Kriminalističke teme
Zbornik radova
Godina XIX, Broj 5, 2019.
ISSN 1512-5505

SVEOBUHVATNI PRISTUP NATO-A SAJBER ODBRANI
NATO'S COMPREHENSIVE APPROACH TO CYBER DEFENSE

Pregledni naučni rad

Sergej Cvetkovski[476]
Vancho Kenkov[477]

Sažetak

Inspiracija za rad i problem (i) koji se radom oslovljava (ju): U eri dominacije informacione tehnologije, sajber prostor je postao značajan sigurnosni problem za vlade koje su prisiljene poduzeti dodatne mjere za poboljšanje sajber sigurnosti.
Ciljevi rada (naučni i/ili društveni): U situaciji povećane upotrebe informacionih tehnologija u današnjem globaliziranom svijetu, cyber odbrana postaje veliki prioritet ne samo za pojedine zemlje, već i za njihove kolektivne mehanizme.
Metodologija/Dizajn: Ovaj rad bavi se problemima NATO kibernetičke odbrane i sajber bezbjednosti i mogućim poraznim efektima i posljedicama cyber napada. U tom cilju autori će koristiti dostupnu stručnu literaturu i online publikacije na ovu temu, na kojima će se primijeniti kvalitativna analiza sadržaja. Teret istraživanja bit će na strateškim i operativnim mjerama sigurnosti i obrane Saveza, jer postoji ograničena dostupnost informacija o mjerama taktičkog nivoa koje su povjerljive.
Ograničenja istraživanja/rada: Autori rada nastoje da razrade koordinirani i sveobuhvatni pristup NATO-a u postizanju efektivne sajber odbrane i sigurnosti komunikacionih i informacionih sistema za članice Saveza i njihove partnere.
Rezultati/Nalazi: Pitanja koja se pojavljuju su: koliko NATO savez ozbiljno razmatra rizike cyber napada, na koji način to odražava promjene u politici odbrane i strateškim konceptima Alijanse, koji je pristup rješavanju ovog novog sigurnosnog izazova i koje su obaveze na nivou Saveza?!
Generalni zaključak: Odgovor je da se fokus NATO-a u narednoj deceniji mora odnositi na razvoj sajber-moći.
Opravdanost istraživanja/rada: Tehnologija je u srcu naših čvrsto povezanih društava. Oslanjanje modernih društava na informacionih tehnologija podrazumijeva očigledne bezbjednosne probleme. Cyber prijetnje i napadi postaju sve češći, sofisticiraniji i štetniji. Čak i vojske i službe bezbjednosti koje se u velikoj mjeri oslanjaju na sajber prostor za obavljanje svojih misija nisu imune na takve napade.

[476] Associated Professor. Institute for Security, Defense and Peace - Faculty of Philosophy, Skopje, sergej@fzf.ukim.edu.mk
[477] PhD Professor. Institute for Security, Defense and Peace - Faculty of Philosophy, Skopje, vancok@fzf.ukim.edu.mk

Ključne riječi
sajber prostor, sajber napadi, sajber odbrana, NATO, sveobuhvatnost

Abstract
Reason for writing and research problem (s): In the era of domination of information technology, cyber space has become a significant security issue for governments that are forced to take additional measures to enhance cyber security.
Aims of the paper (scientific and/or social): In a situation of increased use of information technology in today's globalized world, cyber defense is becoming a high priority not only for individual countries, but also for their collective mechanisms.
Methodology/Design: This paper addresses the problems of NATO cyber defense and cyber security and the possible defeating effects and consequences of cyber attacks. To this end, the authors will use the available expert literature and online publications on this subject, on which a qualitative analysis of the content will be applied.
Research/Paper limitation: The authors of the paper make an attempt to elaborate NATO's co-ordinated and comprehensive approach in achieving effective cyber defense and security of communication and information systems for Alliance members and their Partners.
Results/Findings: The burden of the research will be on the strategic and operational security and defense measures of the Alliance because there is limited availability of information on tactical level measures that are kept confidential. The issues that arise are: how much does the NATO Alliance seriously consider the risks of cyber attacks, in which way it reflects the changes in the defense policy and strategic concepts of the Alliance, what is the approach to tackling this new security challenge and what are the commitments at the level the alliance to further improve security in cyber space?!
General Conclusion: The answer is that NATO's focus in the next decade must be on the development of cyber power.
Research/Paper Validity: Technology is at the heart of our tightly knit societies. Modern societies' reliance on information technology implies obvious security problems. Cyber threats and attacks are becoming more common, sophisticated and harmful. Even the military and security services that rely heavily on cyberspace to carry out their missions are not immune to such attacks.

