

Fatjon Malaj

Lektor

Departamenti Administrimit Publik, Universiteti Gjirokastër

Brishtësia e sigurisë dhe stabilitetit në sektorët kibernetik!

Sulmet ndaj infrastrukturës kritike demonstrojnë më qartë natyrën asimetrike të gjeopolitikës kibernetike. Me operacione kibernetike me kosto relativisht të ulët, funksionaliteti i infrastrukturës fizike me vlerë miliarda dollarë mund të ndërpritet dhe jeta shoqërore mund të preket seriozisht. Sulmet ndaj rrjetit të energjisë të Ukrainës kanë rezultuar në pamundësinë e civilëve për të përmbushur nevojat e tyre themelore dhe në ndërprerjen e aktivitetit ekonomik. Kjo tregon se sulmet kibernetike kanë aftësinë të ndikojnë drejtpërdrejt jo vetëm në objektivat ushtarake, por edhe në shoqërinë civile.

Dimensioni gjeopolitik i varësisë teknologjike është gjithashtu i dukshëm në dobësitë e zinxhirëve globalë të furnizimit. Infrastrukturat kritike moderne përfshijnë komponentë të furnizuar nga furnizues të shumtë ndërkombëtarë, duke krijuar dobësi të mundshme në zinxhirin e sigurisë. Kërcënimet e integruara në nivelin e harduerit dhe softuerit, së bashku me rreziqet e infiltrimit përmes portave të aksesit në distancë dhe përditësimeve, e ndërlikojnë mbrojtjen e infrastrukturës kritike.

Ndikimet Ekonomike të Luftës Kibernetike në Bazë Sektoriale

Sektori i Teknologjisë

Sektori i teknologjisë ka një rëndësi të veçantë për shkak të ndjeshmërisë së tij ndaj sulmeve kibernetike dhe efekteve të valëzuara që ato kanë në sektorë të tjerë. Kompanitë e mëdha të teknologjisë dhe furnizuesit e softuerëve janë në zemër të spiunazhit kibernetik dhe sulmeve të zinxhirit të furnizimit. Siç u pa në incidentin SolarËinds, një shkelje e sistemit të një prodhuesi softuerësh preku mijëra klientë të tij. Në mënyrë të ngjashme, një incident tjetër në vitin 2017 përfshinte një shkelje të serverit të përditësimit për CCleaner, një softuer popullor i përdorur globalisht; në këtë sulm, sulmuesit synonin të synonin bazën e gjerë të përdoruesve të softuerit. Gjigantët e teknologjisë gjithashtu mund të pësojnë goditje ekonomike nga sulmet kibernetike herë pas here: për shembull, sulmi i Sony Pictures në vitin 2014 i shkaktoi kompanisë humbje financiare (filmat u rrjedhën, sistemet nuk ishin në rregull për ditë të tëra) dhe dëmtim të reputacionit.

Incidente të tilla mund të çojnë në rënie të çmimeve të aksioneve të firmave të teknologjisë, humbje të besimit të klientëve dhe dënime të rënda ligjore. Për më tepër, sulmet kibernetike që synojnë sektorin e teknologjisë gjithashtu mund të pengojnë inovacionin. Vjedhja e informacionit të dizajneve ose zhvillimit të produkteve nga departamentet e Kërkimit dhe Zhvillimit dhe rrjedhja e tyre në vendet rivale mund të shkatërrojë avantazhin konkurrues të kompanisë në fjalë. Për shembull, vjedhja e sekreteve teknologjike nga kompanitë amerikane të gjysmëpërçuesve dhe telekomunikacionit nga grupet kineze të hakerave ka përshpejtuar përparimin e Kinës në këtë fushë, duke rrezikuar njëkohësisht pjesën e tregut dhe të ardhurat e ardhshme të kompanive amerikane. Kjo situatë mund të krijojë avantazhe të padrejta dhe ndryshime në ekuilibrin ekonomik në garën globale të teknologjisë. Si rezultat, kompanitë e sektorit të teknologjisë detyrohen të ndajnë miliarda dollarë për sigurinë kibernetike, gjë që reflektohet si një kosto për konsumatorët dhe ekosistemin e përgjithshëm të inovacionit.

