# NATO i kibernetička obrana

**Milikić, Valentina**

Sveučilište u Zagrebu
Fakultet političkih znanosti
Diplomski studij politologije

Valentina Milikić

# NATO I KIBERNETIČKA OBRANA

DIPLOMSKI RAD

Zagreb, 2023.

Sveučilište u Zagrebu
Fakultet političkih znanosti
Diplomski studij politologije

Valentina Milikić

# NATO I KIBERNETIČKA OBRANA

DIPLOMSKI RAD

Mentor: prof. doc. dr. sc. Robert Barić
Studentica: Valentina Milikić

Zagreb, 2023.

IZJAVA O AUTORSTVU

Izjavljujem da sam diplomski rad *NATO i kibernetička obrana*, koji sam predala na ocjenu mentoru prof. doc.dr.sc. Robertu Bariću, napisala samostalno i da je u potpunosti riječ o mojem autorskom radu. Također, izjavljujem da dotični rad nije objavljen ni korišten u svrhe ispunjenja nastavnih obaveza na ovom ili nekom drugom učilištu, te da na temelju njega nisam stekla ECTS bodove.

Nadalje, izjavljujem da sam u radu poštivala etička pravila znanstvenog i akademskog rada, a posebno članke 16.-19. Etičkoga kodeksa Sveučilišta u Zagrebu.

Valentina Milikić

# SADRŽAJ

1. UVOD ..... 1
2. TEORIJSKO – KONCEPTUALNI OKVIR ..... 2
2.1 Koncept kibernetičke obrane i kibernetičkog prostora ..... 3
2.2 Strategije, relevantnost i transformacija kibernetičke obrane i NATO–a ..... 5
2.3 NATO i zajedničko djelovanje ..... 6
3. DIZAJN ISTRAŽIVANJA I ANALIZA PODATAKA ..... 7
3.1 Koordinacija i utjecaj kibernetičkih napada na organizacijski razvoj NATO–a ..... 11
3.2 Spremnost NATO – a za kibernetičko ratovanje ..... 13
4. ANALIZA RAZVOJA KIBERNETIČKE OBRANE U NATO–u ..... 14
4.1 Kibernetička obrana u NATO–u ..... 14
4.2 Razvoj promjene kibernetičke obrane od 1999. do 2006. godine ..... 16
4.3 Ključne promjene kibernetičke obrane 2007. i 2008. godine ..... 17
4.4 Ključne promjene kibernetičke obrane od 2008. do 2010. godine ..... 19
4.5 Ključne promjene kibernetičke obrane od 2011. do 2013. godine ..... 20
4.6 Ključne promjene kibernetičke obrane 2014. i 2015. godine ..... 23
4.7 Ključne promjene kibernetičke obrane od 2015. do 2017. godine ..... 25
4.8 Ključne promjene kibernetičke obrane od 2018. do 2021. godine ..... 26
5. IZAZOVI RAZVOJA KBERNETIČKE OBRANE I POLITIČKE ODLUKE ..... 28
5.1 Potencijalni problemi u razvoju kibernetičke obrane ..... 28
5.2 Politički procesi, politička tijela i njihova relevantnost u razvoju kapaciteta kibernetičke obrane i odgovaranja na sigurnosne prijetnje u NATO–u ..... 30
6. ZAKLJUČAK ..... 33
7. LITERATURA ..... 36
8. SAŽETAK I KLJUČNE RIJEČI ..... 39
9. SUMMARY AND KEYWORDS ..... 40

# POPIS ILUSTRACIJA

Tablice

Tablica 1: Transformacija kibernetičke obrane NATO–a ..... 9

# 1. UVOD

S obzirom na to da se reforma NATO[1]–a kao bitnog aktera u međunarodnim odnosima još uvijek provodi potaknuta pojavom novih prijetnji i sigurnosnih okolnosti, važno je identificirati nove eksterne i interne čimbenike u geopolitičkom poretku. Razvoj NATO–a se također oslikava i na novo usmjerenje organizacije prema aktualnim pitanjima razvoja tehnologije koja u suvremenom svijetu poprima posebnu važnost. S obzirom na konstantni proces širenja NATO–a poslije Hladnoga rata tema je još uvijek relevantna. Zbog relevantnosti i opsega reformi NATO–a koja se događa na civilnom, vojnom i političkom području, s relativno novom kibernetičkom dimenzijom, rad je fokusiran na reformu kibernetičkih sposobnosti unutar NATO–a. Reforma kibernetičkih sposobnosti zahtijeva obuhvatni međunarodni i politički kontekst za dubinsko opisivanje uzroka prilagodbe.

Tema rada je kibernetička obrana u NATO–u. Rad definira kibernetičku obranu, identificira sigurnosne prijetnje koje su dovele do određenih pravnih, odnosno političkih[2] promjena koje su utjecale na razvoj kibernetičke obrane, konkretno u NATO–u. Objašnjava uzročno–posljedične veze između kibernetičkih napada i promjena politike. U radu se analizira na čemu se temelji adaptacija mjera u NATO–u; kako i zašto članice surađuju u takvom okviru i nudi pregled bitnih summita koji su doveli do promjena u kibernetičkoj obrani. Stoga da bi se odgovorilo na uzroke promjena u ovom području u NATO–u, rad će biti vođen istraživačkim pitanjem koje glasi: Kako su političke odluke donesene zbog nastalih sigurnosnih prijetnji utjecale na razvoj kibernetičke obrane u NATO–u?

