**Reziqet dhe mbrojtja nga ataku kibernetik**

**Blerim Abedini, Qendra për Studime të Sigurisë dhe Zhvillim-Maqedoni (CSSD).  
Hakerat e sponsorizuara nga shteti dhe ato jo-shtetërore janë rritur në mënyrë eksponenciale. Problemet e sigurisë kibernetike dhe sulmet shkaktojnë çdo vit miliarda dollarë humbje. Çdo vit, mijëra probleme kibernetike janë identifikuar në teknologji nga kompani të njohur, të cilët ende çdo vit kanë qindra problemeve të sigurisë. Forum i Sigurimit Kibernetik 2017 (CSF 2017) është një forum ndërkombëtar mbi sigurinë kibernetike me pjesëmarrjen e ekspertëve ndërkombëtarë dhe rusë, përfaqësues të industrisë së IT (Microsoft Inc.) dhe autoriteteve qeveritare.**

Ka disa lloje të personave, të quajtur zakonisht "aktorët e kërcënimit."  
• Cyber kriminelët: Ata sulmojnë sistemet dhe vjedhin informacion për fitim.  
• Hakerët: Disa hakerë janë profesionistë (të cilët punojnë për të përfituar në kompanitë dhe për të përmirësuar sigurinë), por ka edhe hakerë qëllimkeq.  
• Hacktivists: Këta njerëz janë të motivuar politikisht. Për shembull, organizata si Anonimus bie në këtë grupim.  
• Terroristët- Cyber: Përderisa këto nuk janë të zyrtarizuar, ato mund të bëhen aktyel së shpejti.  
• Shtetet-kombe: bëjnë sulme kibernetike kundër vendeve të tjera.  
Hakerat e sponsorizuara nga shteti dhe ato jo-shtetërorë janë rritur në mënyrë eksponenciale. Pra, një grup i hakerëve mund të ketë ndikim të madh në instalimet ushtarake, operacionet qeveritare, infrastrukturën kritike dhe sistemet aktive të armëve. Pra, një rritje e vazhdueshme ushtarake në armët konvencionale do të rrisë edhe kiber-sulmet në anën tjetër.

Problemet e sigurisë kibernetike shkaktojnë miliarda dollarë humbje çdo vit. Për shembull, ataku në SimpliSafe me të cilin rast preken 300,000 pajisjet, që detyron menaxhuesit ti zëvendësojnë ato. Kompania UK TalkTalk ishte sulmuar dhe patë humbur rreth 50 milion £. Ata gjithashtu humbën më shumë se 100,000 klientëve, dhe vlera e tyre të aksioneve kishte rënë për 20%. Një sulm në vitin 2015 ka rezultuar në 1.4 milion vetura të tërhequr nga Chrysler, më pas skandali Sony që rezultoi në miliona dollarë në humbje. Shembuj të përditshëm mund të jenë: Makina të atakuar, sistemet e alarmit për shtëpitë në SHBA ishte atakuar, pajisjet mjekësore të implantueshme si stimulues kardiakë kanë qenë atakuar, sistemet e aeroplanëve kanë qenë atakuar, infrastruktura kritike e rrjetit të energjisë dhe një digë ka qenë e atakuar, Aplikacionet bankare për celularë kanë qenë të atakuar, teknologjia e qytetit Smart ka qenë e atakuar.  
Çdo vit, mijëra probleme kibernetike janë identifikuar në teknologjitë nga shitës të njohur, të cilët ende kanë qindra probleme të sigurisë çdo vit. Disa ekspertë parashikojnë se deri në vitin 2020 do të jetë 200 miliardë gjësende të lidhura ose të komunikuara si p.sh., makina, aeroplanë, shtëpitë, qytetet dhe kafshët e konektuara.