Sektori Financiar

Sektori financiar është një nga objektivat kryesorë për sulmuesit kibernetikë, pasi përfshin drejtpërdrejt para dhe të dhëna të vlefshme. Bankat, bursat, sistemet e pagesave dhe platformat e kriptomonedhave i nënshtrohen përpjekjeve të panumërta për sulme kibernetike çdo ditë. Në kontekstin e luftës kibernetike, shtetet ose organizatat armiqësore mund të kryejnë sulme të planifikuara për të prishur stabilitetin financiar të një vendi. Për shembull, në vitin 2016, hakerat e lidhur me Korenë e Veriut infiltruan sistemin SËIFT të Bankës Qendrore të Bangladeshit dhe kryen transferta mashtruese

parash prej 81 milionë dollarësh - një sulm që, ndërsa synonte drejtpërdrejt fitimin financiar, gjithashtu i dha një goditje besimit në sistemin bankar ndërkombëtar. Aktorët shtetërorë ndonjëherë mund të përdorin mjete kibernetike për të hedhur sistemin financiar në kaos ose për të krijuar presion ekonomik. Sulmet kibernetike të Rusisë në vitin 2015 që synonin ministrinë e financave të Ukrainës dhe thesarin kombëtar synonin të prishnin transaksionet financiare të vendit. Një skenar tjetër shqetësues është një sulm i koordinuar ndaj bursës së një vendi ose bankave kryesore, që rezulton në fshirjen e llogarive ose manipulimin e transaksioneve. Në një situatë të tillë, mund të lindë panik në tregje, një rënie e vlerave të aksioneve dhe mundësia e një krize të përhapur ekonomike. Një pikë tjetër e dobët e sektorit financiar është vjedhja e të dhënave personale dhe informacionit të identitetit. Në shkeljet e të dhënave në shkallë të gjerë, karta e kreditit, llogaria bankare ose informacioni i identitetit të miliona përdoruesve mund të vidhet dhe të shitet në tregun e zi, duke shkaktuar dëme si për individët ashtu edhe për institucionet financiare. Për shembull, në shkeljen e të dhënave të Equifax në SHBA në vitin 2017, informacioni financiar i 147 milionë njerëzve u rrjedh. Kostoja ekonomike e ngjarjeve të tilla, e matur nga transaksionet mashtruese, dëmet ligjore dhe humbjet e klientëve që vijnë nga humbja e besimit, arrin në miliarda dollarë. Për shkak të të gjitha këtyre rreziqeve, sektori financiar është bërë një nga sektorët që ka rritur më shumë investimet e tij në sigurinë kibernetike. Ndërsa bankat shpenzojnë miliarda çdo vit për siguri, organet rregullatore ndërkombëtare po prezantojnë gjithashtu standarde të reja për të rritur rezistencën kibernetike të

sistemit financiar. Megjithatë, lufta midis sulmuesit dhe mbrojtësit vazhdon pa pushim, dhe metodat inovative të sulmit vazhdojnë të kërcënojnë sektorin financiar. Kohët e fundit, sulmet kibernetike që synojnë bursat e kriptomonedhave (siç është vjedhja e 600 milionë dollarëve nga një platformë kriptovalutash në vitin 2022) kanë hapur fronte të reja. Në fund të fundit, sektori financiar e ruan rëndësinë e tij si një front strategjik në luftën kibernetike, duke synuar ekonomitë kombëtare.