Keywords
cyber space, cyber attacks, cyber defense, NATO, comprehensiveness

Uvod

Tehnologija je u srcu naših čvrsto povezanih društava. Oslanjanje modernih društava na informacionih tehnologija podrazumijeva očigledne bezbjednosne probleme. Cyber prijetnje i napadi postaju sve češći, sofisticiraniji i štetniji. Čak i vojske i službe bezbjednosti koje se u velikoj mjeri oslanjaju na sajber prostor za obavljanje svojih misija nisu imune na takve napade. Vlade širom svijeta počele su da razvijaju procedure i aktivnosti za zaštitu sajber prostora od sajber napada, a ta sposobnost je postala od suštinskog značaja za ostvarivanje sajber odbrane. Mnoge vlade priznaju da se sajber bezbjednost može postići samo kroz međunarodnu saradnju i partnerstvo. Ali posljedice od sajber napada ne utiču samo na pojedinačne vlade, već i na velike međunarodne

organizacije i saveza kao što je NATO savez, pri čemu su napadnuti komunikacijski i informacioni sistemi ovog saveza, tako da i NATO savez primjenjuje koordinirani pristup zaštite ključne informacione i komunikacijske infrastrukture.

Nakon događaja u Estoniji u maju i aprilu 2007. godine, kada je napadnuta informacijska infrastruktura zemlje, NATO je počeo kontinuirano razvijati i poboljšavati zaštitu svojih komunikacijskih i informacionih sistema od napada i neovlaštenog pristupa. Alijansa je također usmjerila svoje aktivnosti na podršku individualnih napora za zaštitu informacione infrastrukture svake države članice. U samom NATO-u u Lisabonu 2010. godine, sajber odbrana je predstavljena kao jedan od najvažnijih izazova Saveza u budućnosti. Posebno je naglašen značaj zaštite informacione i komunikacione infrastrukture NATO-a.

Danas se NATO i njegovi saveznici oslanjaju na jaku i elastičnu kibernetičku odbranu kako bi ispunili ključne zadatke Alijanse za kolektivnu odbranu, upravljanje krizama i sigurnosnu saradnju. NATO savez bi trebao nastaviti da bude spreman da brani svoje mreže i operacije protiv sve veće sofisticiranosti sajber prijetnji i napada s kojima se suočava. Glavni fokus u sajber odbrani NATO-a, pored zaštite mreža koje uključuju operacije i misije, jeste jačanje sajber otpornosti među svim državama članicama saveza.

1. Kiberprostor - novi predmet zaštite

1.1 Novi prostor rata

Prema međunarodnom pravu, postoji opšta saglasnost između država da sajber prostor podleže principima suvereniteta i nadležnosti, jednako kao i zabrana mješanja u poslove drugih država i upotrebe sile. U sajber prostoru države imaju pravo da koriste "kontra-mjere" kako bi uspostavile pravnu situaciju ili de-eskalirale nezakonitu situaciju. Tipično, takve mjere su obično fizičke operacije blokiranja i operacije odbijanja u području, na primjer, kako bi se spriječilo slijetanje ili prelet zrakoplova. U kibernetičkom prostoru, država može legalno preuzeti čin negiranja/odbijanja kao protumjere protiv zlonamjerne sajber aktivnosti sve dok ne dobije naknadu za nanesenu štetu.

Države se ohrabruju da istraže kako primijeniti međunarodno pravo u cyber domenu, u smislu da li su postojeći zakoni dovoljni. Postavlja se pitanje da li su svi cyber napadi kršenje međunarodnog prava?! Možemo nagađati da velike sajber sile ne žele da razgovaraju o crvenim linijama ofanzivnih sajber aktivnosti, što rezultira pozivima na različite napore usmjerene na jačanje političkih apetita za akciju.

U tom pravcu, i Crveni krst je prilično zabrinut zbog humanitarnih troškova sajber napada, ističući da organizacija koristi sajber prostor za komunikacije i logistiku i podložna je brojnim sajber napadima. Države se moraju tačno složiti o tome šta je okarakterizirano kao napad i da li su napaduti podaci zaštićeni međunarodnim humanitarnim pravom

(MHP). U tom smislu, Medjunarodni komitet crvenog krsta MKCK (ICRC) se zalaže za široko tumačenje pojma "napad" unutar MHP, koji također uzima u obzir slučajeve kao što su špijunaža i smetnje. Brisanje ili promjena podataka također može prouzrokovati više štete za civile nego fizičko uništenje nekih objekata, i stoga Međunarodni komitet crvenog krsta (MKCK) smatra podatke kao objekat zaštićen od MHP.

Sajber prostor je prioritetna tema za raspravu u UN-u. Međunarodno pravo također treba da se primjenjuje na sajber prostor, tako da će nauka, aktivnosti i pojedinci imati koristi, što će rezultirati odgovornim ponašanjem država u sajber prostoru kako bi se garantovala sloboda izražavanja i ideja, kao i bezbjedno okruženje za korisnike. Veći fokus je na miroljubivoj upotrebi sajber-prostora uz predanost da će se razviti novi ili primijenjeni postojeći mehanizmi za povećanje povjerenja među državama članicama UN-a o cyber mogućnostima i namjerama. Primjer je pokušaj Organizacije američkih država da implementira norme protiv proliferacije u kibernetskom prostoru, uključujući određivanje lokalnih kontakt tačaka za cyber sigurnost u svakoj državi članici i kroz razvoj nacionalnih planova za kibernetičku sigurnost (Jabbari 2018).

