Vytautas Butrimas*
*Lietuvos Respublikos krašto apsaugos ministerija***

Nacionalinis saugumas ir tarptautinės politikos iššūkiai pasaulyje po *Stuxnet* atsiradimo

Tarptautinė bendruomenė skiria daug dėmesio nusikalstamumui ir socialinio-politinio pobūdžio incidentams kibernetinėje erdvėje. Deja, į įtariamųjų, atsakingų už kibernetinėje erdvėje vykdomus įsilaužimus, susietus su intelektualinės nuosavybės, asmeninių duomenų, pinigų pasisavinimo atakomis ir tinklo paslaugų žlugdymu, sąrašą papuola ne tik dėmesio siekiantys studentai programišiai, kibernetiniai nusikaltėliai ar socialinės-politinės pakraipos programišiai, bet ir vyriausybės. 2010 m. birželio mėn. pasirodžius kenkėjiškai *Stuxnet* tipo programinei įrangai, sukurtai naikinti specialiai numatytus ypatingos svarbos infrastruktūros komponentus, buvo bene pirmasis požymis, kad kai kurios valstybės ėmėsi piktavališkos veiklos kibernetinėje erdvėje. Aktyvaus valstybių kibernetinių atakų rengimo ir vykdymo prieš ypatingos svarbos kitų valstybių infrastruktūras problema tarptautinės bendruomenės buvo ignoruojama. Šios atakos kelia nacionalinio saugumo problemų dėl grėsmių ekonominei ir socialinei valstybių gerovei. Tačiau kai visur esanti kibernetinė erdvė yra kaip bendra aplinka, kur vyksta visi šiuolaikiniai pramoniniai procesai ir plėtojama sąveika tarp kitų valstybių ypatingos svarbos infrastruktūrų, kibernetinio saugumo klausimai peržengia vienos valstybės ribas. Tarptautinė bendruomenė privalo imtis priemonių, kurios užtikrintų, kad valstybėms naudojant šį naująjį ginklą, jis netaptų nevaldomas ir nesukeltų naujų dar rimtesnių tarptautinių konfliktų. Pateikiami trys šios problemos sprendimai ir galimas šios ardomosios valstybių veiklos kibernetinėje erdvėje valdymo tarptautiniu lygmeniu modelis.

Įvadas

Kibernetinė erdvė nematoma, bet visur esanti elektromagnetinės veiklos, paremtos informacijos ir ryšių technologijomis, sritis glaudžiai susijusi su kitomis žmogiškosios veiklos sritimis. Šioje aplinkoje išsivystė sistemos ir procesai, apimantys šiuolaikines finansų, energetikos, transporto ir telekomunikacijų sistemas, grindžiamas naujųjų dinamiškų technologijų pajėgumais. Šios sistemos išaugo į kompleksines tarpusavyje susietas infrastruktūras ir

* *Vytautas Butrimas* – Lietuvos Respublikos krašto apsaugos ministerijos vyriausiasis patarėjas kibernetinio saugumo klausimais. Adresas korespondencijai: Totorių g. 25/3, 01121 Vilnius, tel. (8 5) 273 5775, el. p. vytautas.butrimas@kam.lt .

** Šiame straipsnyje pateikti vertinimai ir mintys yra tik autoriaus ir niekada negali būti vertinamos kaip Lietuvos Respublikos krašto apsaugos ministerijos ir jos padalinių oficiali pozicija.

procesus, kurie yra ypač svarbūs šiuolaikinės visuomenės ir ekonomikos funkcionavimui.

Kartu su naujaisiais pajėgumais atsirado ir nauji pažeidžiamumai. Priešiški veikėjai, išmanantys šiuos pažeidžiamumus, gali vykdyti kibernetines atakas, kurios pajėgios ne tik sužlugdyti ypatingos svarbos paslaugas ar pramoninius procesus, bet ir kelti grėsmę žmonių gyvybei. Nuo to, kokiu mastu kibernetinės atakos paralyžiuoja ypatingos svarbos infrastruktūrų procesus ir paslaugas, priklauso, ar saugumo klausimai yra nacionalinio ar tarptautinio lygmens. Kibernetinė ataka prieš su finansais susijusio objekto telekomunikacijų ir informacinę infrastruktūrą gali sukelti didelę visuomenės įtampą ar net vyriausybės krizę. Įsivaizduokite, kad žmonės visą savaitę negali naudotis savo kredito kortelėmis arba neturi galimybės atlikti kitų elektroninių sandorių. Kiek laiko mes galėtume gyventi naudodami tik grynuosius pinigus, jei prekybos centrai ir degalinės staiga priimtų mokėjimus tik grynaisiais (kaip Kipre, kai vyriausybė įsakė uždaryti bankus 2013 m. pavasarį)?[1] Pagalvokite apie tai, kas nutiktų, jei atominės elektrinės, naftotiekio ir (ar) geležinkelio kontrolės centro operatoriai staiga nebematytų vaizdo ir netektų galimybės valdyti neprastai svarbaus proceso? Tai pasaulyje jau yra nutikę ir sukėlė didžiulių nuostolių ir pareikalavo žmonių gyvybių.

Per pastaruosius 10 metų piktavališkos kibernetinės veiklos ir grėsmių šaltiniai buvo kibernetiniai nusikaltėliai ir kompiuterių programišiai – socialinės-politinės pakraipos programišiai. Dažniausiai, tvarkymasis su tokiais piktavališkais kibernetinės erdvės veikėjais yra paliekamas teisėsaugos institucijoms. Neseniai įvykę ir viešai nuskambėję šių individų ir mažų nusikalstamų grupuočių areštai buvo atlikti dėka suderintų vidaus ir tarptautinės teisėtvarkos organų pastangų[2]. Tarptautinė bendruomenė labiausiai linkusi suprasti kibernetinį saugumą kaip kibernetinį nusikalstamumą arba kaip kibernetinį terorizmą. Geras pavyzdys yra Europos Sąjungos arba Budapešto konvencija dėl kibernetinių nusikaltimų[3]. Kitas pavyzdys yra neseniai paskelbtas ESBO vadovas, nurodantis, kaip apsaugoti ypatingos svarbos energetikos infrastruktūras

[1] Steininger M., „What's behind the bailout crisis in Cyprus?", *Christian Science Monitor*, http://www.csmonitor.com/World/Europe/2013/0329/What-s-behind-the-bailout-crisis-in-Cyprus , 29 03 2013.

[2] Gilbert D., „Dutch Suspect Sven Olaf Kamphuis Arrested for Biggest Cyber Attack in Internet History", *International Business Times*, http://www.ibtimes.co.uk/articles/461848/20130426/spamhaus-suspect-arrests-spain-kamphuis.htm , 26 04 2013.

[3] Council of Europe, *Convention on Cybercrime*, http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm , 23 11 2001.

nuo teroristinių grėsmių, kylančių kibernetinėje erdvėje[4]. ESBO pripažino, kad šios infrastruktūros „sužlugdymas ar sunaikinimas [įvykdytas teroristų] turėtų rimtą poveikį saugumui, saugai, ekonominei gerovei žmonių sveikatai ir pasauliui apskritai“[5]. Tačiau išlieka klausimas, ar teroristai yra vieninteliai grėsmę keliantys veikėjai, galintys panaudoti kibernetinius masinio naikinimo ginklus tam, kad paralyžiuotų arba sunaikintų ypatingos svarbos infrastruktūrą. Nėra aiškių įrodymų, kad „Al-Qaida“ grupuotės tipo teroristai planuotų pasinaudoti kibernetine erdve savo atakoms. Jiems dar trūksta gebėjimų, susidomėjimo ir pajėgumų, kad galėtų patys parengti ir panaudoti kompleksinius kibernetinius ginklus. Egzistuoja dar vienas, mažai įvertintas kibernetinių grėsmių ypatingos svarbos infrastruktūrai šaltinis piktavališka valstybių veikla.

Per praėjusį dešimtmetį piktavališka valstybių veikla kibernetinėje erdvėje virto problema, kurią reikia įtraukti į tarptautinio saugumo politikos dienotvarkę. Kibernetinės atakos jau peržengė patriotinių ar politiškai motyvuotų kibernetinių riaušių, pasibaigusių laikinomis paslaugų blokavimo atakomis, nukreiptomis prieš Estijos vyriausybę, bankų ir žiniasklaidos portalus 2007 m., ribas. Nuo tada jos pakito: imta naudoti kibernetinius ginklus, galinčius sunaikinti ypatingos svarbos infrastruktūras. Tokiais pavyzdžiais gali būti laikoms kibernetinės atakos, prasidėjusios 2009 m. prieš Irano branduolinius objektus, 2012 m. Saudo Arabijos naftos pramonę ir 2012 m. pabaigoje ir 2013 m. pradžioje prieš finansines Jungtinių Amerikos Valstijų institucijas.