Sektorët e Infrastrukturës dhe Transportit

Infrastruktura kritike është gjaku i ekonomisë së një vendi. Infrastruktura si rrjetet e transportit (ajror, hekurudhor, rrugor), furnizimi me ujë, impiantet e trajtimit të ujërave të ndotura dhe shërbimet publike mund të shkaktojnë humbje të konsiderueshme me një efekt shumëfishues në ekonomi kur shënjestrohen nga sulmet kibernetike. Për shembull, le të shqyrtojmë ndikimin e një sulmi kibernetik në sektorin e transportit: Çaktivizimi i një linje ajrore ose sistemi të kontrollit të trafikut ajror për shkak të një sulmi kibernetik çon në anulime fluturimesh, shqetësime për mijëra pasagjerë dhe ndërprerje të aktiviteteve tregtare. Në vitin 2018, një përpjekje për sulm kibernetik në sistemet e informacionit të Aeroportit Heathroë në Mbretërinë e Bashkuar ndërpreu operacionet e aeroportit dhe shkaktoi humbje financiare. Në mënyrë të ngjashme, hakimi i porteve ose sistemeve të navigimit të anijeve në transportin detar mund të prishë rrjedhat globale të tregtisë. Në vitin 2017, sulmi NotPetya, i cili i çoi operacionet portuale të Maersk në një ndalesë, shkaktoi një ndërprerje serioze të tregtisë botërore. Infrastruktura hekurudhore është gjithashtu ndër objektivat kritikë në skenarët e luftës

kibernetike. Dëmtimi i sistemeve të sinjalizimit mund të shkaktojë aksidente trenash ose anulime. Në vitin 2016, një kompani hekurudhore në një vend evropian (Belgjikë) u sulmua me ransomëare, duke shkaktuar ndërprerje në shërbimet e trenave. Çdo ndërprerje në sektorin e transportit krijon një efekt "top bore" në ekonomi përmes ndikimeve dytësore, siç janë pamundësia e punonjësve për të shkuar në punë dhe mosdorëzimi i produkteve në kohë. Infrastruktura urbane është gjithashtu nën kërcënim dixhital. Me rritjen e aplikacioneve të qytetit inteligjent, sisteme të tilla si semaforët inteligjentë, stacionet e karikimit të autobusëve elektrikë dhe kamerat e sigurisë paraqesin gjithashtu një sipërfaqe të mundshme sulmi. Çaktivizimi i këtyre sistemeve mund ta zhytë jetën e qytetit në kaos dhe ta ndalë aktivitetin ekonomik. Për shembull, edhe shkaktimi i të gjitha semaforëve që të mbeten të kuq duke infiltruar sistemin e menaxhimit të trafikut të një qyteti do të thotë humbje të konsiderueshme ekonomike (humbje kohe dhe karburanti, vonesa logjistike, etj.). Në një situatë lufte kibernetike, shërbimet publike kritike të një vendi gjithashtu mund të jenë në shënjestër. Sulmet ndaj sistemeve të kontrollit të administratave të ujit dhe kanalizimeve mund të çojnë në mungesë uji ose ndotje të ujit. Në vitin 2021, një sulmues që infiltroi një impiant përpunimi uji në Florida, SHBA, u zbulua dhe u ndalua në minutën e fundit ndërsa përpiqej të përziente kimikate të tepërta në ujin e pijshëm, duke nënvizuar rrezikun në këtë fushë. Nëse një sulm i tillë do të ishte i suksesshëm, ai do të rrezikonte shëndetin publik dhe do të kërkonte kosto të konsiderueshme për sigurimin e ujit të pastër. Në fund të fundit, sektorët e infrastrukturës dhe transportit janë fusha ku ndikimet

ekonomike dhe shoqërore të sulmeve kibernetike janë shumë të larta. Çdo sulm ndaj këtyre sektorëve do t'i jepte një goditje ekonomisë përmes kostove të riparimit, ndërprerjeve të shërbimit dhe humbjes së besimit. Për këtë arsye, qeveritë e shohin sigurinë kibernetike të infrastrukturës kritike si çështje të sigurisë kombëtare dhe përpiqen ta mbrojnë atë përmes bashkëpunimit të ngushtë me operatorët.