Rad je empirijskog karaktera jer nudi podlogu za kvalitativnu analizu političkih odluka koje su direktan rezultat i svrha održanih NATO summita koji se bave kibernetičkom sigurnošću; te povezuje domenu kibernetičke sigurnosti s domenom političkih odluka. Rad može poslužiti kao podloga za komparativnu analizu sa drugim radovima koji se nastoje baviti tom tematikom. Rad može poslužiti kao osnova za kvantitativnu analizu učestalosti kibernetičkih napada s obzirom na

[1] Organizacija Sjevernoatlantskog ugovora (NATO–North Atlantic Treaty Organisation) je vojno–politički savez zemalja Europe i Sjeverne Amerike. Osnovan je u Washingtonu 1949. godine u svrhu kolektivne obrane od agresije.
[2] Termin 'politički' se u radu koristi kao prijevod engleske riječi 'policy' koja označava zakon, propis, postupak, administrativnu radnju ili praksu vlada i drugih institucija i sl. U hrvatskom književnom jeziku ne postoji prikladan prijevod pojma 'policy'–on se koristi s obzirom na kontekst, što otežava analitičku preciznost u znanstvenim radovima.

povećanje sigurnosnih prijetnji. Odgovori na sigurnosne prijetnje u obliku političkih odluka (kao i tehnološki razvoj) dovode do promjena u kibernetičkoj obrani. Rad može poslužiti kao osnova za analizu brzine usvajanja političkih odluka s obzirom na vremenski razmak od njihovog donošenja do njihove implementacije.

Prema najnovijim istraživanjima M–trenda, vodeće publikacije u industriji koja kombinira obavještajne podatke i sigurnosne uvide o kibernetičkim prijetnjama; profesionalne i poslovne usluge, financije, maloprodaja i ugostiteljstvo, zdravstvo i visoka tehnologija su najugroženiji sektori. Za sprječavanje eksfiltracije obavještajnih podataka u NATO–u i osiguranje mreže od sve češćih kibernetičkih napada i krađa, bitno je podići svijest o novoj realnosti s kojom se suočava NATO, ali i svaka organizacija kojoj tehnološka oprema osigurava financijski i strateški opstanak. Bitno je uočiti da napredak na području kibernetičke obrane, pogotovo u vojno – političkim savezima, ovisi o političkom kontekstu i političkim odlukama koje su donesene kao odgovor na sigurnosne prijetnje; ili za dobivanje političke prednosti upravljanjem postojećim, ali i za izradu novih resursa. Za analizu kibernetičke obrane u NATO–u, poslužit će; sigurnosne prijetnje, političke odluke i promjene u kibernetičkoj obrani kao varijable koje potencijalno mogu dati odgovor na uzrok kibernetičkog napretka; koje će detaljnije biti objašnjene u samoj analizi rada. Za bolje razumijevanje tematike, rad će pojasniti relevantne koncepte vezane uz kibernetičku obranu, kao i politička tijela i procese relevantne za njezin razvoj. Rad će se osvrnuti na kibernetičke kapacitete i sigurnosne izazove u Savezu, kao i na posebnu važnost zajedničkog djelovanja u NATO–u.

## 2. TEORIJSKO – KONCEPTUALNI OKVIR

Studija obuhvaća tri varijable: **sigurnosne prijetnje**, **političke odluke** (održane konferencije/sporazumi/dokumenti/summiti) na kojima se temelje promjene i treću varijablu koju predstavljaju **promjene u kibernetičkoj obrani**, odnosno konkretna implementacija nadogradnje u kibernetičkom sektoru kao direktan rezultat političkih odluka. Sve tri navedene varijable su kodirane i kategorizirane u sedam kategorija koje čine smislene cjeline prema ključu uzročno–posljedičnih veza. **Prva** kategorija obuhvaća konflikt u Kosovu 1999. godine, te razdoblje političkih odluka i promjena u kibernetičkoj obrani od 2002. do 2006. godine. **Druga**

kategorija obuhvaća razdoblje od 2007. godine kada su se dogodili kibernetički napadi u Estoniji, nadolazeće političke odluke 2008. godine, i obuhvaća nadogradnju u NATO–voj kibernetičkoj obrani 2008. godine. **Treća** kategorija obuhvaća sigurnosnu prijetnju rusko–gruzijskog rata 2008. i promjene koje slijede 2009. i 2010. godine. **Četvrta** kategorija obuhvaća sigurnosne probleme u obliku nedovoljne informacijske koordinacije i političke i obrambene promjene od 2011. do 2013. godine kao posljedicu. **Peta** kategorija obuhvaća razdoblje kibernetičkih napada od 2014. i promjene koje su se dogodile 2014. i 2015. godine. **Šesta** kategorija obuhvaća ruske napade na ukrajinsku električnu mrežu 2015. i promjene nastale kao rezultat 2016. i 2017. godine. **Sedma** kategorija uključuje kibernetičke prijetnje, političke odluke i razvoj u kibernetičkoj obrani od 2018. do 2021. godine. Varijable su posložene tako da daju uvid u utjecaj političkih odluka uzrokovanih međunarodnim događanjima na što jednostavniji način koji identificira razloge nadogradnje za koje stoji pretpostavka da se događaju prema kronološkom ključu. Pretpostavka je da se prijetnje mogu pratiti od točke kibernetičkih napada sve do njihovih učinaka na razvoj kibernetičke obrane koja slijedi narednih mjeseci/godina poslije napada u obliku povećane potrebe za resursima sigurnosne zaštite. Provjera postavljenih uzročno–posljedičnih veza se temelji na dvije hipoteze. **Prva hipoteza** glasi: napredak i brzina razvoja kibernetičke obrane ovisi značajno o političkim odlukama i usvajanju istih. Što je implementacija političkih odluka brža to je razvoj kibernetičke obrane brži. **Hipoteza broj dva** tvrdi da: ako ne dođe do ozbiljnih sigurnosnih prijetnji koje mijenjaju strukturu same organizacije (ili one nisu uočene), promjene u kibernetičkoj obrani izostaju.

