбер нападите, стои фактот дека ниту еден пациент не починал како директен резултат од WannaCry. Но тоа ни од далеку не ја намалува сериозната закана на "модерното зло", бидејќи хакирајќи илјадници болнички компјутери и делови од дијагностичка опрема, ќе ги принудат докторите да ги носат резултатите на рака низ цела болница (што е губење на драгоцено време) и би биле откажани повеќе од 20.000 термини за пациенти.

Познат пример е Pugsley cyber attack[29]. Нападот успеал да енкриптира болнички здравствени податоци и да ги држи компјутерските системи под контрола, барајќи биткоин откупнина[30]. Всушност станува збор за симулација на болничко хакирање[31] во која учество земале актери и модели со реална тежина. Сите освен докторите кои морале веднаш да интервенираат без користење на тенологија, биле запознаени со симулацијата. Целта на симлулацијата е да се продлабочли соработката помеѓу хакери (добрите хакери), безбедносните претставници, медицинскиот персонал, персоналот за изработка на медицинска опрема[32]...Учеството и соработката помеѓу овие профили на луѓе може да резултира со навремено реагирање или уште поважно превенирање сајбер напади насочен токму кон здравствениот систем.

Всушност овде се наметнува прашањето за условно кажано модернизацијата на 21 –от век. Дали е потребно сите релевантни национални инфраструктури да се "зависни" од технологија и приклучок на интернет? Дали круцијалните податоци, кодови, шифри,

[28] Cambridge Centre for Risk Studies- Cyber Terrorism Insurance Futures 2017.

[29] https://www.theverge.com/2019/4/4/18293817/cybersecurity-hospitals-health-care-scan-simulation

[30] Биткоин е дигитална, виртуелна криптовалута или електронски пари. Кога се користи со голема буква-Биткоин, се мисли на платежниот систем кој се појави 2009 година, додека кога се користи малата буква-биткоин се мисли на дигиталната валута.Системот не е во ничија сопственост, а валутата не е контролирана од ниту еден ентитет (централна банка).

[31] https://the-parallax.com/2018/12/19/how-hackers-are-approaching-medical-cybersecurity/

[32] http://phoenixmed.arizona.edu/cybermed

информации е потребно да фигуриираат електронски, кога е ставена под знак прашање нивната безбедност?

5. Правила за дигиално војување

Колку меѓународното право може да се примени во сферата на сајбер тероризмот, сајбер криминалот? Прашања на кои упатуваат мноштво на експерти, обидувајќи се да пронајдат што е можно посоодветно решение за регулирање на оваа глобана проблематика. Секако овде се неминовните повелби од Талин, но и низа други истражуавања[33] на компетентни профили на автори кои се за и против примена на меѓународното воено право во делот на "сајберманијата". Ставот кој е интересен за разгледување и е најсоодветен е воведувањето на т.н Дигитална Женевска Конвенција. Тоа би било конвенција која сеопфатно ќе ја регулира дигиталната сфера на криминал, која можеби ќе продуцира и етаблирање на посебен меѓународен трибунал за оваа проблематика. Такво решение е идеално бидејќи ќе обезбеди стручност на кадарот, посебна конвенција исклучиво наменета за детално регулирање на сајбер доменот...

Заклучок:

Голем број на автори веќе зборуваат за cyber law-интернет право? Всушност сметаат дека веќе виртуелниот свет наместо да се покорува на законите на одредена држава, треба да се потпира на виртуелни интернет закони. "Интенет граѓани" наместо да се идентификуваат како физички личности, ќе се препознаваат по нивните usernames или маил адреси. Не знам како други би го интерпретирале ова но сметам дека вакво сценарио не треба да постои.

Наместо такви сценарија многу подобро би било да се воведе меѓународна конвенција која сеопфатно ќе ја регулира сајбер материјата. Зошто? Бидејќи додека се пишува овој труд, постојат претпоставки дека веќе се работи на нови штетни софтвери, злонамерни апликации, прикриеени информатички платворми, компјутерски "sui generis" вируси, шпионски кодови заштитени како тврдина, информатички оружја со неизмерна сила...Се уште тешко се справуваме со моменталните, актуелни, детектирани и потврдени информатички злодела, а веќе на повидок се нови, кои само може да замислиме што се може да предизвикаат.