Nesiėmus tarptautinių veiksmų, nukentėjusių valstybių reakcija į šias atakas vedė prie kibernetinės ginkluotės varžybų pradžios ir netgi prie grasinimų atsakomuoju smūgiu[6]. Tarptautinės institucijos, kurių užduotis yra skatinti taiką ir tarptautinę tvarką, nepasiekė sutarimo, kokių veiksmų imtis šiuo atveju. Tačiau problema ir toliau neišnyks, kadangi kibernetinės atakos, nukreiptos prieš ypatingos svarbos infrastruktūras, turi didelį valstybių sienas peržengiantį poveikį, kuris gali destabilizuoti tarptautinę padėtį. Dabar valstybės supranta, kaip sunku nustatyti užpuoliką ir tai, kad sėkmingų paneigimų kaina yra palyginti nedidelė. Kokius naujus iššūkius ši piktavališka valstybių veikla kibernetinėje erdvėje kelia formuojant tarptautinę saugumo politiką? Kuo rizikuoja tarptautinė bendruomenė nesiimdama veiksmų, kad ši problema būtų sprendžiama? Ką galima būtų padaryti siekiant išspręsti šią problemą

[4] Organisation for Security and Cooperation in Europe, *Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP) from Terrorist Attacks Focusing on Threats Emanating from Cyberspace* , http://www.osce.org/atu/103500, 2013.

[5] Ten pat, p.7.

[6] Alexander D., „US reserves right to meet cyber attack with force“, *Reuters*, http://www.reuters.com/article/2011/11/16/us-usa-defense-cybersecurity-idUSTRE7AF02Y20111116, 15 11 2011.

ir sumažinti galimybę kibernetinei atakai peraugti į didesnį konfliktą? Straipsnyje bus aptartos šios problemos ir tarptautinė bendruomenė skatinama kreipti daugiau dėmesio į piktavališkos valstybių kibernetinės veiklos problemas ir jas spręsti .

1. Aplinkoje, kur nėra kibernetinės erdvės „šerifo“, valstybės tampa kibernetinės erdvės „nusikaltėlėmis“

2007 m. piktavališka valstybių veikla atsirado kaip naujas kibernetinių grėsmių, nukreiptų prieš ypatingos svarbos infrastruktūras, šaltinis. Jau buvo daug rašyta apie 2007 m. balandžio mėn. paslaugų blokavimo kibernetines atakas, nukreiptas prieš elektroninius Estijos vyriausybės ir bankų tinklus. Jos buvo pavadintos pirmuoju kibernetiniu karu[7], galimai vykusiu vyriausybei palaikant. Nors šios paslaugų blokavimo atakos buvo laikinai sėkmingos, jos nepadarė realios ilgalaikės fizinės kompiuterinės įrangos ar informacinių sistemų žalos. Bronzinio kario statulos incidentas buvo pakankama priežastis, susivienijusiems prorusiškiems kibernetiniams nusikaltėliams ir politiniams programišiams sukelti kibernetines riaušes. Nors buvo neįmanoma įrodyti, estai laikė savo kaimynę Rusiją atsakinga už šias atakas. Verta prisiminti, kad Estija buvo priversta atsijungti (keletui valandų) nuo interneto. Niekas nepasitarnautų potencialaus agresoriaus veiksmams prieš valstybę labiau, negu nutrauktas aukos gebėjimas bendrauti su išoriniu pasauliu.

Dar grėsmingesnė ir verta paminėti kibernetinės erdvės ataka įvyko tų pačių metų pabaigoje. 2007 m. rugsėjo mėn. Izraelio oro pajėgos sėkmingai įsibrovė į Sirijos oro erdvę ir bombardavo slaptą branduolinį objektą. Šis, atrodo, lengvas įsibrovimas į oro erdvę sukėlė kai kurių aviacijos ekspertų įtarimų[8]. Daugeliui kilo klausimas, kaip vienai moderniausių Artimųjų Rytų oro gynybos sistemų nepavyko užfiksuoti ir reaguoti į rimtą savo oro erdvės pažeidimą ir savo suverenios teritorijos bombardavimą (beje, Sirijos oro gynyba vėliau neturėjo jokių problemų, susekė ir numušė vieną reaktyvinį Turkijos lėktuvą, skridusį virš Viduržemio jūros[9])? Ekspertai išreiškė mintį, kad Izraelio kariuomenė pasinaudojo „kibernetiniu triuku“, kad sutrikdytų ar išvestų iš

[7] Traynor I., „Russia accused of unleashing cyberwar to disable Estonia“, *The Guardian*, http://www.theguardian.com/world/2007/may/17/topstories3.russia, 15 05 2007.

[8] Carroll W., „Israel's Cyber Shot at Syria“, *Aviation Week*, http://defensetech.org/2007/11/26/israels-cyber-shot-at-syria, 26 11 2007.

[9] Burch J. „Pilot bodies from downed Turkish jet retrieved“, *Reuters*, http://www.reuters.com/article/2012/07/05/us-syria-crisis-jet-bodies-idUSBRE8640KU20120705 , 05 07 2012.

rikiuotės Sirijos oro gynybą[10]. Richardas A. Clarke'as, buvęs JAV vyriausybės patarėjas nacionalinio saugumo klausimais, manė, kad šis paaiškinimas buvo gana tikėtinas, jog būtų įtrauktas į jo knygą kaip kibernetinio karo pavyzdys[11]. Sumanytojų tikslas buvo akivaizdžiai pasiektas. Įtartinas branduolinis objektas buvo neutralizuotas beveik be jokių pasekmių puolėjams. Kaip ir Estijos kibernetinės atakos atveju, nebuvo galima įrodyti, kad vyriausybė rėmė piktavališką kibernetinę veiklą. Išmoktas pamokas apie tokių atakų efektyvumą ir tarptautinio atsako trūkumą, žinoma, pastebėjo tų atakų organizatoriai ir, galbūt, tie, kurie dar tik svarstė apie galimybę vykdyti panašias atakas.

Nors ataka prieš Sirijos karinę oro gynybos sistemą sukėlė mažai susirūpinimo, nereikia pamiršti, kad ji naudoja panašius lokatorius, kokie yra naudojami civiliniam oro eismui reguliuoti. Civilinė aviacija yra dalis transporto infrastruktūros, kurios valdymo sistemos yra pažeidžiamos kibernetinių incidentų ir atakų atveju.

2008 m. rugpjūčio mėn. kibernetinė ataka, kaip priemonė skirta laikinai sutrikdyti šalies kibernetinę erdvę, įgijo naują dar baisesnę formą – imta naudoti kibernetines atakas kartu su tradicinėmis karinėmis operacijomis. Tokia forma apėmė keletą elementų, prieš metus panaudotų atakoje prieš Estiją: masinis patriotizmas, reikiamai nukreiptas socialinių tinklų, profesionalūs užkrėstų kompiuterinių tinklų operatoriai, organizuoto nusikalstamumo elementai ir įtariama (bet neįrodyta) vyriausybės parama. Taip buvo įvykdyta gerai suplanuota, tinkamu laiku atlikta šalį silpninanti kibernetinė ataka ir prieš Gruzijos vyriausybės ir civilinių institucijų tinklus. Šios atakos metu pavyko atkirsti Gruzijos vyriausybę, jos gyventojus ir pasaulį nuo galimybės naudotis internetine informacija apie įvykius šalyje. Trumpiau tariant, Gruzijos galimybė organizuoti ir koordinuoti savo nacionalinę gynybą buvo labai komplikuota. Vienas kibernetinės atakos prieš Gruziją tyrimas teigė, kad atsirado dar pavojingesnė kryptis – galimybė fiziškai sunaikinti ypatingos svarbos infrastruktūros komponentus[12]. Neaišku dėl kokios priežasties, tačiau kaltininkai nutarė susilaikyti[13]. Nepaisant keleto areštų Gruzijoje, tarptautinė bendruomenė nesiėmė jokių veiksmų, siekdama nubausti atsakingus už šias kibernetines atakas asmenis. Buvo išmokta ir įsisąmoninta, kad piktavališki

[10] Fulghum D. A., „Why Syria's Air Defenses Failed to Detect Israelis", *Aviation Week*, http://www.aviationweek.com/Blogs.aspx?plckBlogId=Blog:27ec4a53-dcc8-42d0-bd3a-01329aef79a7&plckPostId=Blog:27ec4a53-dcc8-42d0-bd3a-01329aef79a7Post:2710d024-5eda-416c-b117-ae6d649146cd , 03 10 2007.

[11] Clarke R., *Cyber War*, Harper Collins, 2010, p. 7.

[12] Bumgarner J., Scott B., „Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008.", *U.S. Cyber consequences Unit.*, http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf , 2009, p. 5.

[13] Ten pat, p.5.

veiksmai kibernetinėje erdvėje yra patrauklus pasirinkimas, kai niekas net nebando pričiupti ir nubausti.

1.1. *Stuxnet*

2009 m. pradžioje vis dar nebuvo neginčijamų įrodymų, kad valstybės dalyvauja rengiant ir vykdant kibernetines atakas. Taip buvo iki pat 2010 m. vasaros, kai kibernetinio saugumo bendruomenę pasiekė pirmieji pranešimai apie sudėtingą kibernetinį ginklą, sukurtą atakuoti ypatingos svarbos infrastruktūras. *Stuxnet* kenkėjiškos kompiuterinės programos buvo netikėtos daugeliui analitikų. Techniniu požiūriu, pavojingiausi *Stuxnet* elementai trukdė valdyti ir kontroliuoti procesus, vykstančius kompleksinėse pramoninėse sistemose[14]. Piktavališka šio kibernetinio ginklo programavimo sistema sukeldavo įrangos ir su ja susijusių pramoninių procesų kontrolės praradimą ir „vaizdo išnykimą“. To buvo pasiekta perimant ir įvedant klaidingus operatoriams siunčiamus duomenis, rodančius, kad sistemos funkcionuoja normaliai, nors iš tikrųjų buvo priešingai. Paprasčiau tariant, poveikis buvo panašus į tai, kas nutiktų automobilio vairuotojui, kai variklio mechanizmais būtų manipuliuojama nukreipiant automobilį nuo uolos. Tokiu atveju vairuotojas nejaustų nerimo ir poreikio imtis veiksmų, kadangi kelio priekyje vaizdas, jo manymu, yra normalus. Net jei jis bandytų imtis veiksmų norėdamas išsigelbėti, paaiškėtų, kad jis negali kontroliuoti vairo, stabdžių pedalo ir variklio. *Stuxnet* yra kitoks dėl to, kad jis neatakavo „Windows“ kompiuterių. Greičiau jis siekė sugadinti įrangą, naudojamą reikšminguose gamybos procesuose. Jis nebuvo ir kibernetinis nusikaltimas, nes akivaizdu, kad nebuvo pelningas. Priešingai, techninio meistriškumo lygis ir intelektualinis indėlis, reikalingas parengti ir nukreipti šį ginklą į numatytą taikinį (urano sodrinimo gamykla Irane) rodė valstybės lygmens veiklą (norint daugiau sužinoti apie *Stuxnet* ir operaciją „Olympic Games“, verta perskaityti Davido E. Sangerio knygą)[15].