Sajber prostor je oblast informacionog okruženja koja se sastoji od nezavisne mreže informacione infrastrukture, uključujući Internet, telekomunikacione mreže, računarske sisteme i ugrađene procesore i kontrolore (Kissel, 2011). Sajber prostor nema zajedničku definiciju i ovaj termin se koristi za opisivanje ne-fizičkog prostora koji se sastoji od više komunikacijskih i informacionih sistema koji su povezani sa globalnom mrežom. Termin se koristi za opisivanje virtuelnog svijeta informacionih sistema gdje se predmet u sajber prostoru odnosi na pakete informacija koji protiču kroz kompjuterski sistem ili mrežu. Sa pojavom Interneta, sajber prostor sada obuhvata globalnu mrežu kompjutera.

Sajber prostor, koji se smatra petim prostorom ratovanja (nakon kopna, mora, vazduha i svemira) sastoji se od svih kompjuterskih mreža u svetu i svega što one povezuju i kontrolišu preko kablove, vlakna i bežične veze. Što se tiče mreže, sajber prostor nije samo Internet, već i mnoge druge mreže koje ne bi trebalo da budu dostupne preko interneta (Schreier, Weekes i Winkler 2011, str. 8). Sajber prostor je medij koji se sastoji od velikog broja učesnika sa sposobnošću interakcije i je domen koji karakteriše upotrebu elektronskog i elektromagnetnog spektra za skladištenje, modifikovanje i brisanje podataka putem mrežnih sistema i povezane fizičke infrastrukture (Baykal, 2013, str. 7). U eri informacionih tehnologija i povezivanja ljudi kroz komunikacione i informacione sisteme, sajber prostor postaje jedna od kritičnih oblasti nacionalne bezbjednosti, jer je ranjivost država na sajber kriminal značajan bezbjednosni rizik.

Sve veći naglasak se stavlja na razmatranja da se čini da rat prelazi u sajber prostor. Realizacija potencijalnog rata u sajber-prostoru dovešće do formiranja novih organizacija, koncepata i elemenata sukoba koji su paralelni, ali još uvijek različiti od konvencionalnih načina ratovanja (Moran, 2009, str. 138-139).

Uz sve veću ovisnost o informacijskoj tehnologiji, sve vitalne infrastrukture u državi su osjetljive na neku vrstu vanjskog napada. Aktivnosti koje se koriste za prijetnju vladama i međunarodnim organizacijama smatraju se sajber terorizmom i kao takve oslabljuju vladine ili vojne komunikacijske i informacione sisteme. Pojedinci, nacionalne grupe i cijele vlade koriste sajber prostor za ostvarivanje interesa kroz zlonamjerne aktivnosti. Terorističke grupe se regrutuju, obučavaju i djeluju kroz interneta. Kroz Internet organizuju se i kriminalne organizacije, kradu se i koriste se finansijski podaci sa profitom koji prelazi onaj trgovine drogom. Obavještajne službe također kradu poslovne i državne tajne putem interneta (Reveron, 2012, str. 3).

Čak i ako se stručnjaci ne slažu oko obima i prirode prijetnje, države još uvijek moraju usvojiti određene mjere za jačanje zaštite informacionih sistema. Ona bi trebala uključivati blisku saradnju među državama, izraženu kroz zajedničke vježbe kroz koje će se provoditi simulacija i modeliranje sposobnosti za razumijevanja utjecaja mogućeg napada na međusobno povezane i međusobno ovisne informacijske infrastrukture. To će doprinijeti razvoju novih mogućnosti za otkrivanje i identifikaciju mogućih negativnih implikacija na informacionu infrastrukturu. Poduzete mjere kategorizirane su kao kibernetička sigurnost, sajber obrana i informacijska sigurnost.

1.2 Sajber bezbjednost i sajber odbrana

Sigurnost sajber prostora danas predstavlja značajan izazov za nacionalnu sigurnost. Sajber bezbednost se odnosi na tehnologije, procese i prakse koji su dizajnirani da zaštite mreže, računare, programe i podatke od napada, od oštećenja ili od neovlašćenog pristupa. U kontekstu sajber bezbjednosti, vlada treba da implementira određene mjere kao što su dizajniranje sigurnih i otpornih mreža, sigurni komunikacijski i informacijski sistemi, te korištenje sigurnosnih politika, standarda i održivih sigurnosnih mehanizama. Sajber prostor postaje prilično dinamično okruženje koje prelazi državne granice i uvijek stvara nove dimenzije nesigurnosti kao rezultat pojave višestrukih centara moći u sajber prostoru, vladinog ili nevladinog. U ovim okolnostima, gore pomenuti akteri će oblikovati događaje u sajber prostoru koji će biti višestruko ciljani i uticati na komunikacijske i informacione sisteme sa katastrofalnim posljedicama.