## 2.1 **Koncept kibernetičke obrane i kibernetičkog prostora**

Za razumijevanje kibernetičke obrane, bitno je upoznati se s konceptom kibernetičkog prostora, kojega je kibernetička obrana dio. Kibernetički prostor je reguliran međunarodnim pravom u smislu odgovora na kibernetičke napade, jer spada u gospodarsku i komunikacijsku sferu bitnu za napredak društva, te zbog toga kibernetički napadi kao takva prijetnja uživaju pozivanje na protumjere (Hammock, 2017:88). Unatoč tome regulacija međunarodnog prava u području kibernetičkog područja nije dovoljno razvijena. Nema jasnih kriterija na temelju kojih bi bio pokrenut kolektivni odgovor na kibernetičku prijetnju. Problemi koji se tiču primjene međunarodnog prava na kibernetički prostor se mogu podijeliti u pet kategorija. Prva kategorija se odnosi na nedostatnu inicijativu većine država da izraze mišljenje i odrede pravila koja bi se

primjenjivala u međunarodnom pravu (Carnegieendowment.org, 2021). Druga kategorija se odnosi na nedostatak dogovora oko pravnog okvira i načina na koji bi se međunarodno pravo bavilo pitanjem samoobrane u slučaju kibernetičkog napada (Carnegieendowment.org, 2021). Treća kategorija odnosi se na poteškoće koje bi proizašle iz interpretacije međunarodnog prava, pripisivanja krivnje za kibernetičke napade i prikladnost djelovanja međunarodnog prava na području nad kojem države, cjelokupno gledano, nemaju kontrolu (Carnegieendowment.org, 2021). Četvrta i peta kategorija problema se odnose na pravnu prikladnost i praksu država koje se rijetko pozivaju na međunarodno pravo kada optužuju druge države na izvršenje kibernetičkog napada (Carnegieendowment.org, 2021). Pravni problem pripisivanja krivnje se dodatno komplicira pitanjem prikladnosti primjene međunarodnog prava na aktere koji nisu države. Problemi vezani uz regulaciju međunarodnog prava na kibernetičkom području predstavljaju izazov koji zahtijeva pozornost jer kibernetički napadi mogu izazvati ozbiljne posljedice na državnu stabilnost.

Za očuvanje stabilnog sustava potrebna je izgradnja dostatne razine kibernetičke sigurnosti. Kibernetička sigurnost, u svojoj najosnovnijoj razini podrazumijeva sigurnost od kibernetičke eksploatacije (pokušaji da se steknu informacije iz računalne mreže) i sigurnost od kibernetičkih napada (težnja za uništavanjem, remećenjem računalne mreže) (Burton, 2015:299). Kibernetički prostor kao domenu operacija uz tradicionalne domene kopna, mora i zraka, NATO je prepoznao 2016. godine; što je vojnom sektoru omogućilo bolju zaštitu operacija od kibernetičkih prijetnji, obuhvaćajući i oslanjanje na nacionalne kibernetičke sposobnosti saveznika (NATO, 2021a).

NATO–ova kibernetička obrana kompleksan je sustav procesa, teorija i suradnje za provedbu politike kibernetičke obrane, te se ona odnosi na ukupnost aktivnosti koje se provode u interesu kibernetičke sigurnosti NATO–a (Nagy i Sherifi, 2013: 334). Prema NATO–ovoj politici kibernetičke obrane, njegov glavni prioritet je zaštita komunikacijskih sustava kojima upravlja Savez, te se od nacija očekuje da preuzmu odgovornost i ulažu u razvoj vlastitih sposobnosti jer kritična infrastruktura ostaje nacionalna odgovornost, a NATO pomaže u izgradnji dijeleći prakse, informacije i provodeći vježbe kibernetičke obrane (Nagy i Sherifi, 2013: 334).

NATO pomaže članicama u kibernetičkoj obrani putem vježbi za kibernetičke obrane[3] i

[3] Kibernetička koalicija (Cyber Coalition) je NATO–ova godišnja vježba kolektivne kibernetičke obrane. Planira ga i provodi Savezničko zapovjedništvo za transformaciju pod upravom Vojnog odbora.

obrazovanjem. Pomoć je vidljiva i u obliku dijeljenja i razmjene informacija o zlonamjernim softverima i prijetnjama u stvarnom vremenu putem platforme za razmjenu informacija, razvijanjem ciljeva za saveznike kako bi se olakšao zajednički pristup sposobnostima obrane i održavanjem timova za brzu reakciju kibernetičke obrane (NATO, 2021a).

## 2.2 Strategije, relevantnost i transformacija kibernetičke obrane i NATO–a

S obzirom na to da sposobnosti kibernetičke obrane mogu biti instrument za postizanje razvijenosti informacijske, gospodarske, ekonomske i vojne sigurnosne sfere interesa, dolazi do transformiranja NATO–a. Reforma NATO–a uključuje kibernetičku sigurnost; a njezin razvoj ima direktan utjecaj na državnu moć, ali i moć samoga Saveza. Rad kritičnih infrastruktura ovisi o razini kibernetičke sigurnosti što utječe na cjelokupnu sigurnost države. Više od 100. 000 ljudi se oslanja na NATO mreže uzimajući u obzir da NATO–ova IT infrastruktura pokriva preko 60 različitih lokacija, polazeći od vojnih zapovjedništava, mjesta na kojima se provode NATO operacije, sve do političkih struktura odlučivanja u Bruxellesu (NATO, 2021a). Sustavi NATO–a svakodnevno bilježe sumnjive događaje, od sofisticiranijih do nižih razina napada; od kojih se većina detektira i suzbija automatski, no neki zahtijevaju analizu stručnjaka (NATO, 2021a). Sprječavanje upada u mrežu, otkrivanje, procjenu, dijeljenje i analizu informacija, te sprječavanje gubitka podataka svakodnevno provodi kibernetički tim[4] od 200 članova koji brani NATO–ove mreže 24 sata dnevno (NATO, 2021a). Informacijski razvoj je doveo do intenziviranja pojave hibridnog ratovanja. Linija između rata i mira postaje sve nedefiniranija, te se metode suzbijanja prijetnji temelje na širokoj uporabi informacijskih, ekonomskih, političkih, humanitarnih, vojnih i nevojnih sposobnosti. Hibridno ratovanje je pristup koji kombinira vojna i nevojna sredstva korištena za stjecanje političkog utjecaja nad protivnikom (Ducaru, 2016:10).