Galima sakyti, kad *Stuxnet* atsiradimas yra panašus į Hirosimos atvejį, turint galvoje pakitusią mąstymo sanklodą kibernetinio saugumo ir tarptautinių santykių srityje. Pirmoji žinoma ir įvykdyta vienos valstybės kibernetinė ataka prieš kitos valstybės ypatingos svarbos infrastruktūras parodė, kad „pirštinės nebemūvimos“. Buvo pripažinta, kad ši technologija taikoma siekiant išvesti iš rikiuotės ir sunaikinti įrenginius ir sužlugdyti pramoninius

[14] Langner R., „Cracking Stuxnet: a 21st century cyber weapon“, Ted Conferences, http://www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyberweapon.html , 03 2011.
[15] Sanger D., *Confront and Conceal*, Crown Publishers, New York, 2012, p. 504

procesus. Ši operacija, kuri tikriausiai buvo politiškai motyvuota (neleisti Irakui pasigaminti bombos), taip pat sukūrė naują problemą, nurodančią, kad kibernetiniai ginklai gali patekti mažiau kvalifikuotiems politiniams programišiams, nusikaltėliams ir netgi teroristinėms grupuotėms[16]. Deja, *Stuxnet* kodas pateko į internetą, kur jis gali būti laisvai kopijuojamas ir analizuojamas. Metodus galima išstudijuoti, o programinę sistemą pritaikyti, siekiant vykdyti naujas ardomąsias kibernetines atakas. Ypatingos svarbos infrastruktūra (telekomunikacijos, energetikos, finansų), kuri iš esmės iki tol gyvavo savame izoliuotame uždarų komunikacijos tinklų ir technologijų pasaulyje, tapo nauja programišių interesų sritimi. Ne vien vyriausybės gali ieškoti būdų, kaip išnaudoti naujai atsiradusius pažeidžiamumus ir padaryti fizinę žalą nacionalinių ypatingos svarbos infrastruktūrų pramonės valdymo sistemoms. Pirmą kartą buvo galima pagrįstai galvoti apie realaus kibernetinio terorizmo galimybes. Ši technologija dabar tapo prieinama teroristų grupuotėms, kurioms trūko gebėjimų sukurti savo kibernetinius masinio naikinimo ginklus (angl. *weapon of mass destruction*, WMD). *Stuxnet* dar kartą privertė pasimokyti iš ankstesnių kibernetinių atakų. Akivaizdi šios operacijos sėkmė ne tik prisidėjo prie reikšmingų infrastruktūrų pažeidžiamumo suvokimo, bet taip pat pateikė naują problemą tarptautinei saugumo politikos bendruomenei: ką daryti su valstybėmis, žaidžiančiomis kibernetinius žaidimus su viena kitos ypatingos svarbos infrastruktūromis? Kalbant apie ataką prieš Siriją 2007 m., *Stuxnet* operacijos kritika buvo nutildyta. Galbūt, kai kas galvojo, kad ji pasitarnavo naudingam tikslui sumažindama grėsmę (neleisti Iranui pagaminti bombos). Neįvertinama tai, kad dauguma potencialių *Stuxnet* tipo atakų taikinių, t. y. objektų, kurie yra mažiau apsaugoti (nepožeminiai) ir labiau pažeidžiami (daugiau galimybių prasiskverbti), yra ne Vidurio Rytuose, bet išsivysčiusiose šalyse Europos, Šiaurės Amerikos ir Azijos regionuose, turinčiuose ypatingos svarbos infrastruktūrų.

1.2. „Saudi Aramco“ 2012

2012 m. gruodžio mėn. dar vienos valstybės ypatingos svarbos infrastruktūra patyrė kibernetinę ataką. Saudo Arabijos naftos kompanija „Saudi Aramco“ patyrė tikslinę kibernetinę ataką prieš savo kompiuterius. Šiam kibernetiniam ginklui, pavadintam SCHAMOON, pavyko visiškai ištrinti dau-

[16] Simonite T., „Stuxnet Tricks Copied by Computer Criminals“, *MIT Technology Review*, http://www.technologyreview.com/news/429173/stuxnet-tricks-copied-by-computer-criminals/, 19 09 2012.

giau negu 30 000 kompiuterių kietųjų diskų. Atrodo, kad ši ataka apsiribojo vien kompanijos administracija ir neatakavo ypatingos svarbos infrastruktūros dalių, susijusių su naftos gamyba ir apdorojimu. Tačiau Saudo Arabijos žmonės šią kibernetinę ataką traktavo kaip grasinančią ne tik ypatingos svarbos energetikos infrastruktūrai, bet ir jų ekonomikai[17]. Nors įtikinamų įrodymų nebuvo, įtarimas, kad už tai atsakinga kitos vyriausybės kibernetinė jėga[18], buvo stiprus. Dar kartą buvo pabrėžta, kad kibernetinės atakos yra patrauklus ir labai efektyvus įrankis, norint mažomis sąnaudomis pridaryti priešininkui žalos ir nebūti teisiškai už tai atsakingiems. Šią problemą vis labiau sunkino tai, kad atsirado požymių, jog šios atakos buvo kontrsmūgiai, surengti kaip atsakas į ankstesnes atakas[19]. Be to, atrodė, jog ima ryškėti tam tikras modelis. Tokie rajonai, kaip Vidurio Rytai, žinomi dėl ilgalaikių rusenančių konfliktų, įsiliejo į kibernetinę erdvę kaip nauja konflikto dimensija ir atvirkščiai. Dar vienas to pavyzdys yra kibernetinė ataka prieš Pietų Korėjos vyriausybės žinių agentūras ir finansų tinklus, kuri baigėsi daugiau nei 30 000 kompiuterių ir jų duomenų sunaikinimu[20].

2. Tarptautinių organizacijų reakcija į savo narių veiksmus kibernetinėje erdvėje

Kokia buvo tarptautinės bendruomenės reakcija į šių valstybės remiamų kibernetinių atakų panaudojimą prieš kitos valstybės ypatingos svarbos infrastruktūrą? Atsakymas: praktiškai jokios. Atsimenu dalyvavimą Interneto valdymo forumo (angl. *Internet Governance Forum*, IGF), turinčio Jungtinių Tautų mandatą, susitikimuose Vilniuje 2010 m. rugsėjo mėnesį. Interneto privatumas ir prieigos laisvė buvo dominuojantys klausimai, tačiau, kaip teigė kai kurie autoriai[21], IGF ignoravo rimtesnius įvykius kibernetinėje erdvėje, susijusius su nacionalinio saugumo klausimais ir tiesiogiai susijusius su aptariamomis problemomis. Šiame ir kituose tarptautiniuose forumuose praktiškai ne-

[17] AL Arabiya with AFP, „Saudi Aramco says cyber-attack targeted kingdom's economy", *Al Arabiya News,* http://english.alarabiya.net/articles/2012/12/09/254162.html, 09 12 2012.
[18] Perlroth N., „In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back „, *New York TImes*, http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html, 23 10 2012.
[19] Ten pat.
[20] Dunn J., „South Korean cyberattacks used hijacked patch management accounts", http://www.pcworld.com/article/2031860/south-korean-cyberattacks-used-hijacked-patch-management-accounts.html#tk.nl_today, *PC World*, 23 03 2013.
[21] Transcript, *Internet Governance Forum*, http://www.intgovforum.org/cms/component/content/article/102-transcripts2010/658-sop, 10 09 2010.

figūravo klausimas, kaip reikėtų vertinti trečiąjį kibernetinių grėsmių šaltinį, t. y. tam tikrų valstybių veiklą. Tų pačių valstybių, kurios yra aljansų narės ir kartu su kitomis dalyvauja konferencijose ir forumuose, prižiūrinčiuose kibernetinį saugumą, interneto laisvės ir gynybos politiką.