Затоа идејата за Дигитална Женевска Конвенција и те како е потребна. Ако Женевските Конвенции ги штитеа граѓаните од последиците на војната, тогаш нивната дигитална метаморфоза ќе ги штите од виртуелните опасности.

[33] https://www.dw.com/mk/%D0%BD%D0%B0%D1%82%D0%BE-%D1%81%D0%B0%D0%BA%D0%B0-%D0%B4%D0%B0-%D0%B2%D0%BE%D0%B2%D0%B5%D0%B4%D0%B5-%D0%BF%D1%80%D0%B0%D0%B2%D0%B8%D0%BB%D0%B0-%D0%B7%D0%B0-%D0%B2%D0%BE%D1%98%D0%BD%D0%B0-%D0%BF%D1%80%D0%B5%D0%BA%D1%83-%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82/a-17762941

Користена литература

Ачкоски,Ј. Сигурноста на компјутерските системи, компјутерски криминал и компјутерски тероризам, Скопје,2012 година

Adler F; Mueller G; Laufer W. Criminology and the criminal justice system – sixth edition

Богданоски, М, Петрески, Д. Меѓународно научно списание за одбрана, безбедност и мир

Богданоски,М,Богданоски,М. Сајбер нападите како најсовремена закана за воените операции и критичната инфраструктура

Габеров,М. Феноменологија на сајбер криминалитетот,2015 година

Габеров, М. Правото на приватност и сајбер просторт,2015 година

Гелке,А.Новата ера на тероризмот и меѓународниот политички систем.

Калач, Ј. Сајбер тероризмот како закана кон безбедноста на државата,2017 година

М.Богданоски, М.Богданоски, Е.Николов, Д.Петревски, Сајбер нападите како најсовремена закана за воените операции и критичната инфраструктура, MILCON, Скопје, 2012

Cyber terrorism: Assesment of the threat to insurance, Cambridge centre for Risk Studies, 2017

Шалијан,Ж,Блин,А. Историја на тероризмот.

Конвенции:

Европска Конвенција за компјутерски криминал,Будимпешта,2001 година.

Дополнителен протокол на Конвенцијата за компјутерски криминал за инкриминација на дела од расистички, ксенофобички вид по пат на информатички системи-Стразбур,2003 година.

Конвенција на Советот на Европа за перење, откривање, заплена и конфискација на приноси од казниво дело и финанасирање на тероризам-Варшава,2005 година.

Линкови:

https://www.cylance.com/content/dam/cylance/pdfs/reports/Cylance_Operation_Cleaver_Report.pdf

https://the-parallax.com/2018/12/19/how-hackers-are-approaching-medical-cybersecurity/

[1] http://phoenixmed.arizona.edu/cybermed

https://the-parallax.com/2018/12/19/how-hackers-are-approaching-medical-cybersecurity/

[1] http://phoenixmed.arizona.edu/cybermed

https://www.theverge.com/2019/4/4/18293817/cybersecurity-hospitals-health-care-scan-simulation

https://oag.ca.gov/system/files/12%2008%2014%20letter_0.pdf

https://www.rollingstone.com/movies/movie-news/sony-cancels-interview-new-york-premiere-amid-terror-threats-194486/

https://variety.com/2014/film/news/sony-has-no-further-release-plans-for-the-interview-1201382167/

[1] https://www.bbc.com/news/world-asia-30608179

http://large.stanford.edu/courses/2015/ph241/holloway1/
https://ccdcoe.org/tallinn-manual.html
https://www.dw.com/mk/%D0%BD%D0%B0%D1%82%D0%BE-%D1%81%D0%B0%D0%BA%D0%B0-%D0%B4%D0%B0-%D0%B2%D0%BE%D0%B2%D0%B5%D0%B4%D0%B5-%D0%BF%D1%80%D0%B0%D0%B2%D0%B8%D0%BB%D0%B0-%D0%B7%D0%B0-%D0%B2%D0%BE%D1%98%D0%BD%D0%B0-%D0%BF%D1%80%D0%B5%D0%BA%D1%83-%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82/a-17762941