U odnosu na tradicionalno oružje, kibernetičko ima svojevrsne prednosti poput: financijske efikasnosti u proizvodnji kibernetičkog oružja i njegovo simultano korištenje za napade na različite organizacije i vlade (Ruiz i Winter, 2017:79). Prednosti uključuju i mogućnost višestruke uporabe, poteškoća u identificiranju izvora napada, te njegova sposobnost nadilaženja samoga kibernetičkog prostora i uzrokovanja kinetičkih učinaka (Ruiz i Winter, 2017:79).

[4] Kibernetički tim NATO–a sprječava upade u mrežu, otkriva i dijeli informacije o zlonamjernom softveru, sprječava gubitak podataka i provodi procjene funkcionalnosti sustava.

## 2.3 **NATO i zajedničko djelovanje**

Kolektivna obrana NATO–a je zapisana u članku 5 Sjevernoatlantskog ugovora. Kolektivnom obranom članice se obvezuju djelovati udruženim protunapadom ukoliko jedna od članica bude napadnuta. Suradnja je bitna za učinkovito odgovaranje na hibridne prijetnje, stoga treba razvijati komplementarne strategije. Posebno treba naglasiti suradnju NATO–a i Europske unije. Područja koja su iznimno bitna za napredak kooperacije EU–a i NATO–a i koja treba aktivno razvijati su strateške komunikacije, kibernetička obrana, svijest o okolnostima i civilno–vojna kooperacija (Ducaru, 2016:16). U prosincu 2016. godine Europska unija i NATO su dogovorili paket od preko 40 mjera usmjerenih na rješavanje hibridnih prijetnji, no dolazi do ograničavanja suradnje zbog fokusa na različite programe EU i NATO–a, jer dok EU drži fokus na regulativnoj razini i praksu kibernetičke obrane putem mehanizama kao što je NIS Direktiva[5], NATO se uglavnom fokusira na pripravnost i izgradnju sposobnosti u kibernetičkoj obrani (Mad'ar, 2019:18). Obje organizacije naglašavaju da je kibernetička sigurnost nacionalna odgovornost (Pernik, 2011:7). Burton naglašava da kibernetički napadi nisu samo nacionalni problem. Zbog sve češće prirode takvih napada koji uzrokuju sve skuplju štetu vladinim upravama, potencijalnim transportnim i opskrbnim mrežama i drugoj kritičnoj infrastrukturi, trebaju podleći pod kolektivnu prijetnju (Burton, 2015:307).

Po organizacijskoj pripravnosti, NATO je u prednosti u odnosu na Europsku uniju koja je tek krajem 2014. godine usvojila prvi okvir politike kibernetičke obrane (Mad'ar, 2019:18). Dakle da bi došlo do bolje kooperacije i kompatibilnosti NATO treba raditi na jačanju EU kapaciteta što bi dovelo do sinkroniziranije suradnje. Suradnja smanjuje transakcijske troškove i prostor za podjele, a to se ostvaruje kroz institucionalne okvire (Burton, 2015:319). Suradnja NATO–a s partnerima je bitna zbog efektivnijeg provođenja istraživanja. Trajanje istraživačko–razvojnog rada može biti skraćeno kooperacijom privatnog, akademskog i javnoga sektora pod uvjetom razvijenih mehanizama razmjene informacija (Cybersecforum.eu, 2017:34). Unutar okvira

[5] NIS (Network and Information Security) se sastoji od tri dijela; 1. Nacionalne sposobnosti (članice moraju imati određene sposobnosti poput CSIRT–a i kibernetičkih vježbi), 2. Prekogranične suradnje (EU CSIRT mreža, skupina NIS–a za suradnju), 3. Nacionalnog nadzora kritičnih sektora (članice moraju nadzirati cyber sigurnost kritičnih tržišnih operatera u svojoj zemlji, nadzirati kritičnim sektorima energije, prometa, vode, zdravstva, sektora financija i digitalne infrastrukture, te nadzirati pružatelje digitalnih usluga poput mrežne tražilice i tržišta).

NICP–a[6] takvi se mehanizmi ostvaruju na osnovi IPA[7] sporazuma kojega NCIA[8] sklapa s industrijskim sektorom, s tvrtkama kao na primjer FireEye ili RSA Security (Cybersecforum.eu, 2017:34). Industrija u ulozi opskrbljivača pribavlja pristup najnovijim dostignućima u znanosti i tehnologiji što je ključno za pronalaženje rješenja za poboljšanje i zaštitu kibernetičke sigurnosti.

## 3. DIZAJN ISTRAŽIVANJA I ANALIZA PODATAKA

Ovaj rad koristi kvalitativni pristup razvoja i istraživanja razine spremnosti NATO–a da odgovori na čin kibernetičkog rata. Metoda prikupljanja podataka uključuje analizu političkih dokumenata, članke iz časopisa, preglede, objave dostupne na NATO–vim stranicama i izvješća o obrani. U radu se analiziraju povijesni odgovori i razvoj kibernetičke obrane u NATO–u izazvani kibernetičkim napadima na državne kritične infrastrukture. Sposobnost kibernetičke obrane je bitno analizirati s obzirom na sve veći značaj kibernetičkog, ali i hibridnog ratovanja kao prijetnje.

Istraživačko pitanje se odnosi na organizacijski razvoj koji je popraćen zajedničkim djelovanjem i donošenjem političkih promjena u okviru NATO–a. S obzirom na to da je kibernetička obrana povijesno gledano relativno novo područje obrane, koje je u NATO–u kao domena u ratovanju; koja je dio kolektivne obrane, formalno prepoznata 2016. godine, analiza će se usredotočiti na razdoblje od 1999. godine kada se dogodio 'Prvi web rat' do 2021. godine.

Napredak i brzina razvoja kibernetičke obrane ovisi značajno o političkim odlukama i brzini usvajanja istih. Jedinica analize, odnosno slučaj u kojemu se javlja fenomen koji se analizira (kibernetička obrana) je organizacija NATO. Dakle, radi se o dizajnu maloga N, odnosno o studiji slučaja koja sadržava kvalitativnu analizu procesa. Radi se o kvalitativnoj analizi sadržaja

[6] NATO industrijsko kibernetičko partnerstvo (NATO Industry Cyber Partnership) je inicijativa koju je pokrenuo NATO za jačanje suradnje s industrijom i akademskom zajednicom u vezi s kibernetičkim prijetnjama. Inicijativa je pokrenuta 2014. godine.