Tam tikros pastangos dėl valstybių dalyvavimo kibernetinėse atakose problemos sprendimo vis tik buvo dedamos. Šanchajaus bendradarbiavimo organizacija (Rusija, Kinija, Tadžikistanas, Uzbekistanas) iš tikrųjų 2011 m. rugsėjo mėn. pateikė Jungtinių Tautų Generalinei Asamblėjai laišką, siūlydama Tarptautinį elgsenos kodeksą dėl informacijos saugumo[22]. Tarp kitų pasiūlymų buvo ir pasiūlymas valstybėms susilaikyti ir nenaudoti šių technologijų prieš viena kitos ypatingos svarbos infrastruktūras. Tačiau Vakarų šalys jį greit atmetė[23] kaip per daug šališką ir palankų autoritarinėms valstybėms, siekiančioms kontroliuoti informaciją kibernetinėje erdvėje ir nepatogų socialinį-politinį aktyvumą. Šiuo atžvilgiu Vakarų valstybės pasirodė dviveidės, kadangi pačios senbuvės turi autoritarizmo požymių, to įrodymas gali būti valstybės vidaus ir užsienio elektroninio šnipinėjimo atskleidimas 2013 m., kuris, manoma, apėmė netgi draugiškų valstybių elektroninius ryšius[24].

ESBO bandė spręsti šią problemą. 2011 m., Lietuvai pirmininkaujant ESBO, Vienoje įvyko konferencija, kurioje buvo svarstoma ar ESBO patirtis ginkluotės kontrolės klausimais galėtų būti taikoma kibernetinei erdvei. 2011 m. vasarą ir rudenį šio straipsnio autorius dalyvavo diskusijose apie galimas kibernetinės erdvės Pasitikėjimo ir saugumo įtvirtinimo priemones (angl. *Confidence- and Security-Building Measures*, CSBM). Pagal ESBO sprendimą PC1039, neformali darbo grupė turėjo parengti CSBM projektą, kuris vėliau tais metais būtų pateiktas ministrų susitikimuose Vilniuje. Nors buvo aptarta daug pasiūlymų, nebuvo pateikta tokio, kuris kaip nors apribotų ar suvaržytų piktavališką valstybės veiklą kibernetinėje erdvėje[25]. Deja, bendro susitarimo nepavyko pasiekti ir ESBO ministrų susitikime jokių pasiūlymų dėl CSBM nebuvo pateikta.

2012 m. pabaigoje, Dubajuje, JT Tarptautinė telekomunikacijų sąjunga (angl. *International Telecommunication Union,* ITU) organizavo Pasaulinę tarptautinių komunikacijų konferenciją (angl.*, World Conference on Inter-*

[22] Maurer T., „Cyber norm emergence at the United Nations - An Analysis of the Activities at the UN Regarding Cyber-security“, *Belfer Center for Science and International Affairs*, http://www.un.org/en/ecosoc/cybersecurity/maurer-cyber-norm-dp-2011-11.pdf, 09 2011, p.6668.

[23] Farnsworth T. , „China and Russia Submit Cyber Proposal“, *Arms Control Association*, http://www.armscontrol.org/act/2011_11/China_and_Russia_Submit_Cyber_Proposal 11 2011.

[24] BBC, „Brazil and Mexico probe claims US spied on presidents“, http://www.bbc.co.uk/news/world-latin-america-23938909, 02 09 2013.

[25] Aš žinau, nes buvau vienas iš tų, kurie bandė pateikti tokį pasiūlymą (aut. pastaba).

national Telecommunications, WCIT). Ši konferencija buvo labai įdomi dėl daugelio priežasčių. ITU bandė skatinti atnaujinti būdą, kaip pasaulinės komunikacijos turėtų būti reguliuojamos. Buvo pasiūlymų atnaujinti nuostatus įtraukiant tai, ko nebuvo paskutinį kartą tvirtinant reglamentą 1989 m., t. y. nuostatas apie internetą. Nors WCIT susitikimuose nepavyko pasiekti susitarimo dėl atnaujinto telekomunikacijų reglamento interneto atžvilgiu, jų metu buvo atskleista kita problema augantis nesutarimas tarp Rytų ir Vakarų interneto valdymo klausimais. Tapo akivaizdu, kad didėja susirūpinimas tarp Rytų valstybių (ypač Rusijos ir Kinijos) dėl Vakarų valstybių (ypač JAV) dominavimo, sprendžiant, kaip kontroliuoti internetą. Demokratinės šalys buvo linkusios palaikyti daugiašalį interneto valdymo būdą (su minimaliu vyriausybės dalyvavimu), o autoritarinės vyriausybės siekė didesnės vyriausybės kontrolės reguliuojant interneto turinį ir naudojimą. Interneto „laisvės" šalininkams džiūgaujant dėl „JT nesėkmės „perimti internetą"[26], pavojingas skilimas tarp Rytų ir Vakarų dėl kibernetinės erdvės valdymo išliko[27]. Aptariant šį klausimą būtų verta paminėti dokumentą „Talino vadovas dėl tarptautinės teisės, taikytinos kibernetiniams karams" (toliau Talino vadovas). Jis buvo parengtas taip vadinamos nepriklausomos tarptautinės ekspertų grupės NATO Bendros kibernetinės gynybos kompetencijų centro Estijoje prašymu[28]. Šis Talino vadovas pateikia kibernetinės erdvės analizę ir gaires, kaip turi būti taikomos nustatytos tarptautinės normos naujoje kibernetinės erdvės srityje. Pateikti požiūriai ir duomenys nėra įpareigojantys, bet tarptautinių ekspertų sąrašas rodo, koks svarbus ateityje bus šis Talino vadovas kaip elgsenos kibernetinėje erdvėje orientyras. Būtina pažymėti, kad ekspertai, prisidėję prie minėto Talino vadovo kūrimo, yra išimtinai iš Vakarų šalių, atstovų iš šalių (ypač iš Rytų), apimančių didžiąją dalį interneto vartotojų, nebuvo įtraukta. Tai, kad šiame sąraše Rytų šalys praktiškai neatstovaujamos, nepadės bendrai priimti šio Talino vadovo kaip orientyrą, skirto politikos strategams, siekiantiems bendradarbiavimo sprendžiant kibernetinio saugumo klausimus. Tikimasi, kad rengiant atnaujintą Talino vadovo versiją, bus pakviesti dalyvauti plačiau atstovaujantys pasaulį ekspertai.

---

[26] Klimburg A., „The Internet Yalta", *Center for a New American Security*, http://www.cnas.org/theinternetyalta, 02 02 2013, p. 2.

[27] Gewirtz D., „Take action before the UN, Russia, and China hijack the Internet", *ZDNET*, http://www.zdnet.com/take-action-before-the-un-russia-and-china-hijack-the-internet7000008003/?s_cid=e539#postComment , 28 11 2012.

[28] NATO Cooperative Cyber Defence Centre of Excellence, http://www.ccdcoe.org/249.html , 2013.

3. Kaip valstybės reagavo į savo kaimynų veiksmus kibernetinėje erdvėje?

Kaip jau buvo minėta, tarptautinė bendruomenė nepadarė pakankamos pažangos kolektyviai reaguodama į piktavališką kibernetinę valstybių veiklą kibernetinėje erdvėje. Kibernetinė erdvė ir toliau lieka nevaldoma teritorija, panašia į Laukinius Vakarus, kur nėra šerifų ar raitųjų tvarkos sergėtojų. Tačiau valstybės jau suvokė šį naują pavojų ir reagavo sukurdamos padalinius, kurių konkreti užduotis – kibernetinė gynyba. Tai nėra nereikšminga tendencija. 2007 m. viena tyrimo studija nustatė, kad tokie padaliniai yra daugiau nei 120 šalių[29].

Pateikiame trumpą sąrašą šalių, kurių vyriausybės, kaip žinoma, turi kibernetinės gynybos ar puolimo padalinius: Australija, Belgija, Brazilija, Kanada, Kinija, Suomija, Vokietija, Indija, Iranas, Izraelis, Japonija, Malaizija, Pietų Korėja, Šiaurės Korėja, Jungtinė Karalystė, Rusija. Bene labiausiai viešai žinoma yra Jungtinių Valstijų reakcija į piktavališką kibernetinę valstybių veiklą [30]. Tokia veikla kibernetinėje erdvėje yra rimta JAV problema, nes ji vis tampa kibernetinio šnipinėjimo ir kibernetinių atakų auka. Suprantama, kad valstybės pastebėjo, jog JAV traktuoja kibernetinę erdvę kaip „operatyvinę sritį“[31], aktyviai kuria savo kibernetines pajėgas, yra susijusi su *Stuxnet* tipo kibernetinių ginklų kūrimu, naudojimu ir yra įtariama vidaus ir užsienio elektroninių ryšių sekimu.

Kinijos kariuomenė yra susijusi su kibernetinio karo padaliniu PLA 61398, apie kurį buvo neseniai sužinota iš viešo pranešimo[32]. Informacijos apie Rusijos vyriausybės kibernetinius padalinius[33] buvo paviešinta mažiau, tačiau atrodo, kad ji ne mažiau aktyvi negu kitos didžiosios kibernetinės valstybės. Atrodo, kad Australijos ryšių direktoratas nori, kad visiems būtų žinoma apie jo planus. Jo interneto svetainės moto yra „Atskleisk jų paslaptis, savą-

[29] „In the Crossfire“, *McAfee*, http://www.mcafee.com/us/resources/reports/rp-in-crossfire-critical-infrastructure-cyber-war.pdf, 2009.
[30] Sanger D., „Budget Documents Detail Extent of U.S. Cyberoperations“, *New York Times*, http://www.nytimes.com/2013/09/01/world/americas/documents-detail-cyberoperations-by-us.html, 31 08 2013.
[31] U.S. Depatarment of Defense, *Department of Defense Strategy for Operating in Cyberspace*, http://www.defense.gov/news/d20110714cyber.pdf 17 07 2011, p. 5.
[32] Mandiant, *APT1 Exposing One of China's Cyber Espionage Units*, http://intelreport.mandiant.com/, 2013.
[33] Sridharan V., „Russia Setting up Cyber Warfare Unit Under Military“, *International Business Times*, http://www.ibtimes.co.uk/articles/500220/20130820/russia-cyber-war-hack-moscow-military-snowden.htm, 20 08 2013.

sias saugok“[34]. Valstybės taip pat aktyviai naudojasi konjunktūra, siekdamos gauti kuo daugiau informacijos apie kibernetinių atakų rengimą ir ginkluotę joms vykdyti[35]. Vertingiausia yra informacija apie neskelbiamus programinės įrangos pažeidžiamumus, žinomus kaip „nulinė diena“. Informacija apie šiuos pažeidžiamumus, kurią galima labai sėkmingai panaudoti, galėtų sudaryti sąlygas ne vienam programišiui praturtėti ir, galbūt, padėtų jam gauti darbą su vyriausybe susijusiose institucijose. Kokia motyvacija slypi už šios veiklos, kuri prilygsta Šaltajam karui ir yra panaši į kibernetinio ginklavimosi varžybas tarp valstybių?