Sektori i Energjisë

Sektori i energjisë është ndoshta objektivi më strategjik i luftës kibernetike, si për vlerën e tij ekonomike ashtu edhe për rolin e tij themelor në funksionimin e të gjithë sektorëve të tjerë. Infrastruktura e energjisë, siç janë rrjetet e energjisë elektrike, tubacionet e naftës dhe gazit, objektet bërthamore dhe rafineritë, janë gjaku i jetës së një vendi. Një sulm kibernetik në këto zona mund të paralizojë ekonominë dhe të kërcënojë drejtpërdrejt sigurinë kombëtare. Ekzistojnë shembuj ekzistues të sulmeve kibernetike që synojnë rrjetet e energjisë elektrike. Ndërprerjet e energjisë elektrike në Ukrainë, të cilat i përmendëm më parë, rezultuan nga kontrolli në distancë i qendrave të shpërndarjes duke përdorur programe keqdashëse. Këto sulme lanë mijëra njerëz pa energji elektrike në mes të dimrit dhe ngritën shqetësime për sigurinë. Nëse një sulm i ngjashëm do të ndodhte në një vend shumë më të madh, ai mund të rezultonte jo vetëm në humbje ekonomike, por edhe në një krizë të madhe humanitare, duke përfshirë humbjen e jetës. Për shembull, po diskutohen skenarë ku një sulm në rrjet që synon të gjithë Bregun Lindor të SHBA-së mund të shkaktojë triliona dollarë dëme, si dhe të çojë në mosfunksionimin e spitaleve dhe humbjen e jetës. Prandaj, po bëhen përpjekje ndërkombëtare për të përmirësuar

sigurinë kibernetike të rrjeteve të energjisë, dhe organizata të tilla si NATO dhe BE po ofrojnë mbështetje për shtetet anëtare në këtë drejtim. Infrastruktura e naftës dhe gazit është një tjetër element kritik i ekonomisë. Tubacionet, platformat e shpimit dhe terminalet e LNG-së tani operohen me sisteme kontrolli industrial (SCADA) dhe janë të ndjeshme ndaj sulmeve kibernetike. Në vitin 2021, një sulm me programe ransomëare ndaj Colonial Pipeline në SHBA, ndërsa nuk e ndaloi drejtpërdrejt rrjedhën e naftës, e detyroi kompaninë të mbyllte tubacionin si masë paraprake, duke rezultuar në ditë të tëra pa karburant të disponueshëm dhe blerje paniku dhe rritje çmimesh në rajon. Mësimi i nxjerrë nga kjo ngjarje është se sa të brishta mund të jenë infrastrukturat e energjisë dhe si një sulm kibernetik, edhe tërthorazi, mund të prishë furnizimin me energji dhe të shkaktojë dëme ekonomike. Një aktor shtetëror që synon qëllimisht infrastrukturën e energjisë së një vendi mund të ketë pasoja të rrezikshme, që arrijnë në një deklaratë lufte. Për shembull, në tensionin midis Iranit dhe SHBA-së, hakerat iranianë sulmuan Saudi Aramco me malëare-in "Shamoon" në vitin 2012, duke fshirë 30,000 kompjuterë dhe duke shqetësuar tregjet rajonale të energjisë dhe duke prishur operacionet e prodhimit të naftës në Arabinë Saudite. Termocentralet bërthamore gjithashtu kërkojnë vëmendje të veçantë në kontekstin e luftës kibernetike. Sulmi Stuxnet zbuloi se është e mundur të shkaktohet dëmtim fizik në një strukturë bërthamore përmes mjeteve kibernetike. Sabotimi kibernetik që çaktivizon sistemet e sigurisë ose bën që reaktorët të dalin jashtë kontrollit në një central bërthamor mund të ketë pasoja katastrofike. Prandaj, strukturat bërthamore mbrohen me masat më të rrepta të sigurisë