[7] Ugovori o partnerstvu s industrijom (Industry Partnership Agreements)

[8] NATO agencija za komunikacije i informacije (NATO Communications and Information Agency): isporučuje naprednu tehnologiju za zapovijedanje, kontrolu, komunikacije, računala, obavještajne podatke, nadzor i izviđanje (C4ISR). Agencija je odgovorna za nabavu tehnologije, eksperimentiranje, promicanje interoperabilnosti, projektiranje i inženjering sustava i arhitekture, kao i testiranje i tehničku podršku. Također pruža usluge komunikacijskih i informacijskih sustava (CIS) kao potporu vježbama, misijama i operacijama Saveza.
Osim toga, Agencija provodi središnje planiranje, inženjering sustava, implementaciju i upravljanje konfiguracijom za NATO–ove sustave zračnog zapovijedanja i kontrole (Air C2).

jer pokušava analizirati kako političke odluke utječu na izgradnju kibernetičke obrane u određenoj organizaciji kroz vrijeme. Istraživanje ujedinjuje područje međunarodnih odnosa i sigurnosnih studija. Istraživačko pitanje je pitanje empirijskog karaktera jer nudi podlogu za kvalitativnu analizu političkih odluka. Istraživačko pitanje sa sobom povlači i pitanje spremnosti NATO–a na hibridno ratovanje i njegovu organizacijsku preobrazbu s obzirom na prijetnje.

Fokus analize je razvoj kibernetičke obrane u NATO–u. Odnosno **razvoj kibernetičke obrane je ovisna varijabla** koja se mijenja, odnosno dolazi do svojevrsne nadogradnje u tom području (i samoj obrani kojoj je fokus bio prebačen s ofenzivnog na defenzivni karakter). **Neovisne varijable su političke odluke** koje su preduvjet reforme NATO–a. S obzirom na to da sigurnosne prijetnje uzrokuju nastanak političkih odluka (ali i obratno), političke odluke će kao takve biti rezultat međunarodnih zbivanja, ali se s obzirom na istraživačko pitanje one definiraju kao neovisne iako se kroz rad moraju objasniti i kao posljedica (odgovor na sigurnosnu prijetnju). Stoga rad osim deskripcije koristi i objašnjavanje uzročnosti pojave. Rad će se većinski koristiti kvalitativnom analizom i deskriptivnom metodom jer prikazuje razvoj organizacije kroz vrijeme. Odnosno pitanje; '**Kako** su političke odluke donesene zbog nastalih sigurnosnih prijetnji utjecale na razvoj kibernetičke obrane u NATO–u?' odražava da se radi o opisivanju razvoja. Istraživačko pitanje se fokusira na razloge zbog kojih se reforma dogodila, te kako se razvijala kroz vrijeme. Rad definira kibernetičku obranu i objašnjava na čemu se temelji adaptacija mjera usvojenih od 1999. do 2021. godine u NATO–u.

Tablica 1: Transformacija kibernetičke obrane NATO–a

| | SIGURNOSNE PRIJETNJE | POLITIČKE ODLUKE | PROMJENE U KIBERNETIČKOJ OBRANI |
|---|---|---|---|
| **KATEGORIJA 1 (1999-2006)** | **konflikt u Kosovu 1999.g.** (srpski hakeri – 'Prvi web rat') | **1999.g.–Strateški koncept**<br>**2002.g.-summit u Pragu**<br>**2003.g. -** devet zemalja NATO-a potpisuju **sporazum** o većoj razmjeni informacija o kibernetičkoj sigurnosti<br>**2006.g.-NATO summit Riga** | **formiranje NCIRC – a** (9/11/2001 – Bush 2001. uspostavlja National Electronic Crime Task Force)<br>2004.g. -uspostavljen **NCSA**<br>**2006.g. -**dodatno osiguravanje NATO inf. sistema protiv cyber napada<br>**- stvoreno Savezničko zapovjedništvo za transformaciju (ACT–SAD) i Savezničko zapovjedništvo za operacije (ACO–Belgija)** |
| **KATEGORIJA 2 (2007/2008)** | **kibernetički napadi u Estoniji 2007.g.** | **2008.g.-**odobrena **prva politika NATO-a o kibernetičkoj obrani**<br>**2008.g.-summit u Bukureštu** – NATO potiče težnju Gruzije i Ukrajine za članstvom | Uspostava **CDMA** (Cyber Defence Management Authority)<br>2007.g. – **ICTM**<br>2008.g. – Uspostava **CCD COE** (Cooperative Cyber Defence Centre of Excellence) |
| **KATEGORIJA 3 (2008-2010)** | **2008.g. Rusko–gruzijski rat i Stuxnet virus**<br>**2010.g. hibridni ratovi u Ukrajini** | **2009.g. - summit Strasbourg-Kehlu**<br>**2010.g. – summit u Lisbonu** | Sigurnosne kibernetičke policy promjene vojnog karaktera<br>-kibernetička obrana treba postati sastavni dio NATO vježbi |
| **KATEGORIJA 4 (2011-2013)** | - nedovoljna informacijska koordinacija između članica NATO–a kao sigurnosna prijetnja | **2011.g. - uključivanje kibernetičke sigurnosti u Strateški koncept**<br>**2012.g.– summit u Chicagu**<br>**2012.g. konferencija "Smart Defense i budućnost NATO–a"**<br>**2013.g.** (dokument) **- Priručnik iz Tallinna o međunarodnom pravu primjenjivom na kibernetičko ratovanje** (pravni i tehnički stručnjaci zajedno surađuju sa CCD COE–om) | **2012.g.-** Stvaranje tima za brzo reagiranje – reagira na kibernetičke napade dok su oni **u tijeku** (**'Rapid Reaction Team'** u NATO–u)<br>**2012.g.–uspostavljena NCIA**<br>**2013.g.- razvoj multinacionalne kibernetičke obrane**<br>- kooperacija legalnih i tehničkih eksperata |