Galbūt, valstybės jau suprato, ką reiškia *Stuxnet*. *Stuxnet* parodė, kad kenkėjiška programinė įranga gali būti sukurta kaip kibernetinis ginklas, nukreiptas prieš ypatingos svarbos valstybės infrastruktūrą. Padaryta žala gali būti reali ir, priešingai nei raketų ataka, ji nesukelia adekvataus atsako ir palieka labai mažą galimybę susekti ir nustatyti kaltininko buvimo vietą. Kibernetinį ginklą naudoti yra naudinga. Taip, jis yra brangus, tačiau pigesnis už reaktyvinį naikintuvą ar bombonešį. Pavyzdžiui, išlaidos kuriant, bandant ir paleidžiant *Stuxnet*, galėjo kainuoti apie 10 milijonų JAV dolerių[36]. Tai tikrai maža kaina už gerai įtvirtintų požeminių įrenginių darbo nutraukimą, užpuolikui nepatiriant nuostolių ir liekant neapkaltintam. Palyginti mažos išlaidos ir atsakomybė yra du pagrindiniai privalumai, kuriuos turi valstybės, siekiančios efektyvaus, saugaus būdo be realios atsakomybės, norėdamos pasiekti nepavykusios užsienio politikos tikslų. Gali būti, kad valstybės jaučiasi verčiamos vystyti kibernetinius gynybos (puolimo) pajėgumus, siekdamos apsiginti nuo tokių atakų ir jas atgrasyti. Nors apie *Stuxnet* daug rašyta nuo tada, kai jis pirmą kartą buvo aptiktas 2010 metais, tačiau tarptautinėje bendruomenėje ir dabar tebetvyro keista tyla. Valstybės siekia gauti informacijos apie „nulinės dienos“ (angl. *zero day*) pažeidžiamumus , ketindamos apsiginti arba norėdamos panaudoti ją savo pačių puolamosioms operacijoms. Tačiau šis susirūpinimas, panašiai kaip jūros vandens gėrimas, kai esi ištroškęs, gali duoti priešingą rezultatą, skaidrumo ir pasitikėjimo prasme.

Kai kurios didžiosios kibernetinės valstybės, tokios kaip JAV, mėgino demonstruoti tam tikrą lyderystę, skatindamos sukurti bendrąją kibernetinės erdvės politiką. Pavyzdžiui, 2011 metų gegužės mėn. JAV vyriausybė paskelbė

[34] Australian Government, Department of Defence, http://www.dsd.gov.au/, 2013.

[35] Perlroth N., Sanger D., „Nations Buying as Hackers Sell Flaws in Computer Code“, *New York Times*, http://www.nytimes.com/2013/07/14/world/europe/nations-buying-as-hackers-sell-computer-flaws.html, 13 07 2013.

[36] Langner R., „The short path from cyber missiles to dirty digital bombs“, Langner Communications GmbH, http://www.langner.com/en/2010/12/26/the-short-path-from-cyber-missiles-to-dirty-digital-bombs/, 26 10 2010.

savo „Tarptautinę kibernetinės erdvės strategiją“[37]. Ji skelbė savo tikslą tarptautinei bendruomenei: „skatinti atvirą, suderinamą, saugią, patikimą informaciją ir ryšių infrastruktūrą, kuri remia tarptautinę prekybinę ir komercinę veiklą, stiprina tarptautinį saugumą ir skatina laisvos valios išraišką ir inovacijas. Siekdami šio tikslo, mes sukursime ir išlaikysime tokią aplinką, kurioje atsakingos elgsenos normos lemia valstybės veiksmus, palaiko partnerystę ir remia teisinės valstybės principus kibernetinėje erdvėje.“[38] Iš tiesų, įspūdingas pareiškimas, kurį padarė viena iš pagrindinių kibernetinių valstybių pasaulyje apie bendrąją politiką kibernetinėje erdvėje. Tačiau jis buvo pateiktas praėjus dvejiems metams po *Stuxnet* paleidimo (veiksmo, kurį daugelis didžia dalimi priskiria pačioms Jungtinėms Amerikos Valstijoms)[39]. Minėtos strategijos išleidimas tuo metu, kai *Stuxnet* atsirasdavo daugelyje pasaulio kompiuterių, vertė matyti JAV kibernetinę politiką kaip piktavališką ir kaip nepiktybinę tuo pačiu metu. Negalima kaltinti kitų valstybių, jei jos yra sutrikusios. Jos, matyt, norėtų žinoti, ar JAV žiūri į kibernetinę erdvę kaip į bendradarbiavimo aplinką ar kaip į erdvę konfliktams[40].

Matyti, kad kai kurios valstybės nepriėmė JAV pasiūlymo dėl taikaus kibernetinės erdvės panaudojimo, kur būtų vadovaujamasi teisinės valstybės principais. Vietoj to jos ėmėsi atsakomųjų priemonių. Pavyzdžiui, po 2012 metų balandžio mėn. įvykdytos *Stuxnet* kibernetinės atakos prieš Irano branduolinį objektą ir po kibernetinės atakos prieš kitą jos ypatingos svarbos infrastruktūros dalį (naftos pramonę)[41], 2012 m. gruodžio mėn. buvo surengta kibernetinė ataka prieš Saudo Arabijos naftos pramonę[42]. 2012 metų pabaigoje ir 2013 metų pradžioje rimtos kibernetinės atakos buvo nukreiptos prieš JAV finansų sistemą[43]. Dėl šių atakų Jungtinės Valstijos tuoj pat apkaltino Iraną[44]. Turint galvoje šias augančio masto ir ilgai trunkančias atakas prieš energetikos ir finansų sektorius, kyla klausimas, ar situacija netampa nekontroliuojama.

---

[37] The White House, *International Strategy for Cyberspace*, http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf, 05 2011.

[38] Ten pat, p. 8.

[39] Sanger D., „Obama Order Sped Up Wave of Cyberattacks Against Iran“, *New York Times*, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=0, 01 06 2012.

[40] Healey J, *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, Cyber Conflict Studies Association, 2013, p. 77.

[41] Roberts P., „Iran Acknowledges Hack Of Oil Ministry“, *Threat Post*, http://threatpost.com/iran-acknowledges-hack-oil-ministry-042312/76470, 23 04 2012.

[42] Al Arabiya and AFP, „Saudi Aramco says cyber attack targeted kingdom's economy“, *Al Arabiya* News, http://english.alarabiya.net/articles/2012/12/09/254162.html , 09 12 2012.

[43] Rothman P., „Cyber terror rages in the banking sector“, http://www.securityinfowatch.com/blog/10796084/cyber-terror-rages-in-the-banking-sector , 28 09 2012.

[44] Perlroth N., „In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back“, New York Times, http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html, 23 10 2012.

4. Kur tai veda ir kodėl reikia kažką daryti, siekiant apsaugoti kibernetinę erdvę?

Kaip visa tai veikia taiką ir stabilumą? Kibernetinių ginklų, kaip pigaus, efektyvaus būdo be realios atsakomybės, siekiant kitaip nepasiekiamų užsienio politikos tikslų, patrauklumas, neliko valstybių nepastebėtas. Šie ginklai gali būti panaudoti, norint sužlugdyti arba sunaikinti slaptą informacinę technologiją ir įvairius telekomunikacijų komponentus. Tai, apie ką kalbame, ir yra svarbūs strateginiai elementai, kurie sudaro svarbiausių nacionalinių infrastruktūrų, atsakingų už elektros energijos gamybą, telekomunikacijas, finansų sistemas, transportą ir kitas struktūras, kurių funkcionavimas užtikrina gyvybiškai svarbias paslaugas šiuolaikinių pramoninių valstybių ekonomikai ir socialinei gerovei, pagrindą. Tas faktas, kad kaltės priskyrimas, t. y. atsakingų už atakas nustatymas, yra labai sudėtingas, suteikia pranašumo užpuolikui, ieškančiam lengvų būdų žalai padaryti. Kita vertus, tiems, kurie rūpinasi gynyba, tai sukelia įtarimą ir verčia jaustis nesaugiai kaimynų ketinimų atžvilgiu. Kodėl mano kaimynas mane šnipinėja? Kodėl mano kaimynai kuria kibernetines pajėgas? Ką jie planuoja daryti (ar jau daro) su jomis? Gal ir man reikia tokias pajėgas sukurti? Sunku rasti įtikinamų atsakymų į šiuos klausimus tokioje mažo skaidrumo ir menko pasitikėjimo aplinkoje. Sunku nesutikti su tais, kurie kalba apie kibernetinio ginklavimosi varžybų pradžią[45].