kibernetike. Megjithatë, sulmet indirekte përmes softuerëve ose pajisjeve të mirëmbajtjes në zinxhirin e furnizimit të këtyre strukturave janë gjithashtu të mundshme. Rëndësia dhe cenueshmëria e sektorit të energjisë e sjellin këtë fushë në ballë të konflikteve kibernetike. Në konfliktet e fshehta midis vendeve, aktivitetet e spiunazhit kryhen shpesh kundër kompanive të energjisë dhe infrastrukturës së tyre; bëhen përgatitje në lidhje me zonat që mund të synohen në rast të një sulmi. Për këtë arsye, kompanitë e energjisë tani punësojnë jo vetëm inxhinierë industrialë, por edhe ekspertë të sigurisë kibernetike; dhe ato krijojnë qendra monitorimi 24/7 për të zbuluar dhe neutralizuar sulmet e mundshme. Megjithatë, sektori i energjisë mbetet një objektiv tërheqës për sulmuesit kibernetikë për shkak të ekuilibrit të tij të lartë rrezik-shpërblim të lartë.

Shqyrtimi gjithëpërfshirës i rëndësisë globale të sigurisë kibernetike dhe efekteve të luftës kibernetike zbulon se sa e brishtë mund të bëhet siguria dhe stabiliteti në botën dixhitale të shekullit të 21-të. Ndërsa interneti dhe teknologjitë dixhitale i ofrojnë njerëzimit komoditete dhe mundësi të mëdha ekonomike, ato gjithashtu i kanë paraqitur shteteve dhe shoqërive kërcënime të papara. Hapësira kibernetike është shfaqur si një front i ri në konkurrencën dhe konfliktin ndërshtetëror. Ngjarjet konkrete të diskutuara në fillim të këtij artikulli kanë vërtetuar se lufta kibernetike ka shkuar përtej diskutimit abstrakt dhe ka pasoja shkatërruese në botën reale. Sulmet kibernetike të vitit 2007 ndaj Estonisë i treguan botës se sulmet dixhitale që synojnë ekonomitë kombëtare janë të mundshme dhe efektive, duke i shtyrë organizatat e sigurisë si NATO të përditësojnë strategjitë e tyre.

Stuxnet e zbehu vijën ndarëse midis luftës kibernetike dhe asaj fizike duke vërtetuar se një armë dixhitale mund të krijojë dëme shumë të prekshme në botën fizike. Ngjarje si ËannaCry dhe NotPetya demonstruan se një sulm kibernetik mund të përhapet në mënyrë të pakontrollueshme, duke shkaktuar dëme ekonomike globale. SolarËinds ka treguar se edhe zinxhirët e furnizimit që duken më të sigurt mund të kenë lidhje të dobëta dhe se spiunazhi kibernetik ka arritur një nivel që mund të konsiderohet një krizë në marrëdhëniet ndërkombëtare. Lufta Ukrainë-Rusi është plot me mësime se si operohet në të vërtetë fronti kibernetik në konceptin e luftës hibride; sulmet kibernetike kanë luajtur një rol plotësues për konfliktet aktuale, ndonjëherë madje duke vepruar si një forcë pararojë për të dëmtuar sistemet kritike. Siç e shohim në shembujt e Rusisë dhe Kinës, fuqitë e mëdha po bëjnë investime të konsiderueshme në fushën kibernetike dhe po e përdorin atë për objektivat e tyre politike dhe ushtarake. Operacionet kibernetike të Rusisë variojnë nga ndërhyrja në punët e brendshme të shoqërive demokratike deri te sabotimi i infrastrukturës së vendeve fqinje; ndërsa Kina është përqendruar më shumë në mbledhjen e inteligjencës ekonomike dhe teknologjike, duke ndjekur avantazhe strategjike afatgjata. Në të dyja rastet, aktivitetet kibernetike janë bërë një pjesë integrale e konkurrencës ndërkombëtare dhe madje edhe e konfliktit. Kjo i ka çuar shtetet të përparësojnë parandalimin kibernetik dhe politikat mbrojtëse dhe të zhvillojnë doktrina të reja. Qasja e SHBA-së ofron një model kundër kërcënimeve të tilla: rritjen e qëndrueshmërisë kombëtare përmes strukturave institucionale (si CISA),