Sajber bezbjednost ili sposobnost da se zaštiti i odbrani upotreba sajber prostora od sajber napada je osnova sajber odbrane. Obezbjeđivanje društva od sajber bezbjednosti postalo je jedan od najvećih prioriteta, i u tu svrhu vlade moraju energično braniti mreže i sisteme prijetnji unutrašnjim i spoljašnjim prijetnjama. Prema Bajkalu (Baykal, 2013, str. 13-14) u opsegu sajber obrane su štetne radnje ili prijetnje (moguće ili stvarne). Sajber odbrana se fokusira na štetne radnje koje su izvorno izvedene iz sajber prostora. Svrha sajber odbrane je da obezbijedi trajnost usluga sajber prostora za korisnike.

Sajber odbrana predstavlja sposobnost da zaštiti i zaštiti sajber prostor od mogućih sajber napada. Sajber napad je napad na sajber prostor u cilju ometanja, onemogućavanja, uništavanja i kontrole računarske infrastrukture ili uništavanja integriteta podataka i informacija ili njihove krađe.

Cyber odbrana danas predstavlja veliki izazov za vlade i može se postići samo kroz međunarodnu saradnju i partnerstvo. Vlade moraju podsticati koherentan odgovor na osiguranje sajber prostora, a na nacionalnom nivou to je zajednička odgovornost svih ministarstava i vladinih agencija, privatnog sektora i građana. Na regionalnom i međunarodnom nivou, ovo uključuje saradnju i koordinaciju sa svim relevantnim partnerima. Također zahtijeva izbor najbolje kvalifikovanog osoblja koje će voditi ove napore (Schreier, Weekes & Winkler, 2011, str. 14). Korišćenje, upravljanje i odbrana kritične informacione strukture je mnogo lakše kada se odgovornost dijeli i kada postoji međunarodna saradnja i partnerstvo.

1.3 Informacijska sigurnost

Sigurnost informacija ili kako i da nazovemo ovo područje koje se bavi sve većim poremećajima u povjerljivosti, dostupnosti i integritetu informacija, je glavni imperativ informacione sigurnosti (Information Security), osiguranja informacija (Information Assurance) i kibernetičke odbrane (Cyber Defense). Svi navedeni termini imaju više sličnosti nego razlike u načinu na koji se percipiraju sigurnost informacija i sigurnost informacijskih sustava. Sve se one međusobno preklapaju i dijele zajednički izazov, sigurnost informacija.

Međutim, postoje i pokušaji da se predstave kao odvojene discipline. Naime, informacijska sigurnost je predstavljena kao podskup informacijske bezbjednosti. Ali, i informaciona bezbjednost je predstavljena kao podskup sajber odbrane, tj. Sajber bezbjednosti i obrnuto. Mogućnost konfuzije proizlazi iz sličnosti i činjenice da je sajber bezbjednost relativno nova disciplina (Withman & Mattord, 2011). Stoga, ona želi da prihvati mišljenje da sajber odbrana pokriva samo sajber prostor, ili da je sajber odbrana u stvari bezbjednost informacija plus bezbjednost mreža. Međutim, povećana opasnost od napada informacijske sigurnosti prisilila je vlade da uzmu u obzir i rizike takvih napada na njihove komunikacijsko-informacijske sustave i druge kritične infrastrukture. Pažnja je također posvećena uključivanju država u informacijski rat i mogućnost kolapsa komunikacione infrastrukture ako se ona ne brani (Pindar i Rigelsford, 2011).

U tom pravcu, pored nacionalnog izazova za zaštitu informacija, zaštita NATO informacionog sistema je sastavni dio funkcionisanja Alijanse.

2. NATO-ov pristup sajber odbrani

Suština debata i aktivnosti sajber odbrane je u trci između napadača i branilaca, oko toga koji će prvi otkriti sljedeću slabost protivnika. Efekti sajber napada mogu biti prilično neočekivani i štetni. NATO je vojno-politički savez sa 70 godina zajedničkog cilja za sprečavanje sukoba i očuvanje mira i stabilnosti za oko 1 milijardu ljudi u evroatlantskom području. NATO, kao Savez od 29 zemalja članica Sjeverne Amerike i Evrope, nastoji to ostvariti obećavajući da će se članice braniti međusobno suglasno frazi: svi za jednoga, jedan za sve - obaveza poznata kao kolektivna odbrana.478 Oni prepoznaju rizik od sajber napada. Isti princip kolektivne odbrane odnosi se na pristup NATO-a sajber prostoru. NATO-ovo razmišljanje o sajber odbrani napreduje posljednjih godina. Sajber odbrana se više ne smatra čisto tehničkim pitanjem, već je dobila politički i strateški značaj. Široko rasprostranjeni sajber napadi koji su poremetili vladine i bankarske sisteme u Estoniji 2007. godine jasno su ukazali na evoluciju percepcije potencijalnih ranjivosti u našim srodnim i digitaliziranim društvima. Od napada u Estoniji, sajber odbrana je postala suštinski prioritet Alijanse.