Reikia atsižvelgti ir į tai, kokį spaudimą gali patirti vadovai, verčiami kaip nors veikti, kai atakuojama svarbi jų valstybės infrastruktūra. Visiškai įmanoma, kad pasirinkus atsakomąsias priemones, jos gali būti nukreiptos prieš nekaltą šalį, o ne prieš tikrąją kaltininkę. Pavyzdžiui, yra kai kurių požymių, kad kibernetinė ataka, nukreipta prieš Pietų Korėją 2013 metų pavasarį, galėjo būti sukurta arba Šiaurės Korėjoje, arba Kinijoje[46]. Kaip šalis gali būti tikra, kad ji teisingai nustatė atakos kaltininkę? Šis tikrumo trūkumas, susijęs su kaltininko nustatymu, yra dar vienas santykių nestabilumo požymis.

Kibernetinės erdvės naudojimas yra klausimas, dėl kurio kyla rimtų nesutarimų tarp didžiųjų valstybių. Tai, kaip šios valstybės reaguoja, taip pat didina jų tarpusavio santykių ir santykių su kitomis valstybėmis, patekusiomis į „kryžminę ugnį", nestabilumą. JAV ir Kinijos tarpusavio kaltinimai dėl kibernetinio šnipinėjimo ir viena kitos ypatingos svarbos infrastruktūrų kiber-

[45] Guy-Philippe Goldstein, „How cyberattacks threaten real-wold peace", Ted Conferences, http://www.ted.com/talks/guy_philippe_goldstein_how_cyberattacks_threaten_real_world_peace.html, 10 2011.
[46] Donohue B., „South Korea Blames North Korea for March Cyberattack", *Threat Post*, http://threatpost.com/south-korea-blames-north-korea-march-cyberattack-041013, 13 04 2013.

netinė žvalgyba yra geri to pavyzdžiai[47]. Svarstydamas galimus JAV motyvus, slypinčius *Stuxnet* sukūrime, vienas iš komentatorių pateikė nerimą keliančią išvadą. Jis teigia, kad ši kibernetinė supervalstybė, reaguodama į atakas prieš savo kibernetinės erdvės objektus, panaudojo *Stuxnet* norėdama pranešti savo potencialiems priešininkams: „Gerai pagalvokite, prieš atakuodami mus. Tai pavyzdys to, ką galime padaryti. Mes ir vėl tai padarysime.“[48] Galbūt galima suprasti norą atgrasinti potencialų agresorių, giriantis savo kibernetine ginkluote, tačiau kibernetinės erdvės naudotojui, gyvenančiam ne JAV, maža paguoda. Neteisinga galvoti, kad kibernetinis ginklas turi būti naudojamas, norint atgrasinti ir daryti įtaką kitiems, siekiant, kad jie elgtųsi kitaip. Daugeliu atvejų, tai sugebėjimas, kurį gali vienodai turėti tiek galingosios, tiek ir ne tokios galingos valstybės. Nepaisant didelių branduolinio klubo narystės reikalavimų, šiandien bet kuri valstybė gali sukurti arba įsigyti rinkoje savo skaitmeninį kodą kibernetiniam ginklui ir gali tapti kibernetine valstybe.

Dar vienas susirūpinimą keliantis dalykas yra tas, kad valstybių ypatingos svarbos infrastruktūros yra stipriai susijusios tarpusavyje. Kibernetinė erdvė ir yra ta aplinka, kurioje vyksta šiuolaikinė prekyba ir tarptautiniai ryšiai. Piktybiškai nusiteikusi valstybė ar aktyvi patriotiška „kibernetinė kariuomenė“, atsakydama į kibernetinę ataką ir nukreipdama savo kibernetinę ginkluotę prieš šalį tariamą kaltininkę, gali sukelti nenuspėjamas pasekmes. Taip yra dėl to, kad kibernetinė erdvė visame pasaulyje yra labai susijusi su kitais tinklais ir sistemomis. Atakos (ir bet kokios kontratakos, kurių bandytų imtis taikinys), greičiausiai, pereitų per nenuspėjamą skaičių tinklų ir sistemų, esančių kitose šalyse. Tikėtina, kad dėl ypatingos svarbos infrastruktūros tarpvalstybinio pobūdžio (pavyzdžiui, dėl bendrų elektros tinklų arba dujų vamzdynų) tokių konfliktų padariniai palies ir kitas nacionalines infrastruktūras ir institucijas[49]. Atsakomosios operacijos į kurios nors valstybės kibernetinę ataką, manant, jog toji yra už ją atsakinga, gali turėti neprognozuojamų pasekmių, nepaisant to, kad tai galėtų būti pateisinama.

Netgi kibernetinio šnipinėjimo atvejį galima interpretuoti kaip karinį veiksmą (tiesą sakant, taip manė JAV, kai ji nustatė Rusijos vykdomą kiberne-

[47] Healey J., *A Fierce Domain: Conflict in Cyberspace, 19862012*, Cyber Conflicts Studies Association, 2013, p. 171-173.

[48] Morton C., „Stuxnet, Flame, and Duqu – the Olympic Games“ in Healey J., ed., *A Fierce Domain: Conflict in Cyberspace, 1986-2012*, Cyber Conflicts Studies Association, 2013 p. 231.

[49] National Research Council of the National Academies, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, http://www.nap.edu/openbook.php?record_id=12651&page=R1 , The National Academies Press, 2009, p.4649.

tinio šnipinėjimo atvejį)[50]. Kai kas gali paskubėti priimti kibernetinį šnipinėjimą kaip dalį priimtos „realiojo" pasaulio tvarkos. Iš tikrųjų, viskas yra kitaip, kai šnipinėjimas vykdomas elektroniniu būdu kibernetinėje erdvėje. Skirtingai nuo tradicinio šnipinėjimo, kai žmogus vagia informaciją, kibernetinio šnipinėjimo veikla yra specifinė, nes elektroniniam šnipui įsiskverbus į sistemą, reikia labai mažai pastangų, norint pereiti nuo šnipinėjimo (dokumentų parsisiuntimo) iki sabotažo veiksmų. Šnipas gali palikti loginę bombą pagrindinėje sistemoje, kuri vėliau pagal komandą galėtų suveikti. Tai vadinama mūšio lauko parengimu. Įsiskverbus į sistemą ir joje įsitvirtinus, beveik nebelieka skirtumo, kuris veiksmas vykdomas šnipinėjimo ar sabotažo. Užtenka nuspausti ENTER klavišą. Tokia kovos lauko parengimo veikla, jei ją aptinka auka, gali būti labai provokuojanti ir tam tikros įtampos metu gali lengvai peraugti į rimtą konfliktą.

Dar viena įtampos tarp valstybių priežastis yra kibernetinės atakos kaip įrankis, siekiant daryti įtaką kaimynų vidaus politikai[51]. Pavyzdžiui, galimas dalykas, jog būtent tai buvo kibernetinės atakos prieš Estiją 2007 metais pagrindas. Suaktyvėjo patriotinės riaušininkų grupuotės, remiančios savo vyriausybės (šiuo atveju – Rusijos) politiką arba propaguojančios savo pačių programą[52]. Kaip valstybės toliau spręs šių savanoriškų „kibernetinių karinių grupuočių" veiksmus santykių su kitomis valstybėmis atžvilgiu? Kaip jos reaguos į kitų vyriausybių nusiskundimus dėl atakų, kurias surengė šios kariuomenės, esančios jų teritorijoje?

Pranašumai, kuriuos potencialiam užpuolikui suteikia kibernetiniai ginklai, t. y. jų ekonomiškumas ir „nepakaltinamumas", labai vilioja. Valstybės pripažįsta, kad jos tampa vis labiau priklausomos nuo kibernetinės erdvės tam, kad galėtų augti jų ekonomika ir visuomenės gerovė. Jei nėra jokios kibernetinės policijos, kurią prireikus galima būtų pasitelkti, valstybės ir toliau kuria savo kibernetinius pajėgumus. Šioje netikrumo ir įtarumo aplinkoje bet koks kibernetinis konfliktas gali greitai peraugti į didesnius tarpvalstybinius konfliktus. Taip pat tikėtina, kad kartu su bet kokiu tradiciniu tarpvalstybiniu konfliktu bus ir kibernetinės atakos komponentų, kurie apsunkins to konflikto sprendimą. Logiška, kad tarptautinės organizacijos yra vieta, kur galima būtų ieškoti „teisėjų" šiose naujose ir potencialiai žlugdančiose varžybose.

---

[50] Elkus A., „Moonlight Maze" in Healey J., ed., *A Fierce Domain: Conflict in Cyberspace, 19862012*, Cyber Conflicts Studies Association, 2013, p. 152160.

[51] Healey J., *A Fierce Domain: Conflict in Cyberspace, 19862012*, Cyber Conflicts Studies Association, 2013, p. 191.

[52] McAfee Labs, *McAfee Threats Report: First Quarter 2013*, McAfee, http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q1-2013.pdf , 2013, p. 33.

5. Ką gali padaryti tarptautinė bendruomenė, norėdama sumažinti konflikto, kylančio dėl piktavališkos valstybių veiklos kibernetinėje erdvėje, eskalavimo pavojų?