ndalimin e kërcënimit në burimin e tij me kapacitet ushtarak (USCYBERCOM) dhe vendosjen e parandalimit përmes normave në arenën ndërkombëtare. Megjithatë, suksesi i këtij modeli nuk matet duke parandaluar sulmet, por duke minimizuar ndikimin e tyre kur ato ndodhin. Sepse siguria 100% në arenën e luftës kibernetike duket e pamundur; Ajo që ka rëndësi është menaxhimi i rreziqeve dhe ndërtimi i qëndrueshmërisë. Duke parë natyrën në ndryshim të luftës, bëhet e qartë se jetojmë në një epokë dixhitalizimi dhe kërcënimesh hibride. Në betejat e së ardhmes, programet keqdashëse dhe algoritmet do të luajnë një rol po aq të rëndësishëm sa tanket dhe pushkët. Luftërat ndërshtetërore për pushtet do të ndërthuren me fushata dezinformimi që synojnë të ndikojnë në mendjet e shoqërive dhe sabotim kibernetik që synon infrastrukturën kritike. Prandaj, strategjitë e sigurisë së shekullit të 21-të do të jenë të paplota pa marrë parasysh dimensionin dixhital. Zhvillimi i planeve të mbrojtjes kibernetike nga aleancat si NATO, krijimi i ushtrive kibernetike nga vendet individuale dhe fokusi në rritje i ligjit ndërkombëtar në këtë fushë janë pasoja natyrore të këtij ndryshimi. Në frontin ekonomik, sulmet kibernetike kanë treguar se kanë ndikime të shumëfishta në të gjithë sektorët. Kompanitë e teknologjisë dhe infrastruktura e IT-së janë qendrore në këtë pamje, duke shërbyer si objektiva dhe mjete; sektori financiar është jashtëzakonisht i rëndësishëm për shkak të lidhjes së tij të drejtpërdrejtë me stabilitetin ekonomik; transporti dhe infrastruktura urbane mund të kenë pasoja shkatërruese për jetën shoqërore; dhe sektori i energjisë, duke qenë themelor për gjithçka, është një lloj "objektivi strategjik". Masat që duhen marrë, investimet që

duhen bërë dhe planet e emergjencës që duhen zhvilluar në këta sektorë tani janë bërë pjesë e planifikimit të sigurisë kombëtare. Rezistenca e infrastrukturës kritike do të jetë vendimtare për aftësinë e një vendi për të mbijetuar në kushtet e luftës kibernetike. Si pasojë, shprehja "rëndësia globale e sigurisë kibernetike" nuk tregon më një theks teorik, por një domosdoshmëri praktike. Shtetet, kompanitë dhe individët duhet të përballen si me mundësitë ashtu edhe me rreziqet e ofruara nga bota dixhitale. Lufta kibernetike ka transformuar konceptin klasik të luftës; ajo ka krijuar një arenë ku distancat gjeografike kanë humbur kuptimin e tyre dhe rolet e agresorit dhe viktimës mund të ndryshojnë në çdo moment. Bashkëpunimi ndërkombëtar, shkëmbimi i informacionit dhe marrja e masave parandaluese në kohë paqeje janë jetike për suksesin në këtë arenë të re. Përndryshe, ekonomia jonë globale gjithnjë e më dixhitale dhe rendi i sigurisë do të mbeten të brishta, të prekshme nga tronditja nga një shtypje e vetme e tastit.