2.1 Politika u oblasti sajber odbrane i hronologija obaveza

U aprilu 2008. godine, NATO je odobrio Politiku kibernetičke odbrane kao zajednički koordinirani pristup čiji je cilj zaštita ključnih informacijskih i komunikacijskih sistema i jedini odgovor na sajber napade. Prateći prioritete, osnovan je Organ za upravljanje sajber odbrane CDMA (Cyber Defence Management Authority), sa ovlašćenjem da upravlja krizom u sajber odbrani i da reaguje u slučaju sajber napada na svoje članove. CDMA je imala zadatak da sprovede sajber odbranu NATO informacione i komunikacione infrastrukture. Politika sajber odbrane naglašava potrebu da se zaštiti ključni informacioni sistem Saveza i da se pruži mogućnost da se zemljama članicama, na njihov zahtev, pomogne da zaustave sajber napad. Infrastruktura unutar NATO-a je neizbježno povezana. Ona prelazi nacionalne granice i ono što se dešava u jednom dijelu mreže može vrlo brzo utjecati na drugu, uzrokujući potencijalno katastrofalne rezultate (Hartmann, 2009, str. 186-187).

Na samitu NATO-a u Lisabonu, sajber bezbjednost je prikazana kao novi bezbjednosni izazov sa kojim se NATO mora suočiti u narednim godinama, a NATO je identifikovao sajber odbranu kao važan prioritet. U takvim okolnostima, Alijansa mora pomoći državama članicama da razviju sposobnosti koje se mogu brzo koristiti u skladu sa misijama Alijanse. Za "manje" članice Alijanse biće lakše razviti zajedničke odgovore na kibernetičke prijetnje, umjesto da djeluju samostalno u tom smjeru. NATO kao organizacija može pomoći i dati savjete o tome kako zaštititi kritičnu informacijsku infrastrukturu. Također, izgradnja bliskih veza sa privatnim sektorom, koji ima veliku ekspertizu, od posebne je važnosti. Neophodno je pronaći bolje načine kroz javno-

[478] Član 5. Severnoatlantskog ugovora.

privatna partnerstva kako bi se istražio vojni potencijal novih tehnologija, ali sa pažljivim aktivnim uključenjem javnog sektora u ove studije.

Strateški koncept NATO-a iz 2010. godine izražava potrebu da se zaštite informacioni i komunikacioni sistemi NATO-a kao rezultat brzog razvoja i sve veće sofisticiranosti sajber napada. Strateški koncept izražava zabrinutost da sajber napadi postaju sve učestaliji, organizovaniji i izazivaju veliku štetu javnim upravama, preduzećima, ekonomijama i potencijalnim transportnim i snabdjevenim mrežama, kao i drugim kritičnim infrastrukturama. Potencijalna šteta od ovih napada može da dostigne prag koji ugrožava nacionalni i evroatlantski prosperitet, bezbjednost i stabilnost (NATO, 2010).

U 2011. godini usvojena je revidirana politika NATO-a za sajber odbranu, sa jasnom vizijom napora u oblasti kibernetičke odbrane, kao i Akcionog plana za njenu implementaciju. Svrha ove revidirane politike je bila da se ponudi koordinirani pristup sajber odbrani u Savezu, sa fokusom na sprečavanje sajber napada i da se sve strukture NATO-a podvrgnu centralizovanoj zaštiti. Politika je također naglasila saradnju sa partnerskim zemljama, međunarodnih organizacija, privatnim sektorom i akademskom zajednicom. NATO-ova politika sajber odbrane i prateći Akcioni plan jasno su pokazali da je fokus NATO-a na zaštiti svojih komunikacionih i informacionih sistema. Osnovni principi politike zasnivaju se na prevenciji, izdržljivosti i ne-dupliciranju. Ključ efektivne sajber odbrane je koordinirana odbrana između članica Saveza i mreža NATO-a. Pored toga, postoji obaveza da će NATO pružiti koordiniranu pomoć ako su saveznik ili saveznici žrtve sajber napada i traže pomoć (Hunker, 2013).

Pokušaj da se poboljša sajber odbrana NATO potvrđen je na samitu u Čikagu u maju 2012. godine. Postavljanje svih mreža NATO-a pod centralizovanu zaštitu predstavljeno je kao osnovni zadatak. Daljnja reforma, kao dio tekućeg procesa reforme Alijanse, bila je uspostava NATO-ove Agencije za komunikacije i informacije (Agencija NCI) u julu 2012. godine, kako bi se cjelokupna struktura NATO-a dovela pod centraliziranu zaštitu. Glavni cilj NCI-ja je pružanje C4ISR tehnologije (za komandu, kontrolu, komunikacije, računare, obavještavajne, nadzor i izviđanje) i usluge i sposobnosti za komunikacija i informacijske sustave (CIS) za misije Alijanse, uključujući nove prijetnje i izazove kao što su sajber odbrana i raketna odbrana. Agencija također pruža kooperativnu razmjenu informacija između Alijanse, promovirajući potrebu za interoperabilnošću. Agencija je izvršno tijelo NATO-ove Organizacije za komunikacije i informacije (NCIO), koja ima za cilj pružanje sigurnih CIS usluga. NATO je prepoznao potrebu za pružanjem sveobuhvatnih usluga kibernetičke odbrane NATO-u, jer je cijela NATO struktura povezana sa istom mrežom i sve članice suočavaju se sa istim sajber prijetnjama. Prihvatanjem svih mreža NATO-a pod centraliziranom zaštitom, virtualne granice se mogu lakše definirati i izbjeći dupliranje napora i financijskih troškova.