Užduotis siūlyti sprendimus dėl piktavališkos valstybių veiklos kibernetinėje erdvėje negali būti priskirta aukštųjų technologijų specialistams, dirbantiems Informacinių technologijų ministerijoje ar įsigijimų departamentuose, teisėtvarkos institucijose, slaptosiose žvalgybos tarnybose ar sukarintuose kibernetiniuose padaliniuose. Šias sudėtingas problemas, į kurias įeina reagavimas ir susidorojimas su šios tarptautinę dimensiją turinčios veiklos padariniais, gali išspręsti tik politikai ir saugumo politikos formuotojai. Norint pasiekti konkrečių rezultatų, šį darbą reikia atlikti susitelkusios tarptautinės bendruomenės, kuri įsipareigojusi sukurti tarptautiniu mastu privalomus sprendimus, kontekste. Šis tikslas būtų: sukurti tarptautinį susitarimą dėl valstybių elgsenos normų ir pasitikėjimo didinimo, atsakomybės ir skaidrumo tarp valstybių kibernetinėje erdvėje.

Pasiūlymai, kaip spręsti netinkamos valstybių elgsenos kibernetinėje erdvėje klausimą:

1. Įsipareigojimas susilaikyti nuo piktavališkos kibernetinės veiklos, nukreiptos prieš ypatingos svarbos civilinę infrastruktūrą (finansų, energijos tiekimo, transporto ir telekomunikacijų).

Argumentai. Noras apsaugoti valstybinę ekonomiką ir civilius gyventojus nuo finansinių nuostolių ir fizinės žalos turi būti bendras visoms valstybėms. Dėl tam tikros valstybės veiklos kibernetinėje erdvėje valstybių tarpusavio santykiuose gali atsirasti klaidingas supratimas ir nestabilumas. Pavyzdžiui, loginių bombų ar „užpakalinių durų“ panaudojimas valstybės ypatingos svarbos informacijos infrastruktūroje gali būti neteisingai suprastas kaip pasirengimas mūšiui ir gali sparčiai padidinti įtampą. Kibernetinė veikla, nukreipta prieš kitos valstybės ypatingos svarbos infrastruktūrą, dėl finansų sistemų, elektros tinklų, vamzdynų ir kitos šiuolaikinės ypatingos svarbos infrastruktūros integracijos taip pat gali turėti didelį tarpvalstybinį ar net regioninį poveikį.

Kažkas panašaus jau buvo minėta pasiūlymuose, kuriuos pateikė tiek Rytų, tiek Vakarų atstovai. Vieną iš jų pateikė valstybė, kuri yra glaudžiai susijusi su *Stuxnet*. Savo paskutinėje knygoje „Kibernetinis karas“ Richardas Clarke'as, buvęs keleto JAV prezidentų patarėjas saugumo klausimais, pasitelkė savo didelę patirtį branduolinės ginkluotės kontrolės klausimais, pritaikyda-

mas ją kibernetinei erdvei. Perskaitykite jo pasiūlymą dėl Kibernetinio karo apribojimo sutarties[53]. Pasiūlymas, draudžiantis kibernetinių ginklų naudojimą prieš ypatingos svarbos infrastruktūras, yra įtrauktas ir į Šanchajaus bendradarbiavimo organizacijos pasiūlymus dėl Tarptautinės elgsenos kodekso, 2011 metais buvo nusiųstas į JT[54].

Pažado susilaikyti neužtenka. Būtina prisiimti atsakomybę dėl savo įsipareigojimų vykdymo. Iš to atsiranda antrasis pasiūlymas.

2. Įsipareigojimas dėl valstybinės kibernetinės erdvės teisinės atsakomybės. Valstybės sutinka prisiimti atsakomybę dėl piktavališkos kibernetinės veiklos, vykstančios jų jurisdikcijos kibernetinėje erdvėje arba einančios per ją.

Argumentai. Valstybės privalo susitarti dėl minimalių įsipareigojimų tam, kad apsaugotų savo nacionalinę kibernetinę erdvę. Reikia ypač pabrėžti valstybių įsipareigojimą reaguoti į incidentus, kylančius iš arba einančius per tų valstybių jurisdikcijos kibernetinę erdvę. Pavyzdžiui, valstybės turėtų užtikrinti, kad nacionaliniai interneto paslaugų teikėjai ir teisėsaugos institucijos imtųsi reikiamų priemonių prieš asmenis, grupes taip pat ir informacinę ir ryšių įrangą, kurie, kaip yra nustatyta, dalyvauja kibernetinėje atakoje. Tuo taip pat norima pasakyti, kad valstybės sutinka sukurti pajėgumus, kurie yra reikalingi spręsti kibernetinio saugumo klausimus. Tai reiškia atitinkamų įstatymų ir struktūrų (nacionalinių kompiuterių incidentų reagavimo tarnybų, teisėtvarkos subjektų ir t. t.), kurių reikia, norint vykdyti šį įsipareigojimą, sukūrimą.

Tai irgi nėra nauja idėja. JAV mokslininkai jau kurį laiką diskutuoja apie poreikį valstybėms prisiimti įsipareigojimus už tai, kas vyksta jų kibernetinės jurisdikcijos ribose. Tokios politikos mąstymo pavyzdys gali būti Chriso C. Demchako ir Peterio Dombrowskio straipsnis, kuriame kalbama apie kibernetines sienas ir jurisdikcijos ribas. Jie teigia, kad kibernetinė erdvė nebėra bendra teritorija, kur bet kas gali klajoti ir daryti, ką panorėjęs. Yra tiek daug visko sukurta ir taip rizikuojama valstybės saugumu, kad kibernetinių sienų sukūrimas ir kontrolė yra svarbus žingsnis, užtikrinant ypatingos svarbos infrastruktūrų apsaugą nuo kibernetinių pavojų[55].

---

[53] Clarke R., *Cyber War: The Next Threat to National Security and What to do About it,* Harper Collins, 2010, p. 268271.

[54] Ministry of Foreign Affairs of the People's Republic of China, „China, Russia and Other Countries Submit the Document of International Code of Conduct for Information Security to the United Nations", *Ministry of Foreign Affairs of the People's Republic of China,* http://www.fmprc.gov.cn/eng/wjdt/wshd/t858978.htm, 13 09 2011.

[55] Demchak C., Dombrowski P., „Rise of a Cybered Westphalian Age", *Strategic Studies Quarately* 5 (1), http://www.au.af.mil/au/ssq/2011/spring/spring11.pdf, 2011, p. 5457.

Su teisinėmis atsakomybėmis ir įsipareigojimais yra siejama kaltės priskyrimo problema. Reikia padaryti taip, kad vykdyti kibernetines atakas būtų sudėtingiau, o tikimybė būti pagautam būtų didesnė. Kai valstybė nustatys savo kibernetines sienas ir jas kontroliuos, kibernetinėms atakoms bus daug sunkiau išlikti nepastebėtoms. Tačiau iki šiol buvusios nesėkmingos pastangos, mėginant nustatyti kaltininkus, turi būti perkeltos nuo mėginimo nustatyti, kas faktiškai atakuoja, į tai, „kuri valstybė, jei tokia yra, atsakinga“[56]. Būtent valstybė turi būti atsakinga už tai, kad būtų užtikrinta kontrolė jos kibernetinių sienų ribose ir kad piktavališka kibernetinė veikla, atsiradusi arba einanti per jos kibernetinę jurisdikciją, būtų stebima ir kontroliuojama. Visa atsakomybė už reagavimą ir atakos tyrimą turi būti taikoma ne aukai, bet tiems, kurie yra arčiausiai ir kurie gali reaguoti į incidentą.

3. Stebėjimas, kaip įgyvendinami aukščiau išdėstyti suderinti įsipareigojimai. Valstybės turėtų paremti sudaryti iš savanorių ekspertų ir institucijų, kurie stebėtų ir patartų dviejų aukščiau aptartų punktų vykdymo klausimais, koaliciją.

Argumentai. Turi būti prieinamos tam tikros priemonės, norint stebėti ir informuoti dalyvaujančias valstybes apie piktavališką kibernetinę veiklą, kuri vyksta jų kibernetinės jurisdikcijos ribose arba eina per ją. Reikia sukurti instituciją, kurią sudarytų ekspertai, galintys stebėti ir teikti objektyvų vertinimą apie įsipareigojimų pažeidimus. Tokiu būdu būtų numatyta galimybė daryti švelnųjį spaudimą valstybėms, kurios delsia arba nenori imtis veiksmų dėl nustatytos piktavališkos veiklos, vykstančios jų kibernetinėje jurisdikcijoje.

Tai nėra naujiena bet kam, kas dirba tarptautinių santykių srityje. Tai nėra naivus idealizmas. Tais klausimais, kur suvokiama būtinybė ir kur yra tikrai svarbu, valstybės susivienijo ir pasirašė tarptautinius susitarimus ir konvencijas. Tai ypač pasakytina apie masinio naikinimo ginklų draudimą. Vienas modelis, kaip būtų galima spręsti klausimą, susijusį su valstybių kibernetinių ginklų gamyba ir panaudojimu, yra tarptautinė Cheminio ginklo konvencija. Galbūt, vis dar prisimenant jų panaudojimą Pirmajame pasauliniame kare ir pripažįstant technologijų pažangą, kuri gali palengvinti cheminių ginklų panaudojimą ir padidinti jų galimybę padaryti žalą, ši konvencija įsigaliojo 1997 metais. Ją pasirašė daugiau nei 190 valstybių, atstovaujančių 98 % pasaulio gyventojų. Kartu su šiuo susitarimu buvo sukurta Cheminio ginklo draudimo organizacija (*angl.* Organisation for the Prohibition of Chemical Weapons, OPCW), kurios

[56] Healey J., ed., *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, Cyber Studies Conflict Association, 2013, p. 265.

tikslas yra stebėti ir kontroliuoti, kaip ši konvencija yra įgyvendinama[57]. Cheminio ginklo konvencija gali pasitarnauti, svarstant trijų anksčiau minėtų pasiūlymų įgyvendinimą. Rašant šį straipsnį, OPCW aktyviai prisidėjo, sprendžiant Sirijos krizę. 2013 metais šios organizacijos nuopelnai buvo pripažinti tarptautiniu mastu, kai OPCW buvo skirta Nobelio taikos premija.