Futja e lidhjes pa tel në sistemet e aeroplanëve luftarak ka mundësuar që të arrihen udhëzime më të sakta me kompjuter, kontroll më të mirë dhe manovra më të shpejtë të fluturimit. Këto sisteme sigurojnë informacion të gjerë në lidhje me mjedisin.  
Teknologjia e informacionit nuk është e përfshirë vetë në aksionet luftarake, por ajo luan rol edhe në azhurimin e dhënave të inteligjencës si dhe në planifikimin strategjik. Informacioni si i tillë është bërë i rëndësishëm për të identifikuar armiq në zonat civile për shkak të mungesës së uniformave. Kjo padukshmëri si dhe deshifrimi i saj është çështja kryesore. Përdorimi strategjik i teknologjive të informacionit, si fotografitë satelitore, transmetimet e telekomanduara, madje edhe Facebook dhe Twitter mesazhet / llogaritë, janë duke u përdorur më shumë për të identifikuar armikun, lëvizjet e saja dhe vendndodhjen. Një Komandant i ISIS i cili kishte postuar një selfie në Facebook, ishte hetuar nga agjencioni i Intelligjencës amerikane, dhe pas 22 orëve vendi u gjet i bombarduar.  
Një atak në (DDoS) i çkyçi nga rrjeti 68 faqet e internetit të qeverisë filipinase në përgjigje të një vendimi të gjykatës ndërkombëtar që mohoi pretendimet territoriale të Kinës në rajon. Vetëm ditë më vonë, linja ajrore kombëtare Vietnamit dhe aeroportet e mëdha kanë qenë në shënjestër me një seri sulmesh nga grupi kinez- hakerët 1937CN. Poashtu Kinezët u përpoqën të ndërhyjnë me drone ushtarake ndaj maqinerisë ushtarake të SHBA-së, duke përdorur GPS- zhurma teknikë, të cilat mund të pengojnë aeroplanët e SH.B.A.-së për kryerjen e misioneve të mbikqyrjes në Detin e Kinës Jugore tek ishujt e vegjël.

Disa prej avancimeve në IT teknologjinë e informacionit në Rusi ka [REGNUM](Https://regnum.ru/news/society/2147845.html)- Iniciativa Kombëtare e Teknologjisë në Rusi. Në qershor të vitit 2016, ka bërë të ditur programin për ndërtimin e softverëve në gjuhën rusishte deri në 2035. Gjithashtu, një "hartë rrugore" e programit e cila parashikon qasje të re teknologjike, si ajo teleportimit.  
Kështu bashkërisht do të përdoren informatika kuante, ndërfaqet psikologjike dhe teleportimi. Agjencia për Iniciativa Strategjike (Агентство стратегических инициатив-АСИ), planifikon të zbatojë një sistem të sigurisë për sistemet e informacionit dhe kibernetikë fizike që është e koduar, "SafeNe". Këto janë të specifikuara si "sisteme smart" të cilat janë të planifikuara për t'u përdorur nga ana e fizikantëve të kibernetikës, të cilat përfshijnë rrjete informatikë dhe komponentet fizike të afta për të ndërvepruar me njëri-tjetrin, si që janë robotët, makina të vetë-kontrolluara, dronet, etj. Kostoja e programit në mes të viteve 2017-2018 do të jetë 10.8 miliardë rubla (192 milionë dollarë) të mbështetur nga buxheti federal dhe investitorë privatë.  
​​Forumi i Sigurimit Kibernetik 2017 (CSF 2017) është një forum ndërkombëtar mbi sigurinë kibernetike me pjesëmarrjen e ekspertëve ndërkombëtarë dhe rusë, përfaqësues të industrisë së IT (Microsoft Inc.) dhe autoriteteve qeveritare.