| | | | |
|---|---|---|---|
| **KATEGORIJA 5 (2014/2015)** | **2014.g.- NATO-ove web stranice pogođene kibernetičkim napadom** povezane su s napetostima na Krimu<br><br>**2014.g.**– **Kriza u Ukrajini** | **2014: summit u Walesu: (**daljnji razvoj kibernetičke obrane i nastavak debate iz Estonije (promjene u članku 5 NATO –a: kolektivna obrana)**)**<br>- **dekret 744/2014** | **2015.g**.- Uspostava Nacionalnog centra za kibernetičku sigurnost u Ukrajini koji surađuje s NATO–om i CERT-UA–om |
| **KATEGORIJA 6 (2015-2017)** | **2015.g.- Rusija napada ukrajinsku elektrodistribucijsku mrežu i nakon toga pokrenula DDoS napade**, zbog kojih je 230.000 stanovnika ostalo bez struje do 6 sati. | **2016.g.– summit u Varšavi** (kiberprostor kao operativna vojna domena – NATO odgovara konvencionalnim oružjem na kibernetičke napade)<br><br>**2017.g.– ažuriranje Akcijskog plana kibernetičke obrane** + plan implementacije kibernetičkog prostora kao domene + novi skup ciljeva | **2015.g.- razvijen Memorandum o razumijevanju o kibernetičkoj obrani**<br><br>**2016./2017.g.**– veća suradnja NATO-a i EU u kibernetičkoj obrani<br><br>- uspostava Cyber Defence Pledge |
| **KATEGORIJA 7 (2018-2021)** | zlonamjerne kibernetičke aktivnosti uključujući cyber napade na zdravstvene usluge, bolnice i istraživačke institute tijekom pandemije COVID – 19<br><br>2021.g. - incidenti s ransomwareom i aktivnosti, usmjerene na institucije i kritičnu infrastrukturu, kao i iskorištavanje slabosti u lancima opskrbe | **2018.g.– summit u Bruxellesu** (odluka za uspostavom novog centra za operacije u kibernetičkom prostoru + NATO može koristiti nacionalne kibernetičke sposobnosti za svoje operacije)<br>**2019.g.– prihvaćanje vodiča** koji postavlja niz alata za daljnje jačanje sposobnosti<br>**2021.g. summit u Bruxellesu**: nova Sveobuhvatna politika kibernetičke obrane (obrana + krizni menadžment + kooperativna sigurnost)<br>**2021.g.**– NATO imenuje prvog CIO (službenika za informiranje) | - postavljanje novih cyber alata<br><br>- suradnja NATO–a i EU kroz Tehnički aranžman o kibernetičkoj obrani (koji je potpisan 2016)<br><br>- jačanje u razmjeni informacija, treningu istraživanju i vježbi<br><br>- jača NATO suradnja s industrijom kroz NATO Industry Cyber Partnership<br><br>- aktivna obrana na političkom,vojnom i tehničkom nivo – u<br><br>- novi centar za operacije u kibernetičkom prostoru |

Izvor: autor.

## 3.1 **Koordinacija i utjecaj kibernetičkih napada na organizacijski razvoj NATO–a**

Strateško promišljanje u NATO–u se iz temelja mijenja, a jedan od činilaca promjene je brža priroda suvremenih kibernetičkih napada, koji se odvijaju bez upozorenja, s bilo koje lokacije preko globalno povezane mreže računalnih sustava (Burton, 2015:302). Za suzbijanje takvih prijetnji potrebna je visoka razina koordinacije. Koordinaciju osiguravaju CDMA[9] i NCIRC[10] koji dijele obavještajne podatke i posjeduju mogućnost praćenja incidenata u stvarnom vremenu, a djeluju unutar kibernetičkog zapovjedništva koje se nalazi u središtu Bruxellesa (Burton, 2015:309). NATO je kao rezultat usvajanja Politike kibernetičke obrane proširio svoj prostor djelovanja u tom području, no njegova vlastita operativna sigurnost je prioritet (Burton, 2015:309). Kao koordinacijsko tijelo, u NATO–u je uspostavljen Upravni odbor za kibernetičku obranu, odnosno CDMB[11], uz koji NCIRC otkriva i odgovara na kibernetičke napade (Ccdcoe.org, 2014). NICP spaja nacionalne CERT–ove[12], akademski sektor i IT kompanije. Unutar okvira NICP–a djeluje NCIA koja doprinosi ophođenjem informacijama stvaranjem posebnog sistema koordiniranja informacijama CIICS–a[13] čiji se kapaciteti koriste u sustavima satelitske komunikacije, protuzračne i kibernetičke obrane, te kao dio projekata za podršku u sustavima kontrole i zapovijedanja (Cybersecforum.eu, 2017:33). Neki od primjera nabave kibernetičke obrane uključuju već prije spomenuti NCIRC, nabavu kriptografske opreme za komunikacijsku infrastrukturu i instalacija aktivnog mrežnog elektroničkog sigurnosnog sustava ANWI ESS; čija cijena ulaganja za svaki spomenuti resurs pojedinačno iznosi preko 350 000.00 dolara (Cybersecforum.eu, 2017:33). Nadalje, NATO unaprjeđuje kibernetičku sigurnost putem

[9] NATO–vo tijelo za upravljanje kibernetičkom obranom (Cyber Defence Management Authority): pruža centralizirani ured za koordinaciju odgovora članica na spektar kibernetičkih napada. Sjedište mu je u Bruxellesu. Odgovoran je za pokretanje i koordinaciju akcije kibernetičke obrane kada je to potrebno.

[10] Služba NATO–a za odgovor na računalne incidente (NATO Computer Incident Response Capability) štiti mreže NATO-a pružajući centraliziranu i 24–satnu podršku kibernetičke obrane. Sjedište se nalazi u Monsu.