Azijos Ramiojo vandenyno tinklų ir informacijos saugumo incidentų tyrimų grupė (angl. *Asia Pacific Computer Emergency Response Team,* APCERT) yra regioninio bendradarbiavimo pavyzdys. APCERT sudaro nacionalinės tinklų ir informacijos saugumo incidentų reagavimo tarnybos ir interneto paslaugų tiekėjai Japonijoje, Kinijoje ir Pietų Korėjoje. APCERT traktuoja „internetą ir jo būklę kaip vientisą bendrai naudojamą infrastruktūrą“[58]. Šiai koalicijai pavyko išspręsti kibernetinius incidentus, kylančius dėl politinių konfliktų tarp jos narių[59].

Tokio efektyvaus visuotinio reagavimo į suvoktą bendrą grėsmę kibernetinėje erdvėje pavyzdys yra CONFICKER darbo grupės veikla 20082009 metais. Vyriausybėms didžia dalimi nepavyko suvokti augančio pavojaus internetui, kurį sukėlė CONFICKER viruso kūrėjas, užkrėsdamas vis daugiau kompiuterių, kuriems bet kuriuo metu buvo galima duoti komandą veikti. Norėdami apsaugoti internetą nuo šio naujo ir potencialiai sunaikinančio viruso, darbo ėmėsi savanorių grupė, į kurią įėjo gabūs privatūs asmenys, interneto paslaugų tiekėjai ir nevyriausybinės organizacijos. Ši pagrindinė asmenų grupė sugebėjo pakankamai išvystyti bendradarbiavimą tarptautiniu mastu, kad galima būtų analizuoti, stebėti ir neutralizuoti interneto „bombą“, kokia buvo CONFICKER[60]. Tai tik keletas pavyzdžių, ką gali nuveikti motyvuota tarptautinė bendruomenė.

Išvados

Kibernetinės erdvės, kuri yra daugiau negu visuomeninis internetas, jau nebegalima paprastai suvokti kaip globalios bendro naudojimo vietos, kurioje galima tvarkyti savo verslo reikalus, lankytis tinklalapiuose arba skaityti elektroninį paštą. Į ją reikia žiūrėti kaip į sritį, kuri yra ypač svarbi valstybės

[57] Organisation for the Prohibition of Chemical Weapons, http://www.opcw.org/chemical-weapons-convention/.

[58] Ito Y., „Making the Internet Clean, Safe and ReliableAsia Pacific Regional Collaboration Activities“, *The Institute of Electrical and Electronics Engineer*s, http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5978796 2011.

[59] Ten pat.

[60] Bowden M., *Worm:The First Digital War*, Atlantic Monthly Press, 2011, p. 221.

ir jos piliečių gerovei. Faktas, kuris taptų skausmingai akivaizdus tuo pačiu momentu, kai vienas iš svarbių procesų arba paslaugų yra nutraukiamas daugiau nei keletui valandų. Šioje erdvėje egzistuoja gyvybiškai svarbūs dalykai, kurie tapo pažeidžiami ir turi būti apsaugoti. Neseniai paskelbta informacija apie kibernetinių nusikaltėlių ir politinių programišių suėmimus, nors ir labai sveikintina ir gerai iliustruoja bendradarbiavimą ir augantį teisėsaugos veiksmingumą, rodo, jog saugi kibernetinė erdvė yra užtikrinama tik iš dalies. Kibernetinių nusikaltimų kaina nerodo tikrojo pavojaus masto. Pasaulio ekonomikos požiūriu ši kaina faktiškai galėtų, kaip spėjama viename iš mokslinių darbų, siekti ne daugiau suapvalintos paklaidos dydžio nuo 14 trilijonų metinės ekonomikos[61]. Neproporcingai daug dėmesio skiriama informacijos ir informacinių sistemų (klaidingai vadinamomis ypatingos svarbos informacinėmis infrastruktūromis) apsaugai nuo kibernetinės atakų. Tikrasis pavojus, į kurį reikia atsižvelgti, saugant kibernetinę erdvę, yra nekontroliuojama piktavališka valstybių veikla kibernetinėje erdvėje. Ypač ta veikla, kuria siekiama paralyžiuoti valdymo sistemas ir elektros tinklų, dujų vamzdynų, transporto sistemų ir kitų paslaugų, kurios yra svarbiausios šiuolaikinei civilizacijai, funkcionavimą. Kai kibernetinės erdvės valdymas yra patikėtas fizikos dėsniams ir, nors prižiūrimas aukštos kvalifikacijos technologų, visos problemos negali būti išspręstos. Kibernetinė erdvė taip pat negali būti naudojama sprendžiant dabar pasaulyje vykstančius konfliktus. Buvusio JAV CŽV samdomojo darbuotojo E. Snowdeno paviešinta informacija apie vyriausybės ilgalaikį visuotinį šnipinėjimą ir ilgalaikes kenksmingas kibernetinės veiklos programas 2013 metų vasarą demonstruoja ne tik žmogaus teisių pažeidimus ir demokratinės valstybės tendenciją elgtis taip, kaip elgiasi autoritarinės valstybės, bet ir informuoja ir įspėja visuomenę apie tai, kokias nekontroliuojamas kibernetines galias turi vyriausybės savo rankose.

Nesenai vykusiame Sirijos konflikte buvo siūloma humaniškai pademonstruoti kibernetinius ginklus[62]. Šis faktas verčia prisiminti kai kuriuos 1945 metų svarstymus dėl pirmosios atominės bombos panaudojimo – įspėjamojo jos demonstravimo. Labai abejotina, ar spaudžiant ENTER klavišą, galima išspręsti sudėtingus konfliktus, tokius kokie dabar vyksta Vidurio Rytuose. Todėl, jei tokie pasiūlymai yra viešai aptariami, reikalai darosi nekontroliuojami.

---

[61] Center for Strategic and International Studies, „The Economic Impact of Cybercrime and Cyber Espionage", McAfee, http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf , 07 2013, p. 3.

[62] Healey J., „Why the U.S. Should Use Cyber Weapons Against Syria", *Defence One*, http://www.defenseone.com/technology/2013/08/why-us-should-use-cyber-weapons-against-syria/69776/, 31 08 2013.

Tarptautinė bendruomenė turi stengtis labiau suprasti kibernetinės erdvės pobūdį ir svarbą. Reikalingi nauji kibernetiniai diplomatai ir politikai , kurie vienodai suvoktų tai, kas yra pavojuje, ir pasidalintų šiuo suvokimu. Yra požymių, kad kibernetinė politika pradedama pripažinti nauja saugumo politikos sritimi[63]. Valstybės kibernetinės erdvės veikla yra geriausiai suprantama kaip tarptautinio saugumo, o ne informacijos saugumo klausimas.

Šios problemos negalima perduoti spręsti teisėtvarkai, kariuomenei ar žvalgybos tarnyboms. Šie organai yra linkę veikti slapta. Bendradarbiavimas tarp daugelio viešųjų ir privačių sektorių yra pagrindinis faktorius, užtikrinantis saugią kibernetinę erdvę, slaptumas apsunkintų tokį bendradarbiavimą. Šį klausimą turėtų skaidriai spręsti civiliai vyriausybių vadovai, nes tik jie gali susidoroti su visais nacionalinio ir tarptautinio saugumo klausimais.

2014 metais bus pažymimas šimtas metų nuo Pirmojo pasaulinio karo pradžios. Istorikai tebekomentuoja ir laužo galvas dėl to, kodėl turėjo įvykti toks baisus karas. Viena iš didžiausių Pirmojo pasaulinio karo staigmenų buvo naujų technologijų panaudojimas, siekiant sukelti mirtiną poveikį. Panaudojus kulkosvaidžius, ipritą, bombardavimą iš oro ir torpedas, buvo prarasta milijonai gyvybių. Siekdami spręsti šiuolaikinius, besikeičiančius iššūkius dėl valstybių kibernetinėje erdvėje, kurie pateikiami šiame straipsnyje, mes, tikriausiai, galėtume pasimokyti iš minėto karo. JAV istorikė Barbara W. Tuchman savo knygoje *Rugpjūčio ginklai* apie Pirmojo pasaulinio karo pradžią taikliai pastebėjo: „Viena, kas yra būdinga 1914 metams – kaip ir bet kuriam laikotarpiui – kiekvieno, nesvarbu, kurioje pusėje esančio, nusiteikimas nesiruošti sudėtingesnei alternatyvai ir neveikti taip, kaip jie mano esant teisinga.“ Galbūt, valstybės, kurios dalyvavo tame kare, atsižvelgs į tai ir elgsis taip, kad užtikrintų, jog kibernetinių ginklų technologija nebūtų panašių tragedijų XXI amžiuje priežastimi?

2013 m. spalis

[63] Choucri N., *Cyberpolitics in International Relations*, The MIT Press, 2012, p. 238.