Forumi i Sigurimit Kibernetik 2017 u mbajt më 7 shkurt, 2017, në Moskë. Forumi është një pjesë e rëndësishme e ashtuquajtur 'Safe Runet Javës', me ngjarje në Ditën Ndërkombëtare të Sigurisë në internet. Për 10 vjet, ky forum është transformuar në qasjen e re I-Safety. Forumi i Sigurisë Kibernetike ​​është një platformë për të diskutuar një numër çështjesh që lidhen me aspekte të ndryshme të sigurisë kibernetike, si çështja e sigurisë industriale dhe industria nëpërmjet internetit, si: leximi digjital, sigurimi digjital, rregullimi i mbrojtjes- infobase, etj. Kjo është kryesisht orientuar ndaj përfitimeve të shtetit dhe industrisë, për rinovimin e aktiviteteve të tyre që synojnë parandalimin e kërcënimeve të reja kibernetike. Gjithashtu pesha e këtij forumi hap shtigje për dialog në mes të shteteve, të industrisë dhe organizatave të specializuara në mënyrë që të krijojnë një koalicion të fortë kundër krimit kibernetik në mbarë botën. Janë të identifikuar burimet kryesore të krimit kibernetik si: vjedhje e të dhënave personale, përdorimi i aplikacioneve mobile gri(gray), phishing dhe të tjerë. Qasje e integruar për zgjidhjen e këtyre problemeve është një iniciativë globale mbi të. Gjithashtu leximi në media shihet si aftësi e një personi për të punuar me informacione që ai i konsumon nga shumëllojshmëri burimesh, si dhe disa mangësi tjera si mungesa e aftësive të përdoruesve në internet ose nuk janë të edukuar për përdorimin e kompjuterit. Pra, gjëja e rëndësishme sipas debateve në forum është puna edukative mbi përdoruesit jo të aftë për mbrojtjen e të dhënave personale. Si pjesë e Forumit të sigurisë kibernetike, Microsoft-i paraqet një vlerësim të kulturës digjitale. Sipas një studimi të Microsoft, rreth 75% e rusëve u përball të paktën një herë me rrezik në internet. Bazuar në rezultatet e anketës, vendet janë renditur në bazë të nivelit të kulturës digjitale – Indeksi i Qytetërimit Digjital (DCI). Rusia zë vendin e 12 në mesin e 14 vendeve që morën pjesë në studim. Indeksi DCI, kanë kategoritë e rreziqeve, si: të sjelljes, rreziqet e komunikimit të padëshiruar, motive seksuale dhe reputacioni. Adoleshentët nga 14 vende të botës morën pjesë në anketë. Studimi tregon se kërcënimet e internetit janë të përhapura në të gjitha vendet. Dëshpërimet janë humbja e besimit, stresi dhe dëshira e përdoruesve për privatësi në rrjet. Një studim i audiencës ruse tregoi se rusët, në krahasim me përdoruesit nga vende të tjera, janë më të ekspozuar se të tjerët për rreziqet e sjelljes: fyerjeve në internet (44% në një nivel mesatar prej 14% vende tjera), si edhe si keqtrajtimi në rrjet (47% vs. 20%). Znj Ulyana Zinina, drejtor i Punëve të Korporatës për Microsoft në Rusi ka shpjeguar se Microsoft është duke mbrojtur fenomenet negative përmes rrjetit. Për të zvogëluar mundësinë e rreziqeve në rrjet, Microsoft inkurajon palët e interesuara të bashkojnë forcat, dhe përdoruesit për të ndjekur rekomandimet kyçe: të mos publikojnë ose zbulojnë informacion personal për veten e tyre, të trajtojnë lidhje të mira me përdoruesit tjerë , të respektojnë dallimet kulturore. Në rast mosmarrëveshjeje duhet shmangur etiketimet mbi individët.

Pra, ne mund të shohim se bashkëpunimi brenda temës së sigurisë kibernetike është në favor të shteteve në botë. Duke lënë mënjanë ndonjë aktivitet në këtë drejtim do të hapet rrugë viruseve për të qarkulluar në të dhënat tona personale. Pra, siguria kibernetike është në favor të çdo shoqërie të integruar.

**Referenca:**

***Cyber Security Forum 2017 (CSF 2017) – Mеждународный Форум по кибербезопасности, https://runet-id.com/event/csf17/***

***Advanced Cyber Security Center, https://www.acscenter.org/news-events/cybersecurity\_is\_threatening\_americas\_military\_supremacy/***

***Information Strategy at the Rotterdam School of Management, Erasmus University.*** [***Https://informationstrategyrsm.wordpress.com/2015/10/09/modern-wars-how-information-technology-changed-warfare/***](Https://informationstrategyrsm.wordpress.com/2015/10/09/modern-wars-how-information-technology-changed-warfare/)

***The Forbes,*** [***https://www.forbes.com/sites/forbestechcouncil/2017/01/17/why-cybersecurity-should-be-the-biggest-concern-of-2017/#21ee52215218***](https://www.forbes.com/sites/forbestechcouncil/2017/01/17/why-cybersecurity-should-be-the-biggest-concern-of-2017/#21ee52215218)

***REGNUM, The National Technology Initiative, (Программа «Национальная технологическая инициатива» -НТИ).*** [***Https://regnum.ru/news/society/2147845.html***](Https://regnum.ru/news/society/2147845.html)