[11] Upravni odbor za kibernetičku obranu (Cyber Defence Management Board) zadužen je za strateško planiranje i izvršno vodstvo vezano uz NATO mreže. Također potpisuje memorandume o razumijevanju s državama članicama kako bi olakšao razmjenu informacija i koordinirao podršku. Sastoji se od predstavnika svih glavnih dionika kibernetičke sigurnosti unutar NATO–a.

[12] Tim za računalne hitne slučajeve (Computer Emergency Response Team) je skupina stručnjaka za informacijsku sigurnost odgovornih za zaštitu od kibersigurnosnih incidenata organizacije, otkrivanje i odgovor na njih. CERT–ovi rješavaju, pružaju upozorenja i smjernice za rukovanje incidentima. CERT–ovi također provode stalne kampanje podizanja svijesti javnosti i uključuju se u istraživanja usmjerena na poboljšanje sigurnosnih sustava.

[13] Kibernetički informacijski i koordinacijski sustav za incidente (Cyber Information and Incident Coordination System) ne samo da upozorava o mogućim kibernetičkim napadima, već omogućuje i odgovoranje na napad uz pomoć drugih korisnika.

ICI–a[14], Mediteranskog dijaloga[15], EAPC–a[16] i IPAPs–a[17] s posebnim naglaskom na područje sjevernog Atlantika (Burton, 2015:310).

Doktrina kibernetičke sigurnosti NATO–a obuhvaća tri operacijska područja, a to su krizni menadžment upotrebljavan u Estoniji 2007. godine, zatim kolektivnu obranu utjelovljenu u obliku uznapredovane Politike kibernetičke obrane i treće, kooperativnu sigurnost koju NATO sprovodi gradnjom sve obuhvatnije mreže veza (Burton, 2015:310). Posebnu kooperaciju u operacijama u kibernetičkom prostoru (CO[18]) NATO ostvaruje s Nizozemskom putem CSIC–a[19] čiji je domaćin bio Defense Cyber Command (DCC[20]) (Hammock, 2017:88). DCC je dio Kraljevske nizozemske vojske, a unutar njega dolazi do raspoređivanje mrežnih učinaka unutar faznih vojnih operacija (Hammock, 2017:88). Nizozemci su DCC razvili po uzoru na USCYBERCOM[21]. NATO je u kibernetičkoj sigurnosti s Nizozemskom povezan i putem DefCERT–a[22] koji je u stalnom kontaktu s NCIRC–om zbog unaprjeđenja operativne učinkovitosti (Hammock, 2017:90). NATO kroz SPS[23] i Okvira pomoći za obranu i izgradnju kapaciteta[24] pomaže zemljama s kojima kooperira u izgradnji kapaciteta za kibernetičku sigurnost i pomaže u inovacijama civilnih znanosti i rješavanju izazova (NATO, 2021a). Kroz

[14] Istanbulska inicijativa za suradnju (Istanbul Cooperation Initiative) je partnerski forum koji ima za cilj pridonijeti dugoročnoj globalnoj i regionalnoj sigurnosti nudeći zemljama koje nisu članice NATO–a u široj regiji Bliskog istoka priliku za suradnju s NATO–om (Katar, Bahrein, Kuvajt i Ujedinjeni Arapski Emirati trenutno sudjeluju u Istanbulskoj inicijativi za suradnju).

[15] Mediteranski dijalog forum je suradnje između NATO i sedam zemalja Mediterana. Kao cilj ima stvoriti dobre odnose i bolje međusobno razumijevanje i povjerenje u cijeloj regiji (promičući regionalnu sigurnost i stabilnost i objašnjavajući NATO-ove politike i ciljeve). Prvi put je pokrenut 1994. godine.

[16] Euroatlantsko partnersko vijeće (Euro-Atlantic Partnership Council) je multilateralni forum stvoren za poboljšanje odnosa između NATO–a i ne – NATO zemalja u Europi i srednjoj Aziji.

[17] Pojedinačni akcijski planovi partnerstva (Individual Partnership Action Plans) su planovi razvijeni između NATO–a i različitih zemalja koji ocrtavaju ciljeve i komunikacijski okvir za dijalog i suradnju obje strane. Pokrenuti su 2002. godine.

[18] Operacije u kibernetičkom prostoru (Cyberspace operations) sastoje se od vojnih, obavještajnih i uobičajenih poslovnih operacija DOD–a (Department of Defense) u kibernetičkom prostoru.

[19] Španjolsko nacionalno istraživačko vijeće (CSIC) državna je agencija za znanstveno istraživanje i tehnološki razvoj, s posebnim pravnim statusom, vlastitom imovinom i riznicom.

[20] Kibernetičko obrambeno zapovjedništvo (The Defense Cyber Command) je zapovjedništvo odgovorno za kibernetičku sigurnost Nizozemske obrambene organizacije i njezinih partnera. Fokusira se na 3 područja kibernetičke sigurnosti: obrambene sposobnosti, obavještajne sposobnosti i ofenzivne sposobnosti.

[21] US Cyber Command: njegova je misija usmjeravati, sinkronizirati i koordinirati planiranje i operacije kibernetičkog prostora za obranu i promicanje nacionalnih interesa u suradnji s domaćim i međunarodnim partnerima

[22] DefCERT je odjel unutar nizozemskog ministarstva obrane: on služi kao centralizirani entitet za razmjenu znanja i korištenje zaštitnih mehanizama u nizozemskim umreženim dionicama.

[23] NATO program Znanost za mir i sigurnost (Science for Peace and Security Programme) je NATO program koji podržava suradnju i inovacije civilnih znanosti.

[24] DCB (The Defence and Related Security Capacity Building) je inicijativa koja jača NATO–ovu predanost partnerima i pomaže u projektiranju stabilnosti pružanjem potpore zemljama koje traže pomoć od Saveza.