Ofanzivne sposobnosti za sajber napade koje su razvili državni ili nedržavni akteri mogu lako uticati na NATO-ove usluge CIS-a. Da bi postigao efikasnu kibernetičku odbranu i pružio usluge CIS-a, NATO se mora fokusirati na novu dimenziju sajber prostora, sajber-

moć. Prema Hunkeru, (Hunker, 2013) u izgradnji bezbjednosnog prisustva u sajber prostoru, NATO se mora fokusirati ne samo na sprečavanje sajber napada, već i na to kako bi nacije i nedržavni akteri mogli koristiti svoje prisustvo u sajber prostoru da utiču na događaje, sa drugom riječju da izvrši moć. On kaže da se sve rasprave o sajberu u kontekstu Saveza odnose na odbranu, a još manje na rat. Jedan fokus na razvojne doktrine NATO-a treba staviti na posljedice sajber- moći, a ne samo na borbu protiv sajber rata ili odbranu sajber-napada. On predlaže da sajber-moć može poslužiti kao okvir za događaje koji će oblikovati okruženje NATO-a 2030. godine.

Potvrda ozbiljnog pristupa NATO-a sajber odbrani dolazi godinu dana kasnije, 2014, kada su saveznici NATO-a istakli da uticaj sajber napada "može biti štetan za moderna društva, baš kao i konvencionalni napad" (NATO, 2014).

Na samitu NATO-a u Varšavi 2016. godine, lideri saveznika NATO-a obećali su da će ojačati svoju nacionalnu kibernetičku odbranu kao dio Posvećenosti sajber odbrani. Od tada, oni su izveštavali o razvoju nacionalnih sajber strategija, kako su organizovani za sajber odbranu, kakve investicije vrše - i u pogledu finansija i u ljudske resurse, kao i o programa obuke i obrazovanja vezanih za sajber. Na ovom samitu, saveznici su prepoznali sajber prostor kao novi operativni domen u kojem se NATO mora efikasno braniti isto kao što to radi u zraku, na kopnu i na moru. Takvo priznavanje olakšava integraciju dobrovoljnog suverenog nacionalnog sajber doprinosa u misije i operacije NATO-a.

Da bi se efikasno omogućile integracije sajber-sposobnosti u komandnu strukturu NATO-a, na samitu u Briselu 2018. godine, saveznici su se dogovorili da osnuju Cyber Space Center, koji se nalazi u Monsu, u Belgiji. Centar bi trebao biti odgovoran za pružanje svijesti o situaciji, koordinaciju sajber napora i centralizirano planiranje za operacije i misije i predviđa se da će u potpunosti biti operativan do 2023. godine (Brent, 2019).

2.2 Ostvarivanje NATO-ovih prioriteta u sajber odbrani

NATO-ov mandat za sajber odbranu je dvostruk: da zaštiti svoje mreže i ojača sajber-otpor u Savezu od 29 zemalja. Pored stručnjaka za kibernetičku odbranu, NATO ima i timove za brzo reagovanje (RRT) koji se mogu rasporediti kako bi odgovorili na potencijalne sajber napade na mreže NATO-a ili na pomoć NATO saveznicima na njihov zahtjev. Razmjena informacija je neophodna za bolju informiranost i bolju spremnost za rješavanje kibernetičkih prijetnji. U tom cilju, NATO ima na raspolaganju nekoliko instrumenata, kao što je Platforma za razmjenu informacija o zlonamjernom softveru, koja omogućava razmjenu informacija u realnom vremenu. Da bi se osiguralo da su vještine u skladu sa tehnologijom, NATO ima programe obrazovanja, obuke i vježbe koji se i dalje razvijaju.

NATO također prilagođava način na koji funkcioniše, tako da može biti efikasan u sajber domenu kao što je to i u fizičkom svetu. U 2016. godini, saveznici su prepoznali

kibernetski prostor kao domen operacija - baš kao i zrak, kopno i more. To će omogućiti vojnim strukturama NATO-a da bolje zaštite misije i operacije od sajber-prijetnji. Ta orijentacija obezbjeđuje okvir za upravljanje resursima, vještinama i sposobnostima, istovremeno osiguravajući da se sajber odbrana u potpunosti odražava u vježbama, aktivnostima obuke i mjerama odgovora na krizu. Važno je napomenuti da priznavanje sajber prostora kao domena operacija ne mijenja misiju ili mandat NATO-a koji ostaju defanzivni. Na sastanku ministara odbrane NATO-a u novembru, saveznici su se složili oko okvira političkih i pravnih principa čiji je cilj usmjerivanje integracije dobrovoljnih sajber doprinosa država članica. Okvir osigurava da bilo koji savezni angažman u sajber prostoru poštuje NATO-ov odbranbeni mandat, politički nadzor i poštivanje međunarodnog prava. Ovo je također u skladu sa savezničkom podrškom razvoju normi i mjera za izgradnju povjerenja za sigurnost i stabilnost u kibernetičkom prostoru (Ducaru, 2018). Ovo odražava pristup "promjene u igri" u smislu integracije sajbera kroz strategiju i taktiku, obuku i vježbe, kao i u vojno planiranje u svim operativnim domenima.

Unutar NATO-a, veliki naglasak je na razvoju "digitalnog IQ" savezničke vojske.

- U Portugalu je uspostavljena NATO akademija za sajber i komunikacione informacione sisteme, a sajber-otpornost je sada uključena u nastavnim planova za koordinirano obučavanje u svakoj državi članici NATO-a.
- NATO-ov Centar za savršenstvo kibernetičke odbrane u Tallinnu, Estonija, je akreditovana institucija za istraživanje i obuku koja se bavi edukacijom o sajber odbrani, konsultacijama, naučenim lekcijama, istraživanju i razvoju. Iako nije dio NATO-ove komandne strukture, Centar nudi priznatu stručnost i iskustvo u sajber odbrani. Centar za savršenstvo u Estoniji organizuje dvije sajber vježbe godišnje. Prva, „Sajber koalicija“, testira procedure i politike za spremnost i odgovor Alijanse u situacijama rasprostranjenih, stalnih sajber napada. Druga vježba, pod bannerom „Zaključani štit“, testira vještine cyber-stručnjaka u scenarijima ratnih igara crvenih/plavih timova.
- Škola NATO-a u Oberammergauu u Njemačkoj također provodi edukaciju i obuku za sajber-odbranu kao podršku operacijama, strategiji, politici, doktrini i procedurama Saveza.
- Koledž odbrane NATO-a u Rimu, Italija, podstiče strateško razmišljanje o političko-vojnim pitanjima, uključujući pitanja vezana za sajber odbranu.

Godine 2018. ministri odbrane saveznika dogovorili su se da uspostave Centar za kibernetičku operaciju kao dio nove NATO-ove komandne strukture NATO-a, prvog sajber-orijentiranog entiteta u komandnoj strukturi NATO-a. Ovo je prvi korak ka integraciji sajber-sposobnosti u planiranje i operacije NATO-a. U fizičkom području kopna, zraka i mora, operativno planiranje se odnosi na prikupljene/isporučene fizičke snage ili sposobnosti. U sajber-domenu, integracija će se fokusirati na efekte generisane dobrovoljnim nacionalnim sajber-doprinosima, a ne na same sposobnosti, budući da je većina sajber instrumenata jedinstvena i diskretna (Ducaru, 2018).

U kontekstu sajber bezbjednosti, svaki od 29 saveznika NATO-a mora poboljšati sajber odbranu na svojim nacionalnim mrežama i infrastrukturama. Savez je jak koliko i njegova najslabija karika, tako da je podizanje nivoa sajber pripremljenosti i zaštite na nacionalnom nivou važan zadatak. Saveznici izvještavaju da je Zalog za sajber odbrane važan alat za podizanje svijesti kod višeg rukovodstva o važnosti sajber odbrane, što zauzvrat može pomoći u određivanju prioriteta ulaganja u ovoj oblasti. Ona također pomaže da se olakša koordinacija među različitim nacionalnih uključenih strana - od aktera za sigurnost i odbranu, preko onih koji primjenjuju zakon, pa sve do operatere kritične infrastrukturne. Dakle, privatni sektor je ključni igrač u kiberprostoru. Tehnološke inovacije i stručnost iz privatnog sektora su od ključnog značaja kako bi se omogućilo NATO i saveznim zemljama da podignu efikasnu sajber odbranu. Kroz NATO-ovo sajber partnerstvo sa industrijom (NICP), NATO i njegovi saveznici rade na jačanju njihovih odnosa sa industrijom. Ovo partnerstvo se oslanja na postojeće strukture i uključuje entitete NATO-a, nacionalne kompjuterske timove za reagovanje u vanrednim situacijama (CERTs) i predstavnike industrije iz članica NATO-a. Aktivnosti za razmjenu informacija i vježbi, obrazovanja i obuke samo su neki od primjera područja u kojima NATO i industrija rade zajedno. Kibernetička sigurnost podrazumijeva stvarni pristup čitavog društva, od korisnika tehnologije, programera i operatera pa sve do vladinog rukovodstva na kojeg se oslanjamo da bi se sprovodile politike koje nam pomažu da koristimo pogodnosti i ograničavamo rizike u sajber prostoru.

Pošto se sajber prijetnje ne zaustavljaju na državnim granicama niti na granicama organizacija, NATO mora sarađivati sa relevantnim zemljama, organizacijama i privatnim sektorom kako bi poboljšao međunarodnu sigurnost. Između ostalog, NATO sarađuje sa Evropskom unijom (EU), Ujedinjenim nacijama (UN), Savetom Evrope i Organizacijom za bezbjednost i saradnju u Evropi (OEBS). U februaru 2016. godine, NATO i EU potpisali su o Tehnički sporazum o sajber odbrani kako bi pomogli objema organizacijama da bolje spriječe i odgovore na sajber napade. Ovaj tehnički aranžman pruža okvir za razmjenu informacija i razmjenu najboljih praksi među timovima za odgovor u vanrednih situacija (NATO, 2016).

3. Zaključak

Sajber prostor kao novo sigurnosno pitanje može se smatrati petim prostorom ratovanja. U ovom međuzavisnom svetu postoji stalna opasnost od sajber napada na komunikacione i informacione sisteme i infrastrukturu. Poslednjih godina, sajber napadi su bili dio hibridnog rata. Bezbjednost i odbrana ključnih informacionih sistema i infrastrukture postali su prioritet za vlade koje vide efikasnost u njegovoj realizaciji u razvoju zajedničkog odgovora na sajber napade u međunarodnim bezbjednosnim organizacijama.

Alijansa se suočava sa složenom kompleksnom prijetnjom. NATO-ovi informacioni sistemi svakodnevno bilježe brojne sumnjive incidente. Kod većine njih suočavanje se obavlja automatski, ali postoje i one koje zahtijevaju dodatnu analizu i odgovor od stručnjaka. NATO kao međunarodna bezbjednosna organizacija naglašava sajber odbranu kao ključnu sposobnost Alijanse i njenih članica. Zaloga za poboljšanju NATO sajber odbranu je proces koji je u toku, a cilj sajber odbrane Alijanse je da garantuje održive i sigurne komunikacije i informacione sisteme (CIS). NATO saveznici zagovaraju stajalište da se međunarodno pravo, uključujući međunarodno humanitarno pravo i Povelja UN, primjenjuju na sajber prostor. NATO kontinuirano jača svoje sposobnosti za sajber obrazovanje, obuku i vježbe.

Bibliografija

- Baykal N. (ed.) (2013). Lectures Notes: Hands-on Cyber Defence Training Course for System/Network Administrators of The Republic of Macedonia. Ankara: Informatics Institute.
- Brent, L. (2019). NATO's Role in Cyberspace. ,NATO Review. Accessed May 12, 2019.
- http://nato.tagomago.be/files/Pages/2019/Also-in-2019/natos-role-in-cyberspace-alliance-defence/EN/index.htm
- Cyrus Jabbari. (2018). The Application of International Law in Cyberspace: State of Play. October 25h. Accessed May 06, 2019. https://www.un.org/disarmament/update/the-application-of-international-law-in-cyberspace-state-of-play/
- Ducaru, S. (2018). NATO advances in its new operational domain: cyberspace. Accessed February 02, 2019. https://www.fifthdomain.com/opinion/2018/07/05/nato-advances-in-its-new-operational-domain-cyberspace/
- Hartmann, U. (ed.) (2009). Connecting NATO: NCSA Under the Leadership of Lieutnant General Ulrich H.M.Wolf. Berlin: Hartmann Miles-Verlag.
- Hunker, J. (2013). NATO and cyber security. In Herd, P. G. & Kriendler, J. (eds.). Understanding NATO in the 21 st century: Alliance strategies, security and global governance. New York: Routledge.
- Kissel R. (ed.) (February 2011). Glossary of Key Information Security Terms. Accessed May 12, 2019. http://csrc.nist.gov/publications/nistir/ir7298-rev1/nistir-7298-revision1.pdf
- NATO. (2010). Active Engagement, Modern Defence. Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation adopted by Heads of State and Government. Lisbon, Portugal. Accessed May 1, 2019.
- https://www.nato.int/cps/ua/natohq/official_texts_68580.htm
- NATO. (2014). Wales Summit Declaration. Heads of State and Government participating in the meeting of the North Atlantic Council. Wales. Accessed April 2, 2019.
- https://www.nato.int/cps/ic/natohq/official_texts_112964.htm
- NATO. (2016). Nato Cyber Defence. Fact Sheet. Accessed March 03, 2018. https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-eng.pdf
- Pindar, J. & Rigelsford, J. (2011). Cyber security and Information Assurance. The University of Sheffield.
- Reveron S. D. (ed.) (2012). Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World. Georgetown University Press.
- Schreier F., Weekes B., Winkler H. T. (2011). Cyber Security: The Road Ahead. DCAF Horizon 2015 Working Paper Series (4). Accessed March 04, 2016. http://www.dcaf.ch/Publications/Cyber-Security-The-Road-Ahead

- Withman E. M. & Mattord J. H. (2012). Principles of Information Security Fourth Edition. Boston: Course Technology, Cengage Learning.
- Моран, Д. (2009). Географија и стратегија. Во Бејлис, Џ., Вирц, Џ., Греј, К., & Коен, Е. (Eds., 2007), Стратегија во современиот свет, Второ издание (с. 122-139). Скопје: Нампрес.