CCDCOE[25] i zajedničke vježbe nastoji izgraditi jedinstveni pristup kibernetičkoj sigurnosti i razmjenu eksperata u tom području, poduku kao i vojno učvršćivanje: no i dalje službenici preferiraju djelovati samostalno-što ISAC[26] nastoji promijeniti zaštitom ICT[27] uređaja (Hammock, 2017:91). Stoga razvoj komunikacijskih uređaja djeluje kao mehanizam prebacivanja fokusa samostalnog, na zajedničko djelovanje organizacija.

U veljači 2016. godine potpisan je Tehnički sporazum o kibernetičkoj obrani putem kojega NATO surađuje s Europskom unijom, ponajviše u područjima istraživanja, obuke, dijeljenja informacija i vježbi (NATO, 2021). Dakle možemo naglasiti da je iznimno bitno NATO–CERT–EU partnerstvo i da je kibernetička suradnja okidač za organizacijske promjene, strategije i zajedničke vježbe. Ažuriranje NCRSM–a[28] mora uključivati definiranje načina i primjerenoga trenutka kada se trebaju koristiti savezničke nacionalne sposobnosti kibernetičke obrane kada je sustav pod napadom; kao što se i definira upravljanje sposobnostima kada je Savez u opasnosti od tradicionalnih ugroza–čije sposobnosti za djelovanje odobrava NAC[29] (Ducaru, 2016:20).

### 3.2 **Spremnost NATO–a za kibernetičko ratovanje**

Postavlja se pitanje koliko i kada je NATO spreman odgovoriti na sigurnosne prijetnje uvjetovane člankom 5 Sjevernoatlantskoga sporazuma? Najprije treba naglasiti da se strategija Saveza za suzbijanje hibridnih ugroza temelji na trijadi: pripremiti, obraniti i odvratiti, a to se prosljeđuje i na noviju domenu ratovanja u kibernetičkom prostoru u kojemu nacije predstavljaju prvu crtu obrane (Ducaru, 2016:7). Međunarodna suradnja je prijeko potrebna za efektivno odgovaranje na prijetnju, što dovodi do zaključka da se odgovor Saveza na kibernetičke napade još mora razvijati (Ducaru, 2016:7). NATO se obvezao da će braniti članice ukoliko dođe do eskalacije hibridnog ratovanja, no iako je NATO razvio strategije za odgovor na hibridno ratovanje, nije naznačio okolnosti u kojima se one primjenjuju. Suvremene okolnosti zahtijevaju

[25] NATO centar izvrsnosti za kooperativnu kibernetičku obranu (NATO Cooperative Cyber Defence Centre of Excellence): je međunarodna vojna organizacija fokusirana na interdisciplinarno primijenjeno istraživanje i razvoj te konzultacije, treninge i vježbe u području kibernetičke sigurnosti. Nalazi se u Tallinnu.
[26] Centar za razmjenu i analizu informacija (Information Sharing and Analysis Center): je neprofitna organizacija koja pruža mogućnost prikupljanja informacija o kibernetičkim prijetnjama kritičnoj infrastrukturi i pruža dvosmjerne razmjene informacija između javnog i privatnoga sektora.
[27] Informacijska i komunikacijska tehnologija
[28] Priručnik NATO sustava za odgovor na krize (NATO Crisis Response System Manual)
[29] Sjevernoatlantsko vijeće (North Atlantic Council) je glavno političko tijelo za donošenje odluka NATO–a koje se sastoji od stalnih predstavnika zemalja članica Saveza.

nov pristup rješavanju ugroza, a najveća vrijednost NATO–a je upravo u odvraćanju od napada. Za djelotvorno suzbijanje ključna je precizna analiza događaja i brzina identifikacije napadača i razloga za takav pothvat, što uključuje osvještavanje situacije i stručno znanje. Za suzbijanje hibridnih prijetnji i bolju spremnost NATO–a da se suoči s takvim prijetnjama, bitna je suradnja i usvajanje djelotvornih mjera.

# 4. ANALIZA RAZVOJA KIBERNETIČKE OBRANE U NATO–u

## 4.1 Kibernetička obrana u NATO–u

Hladni rat je obilježen pretežito konvencionalnim ratovanjem, a kasnije dolazi do nadogradnje u novoj dimenziji ratovanja koja se odvija u kibernetičkom prostoru. Kao što u vojnim strategijama konvencionalnog ratovanja nailazimo na strategije utemeljene na ofenzivnom djelovanju i defenzivnom djelovanju; tako i u kibernetičkom prostoru nailazimo na strategije utemeljene na istim načelima.

Kibernetičko ratovanje koristi strategiju detektiranja, ometanja i zbunjivanja protivnika. Njome se smanjuje protivnikova sposobnost za napad prikrivanjem, odnosno uklapanjem u informacijski sustav kako bi se postigao efekt prerušavanja u prijateljske snage i omogućio učinkovit napad. Da bi se razumjelo djelovanje u kibernetičkom prostoru, bitno je razlikovati OCO[30] domenu i DCO[31] domenu. OCO domena se odnosi na ofenzivne operacije u kibernetičkom prostoru i temelji se na korištenju mjerila za eksploataciju mrežnoga prostora. DCO domena se odnosi na obranu kibernetičkog prostora i posjeduje preventivni karakter koji koristi intruzivne mjere u borbi protiv neprijateljskih snaga koje štite od samoga upada u kibernetički prostor (Hammock, 2017:80). Primjer djelovanja u kibernetičkom prostoru su NATO–ove vježbe u Poljskoj. U Poljskoj godine 2016., po prvi puta se održavaju operacije u kibernetičkom prostoru u sklopu vojne vježbe ANAKONDA–16 u kojoj se detektiraju vjerodajnice na internetskim stranicama koje su identične operativnim stranicama AN–16, te se time omogućuje učinkovito prepoznavanje protivnika prerušenog u domicilnu stranicu i prevenira njegov upad u sistem (Hammock, 2017:81). Za vježbe je uspostavljen MRT, odnosno

[30] ofenzivne operacije u kibernetičkom prostoru (offensive cyberspace operations)
[31] defenzivne operacije u kibernetičkom prostoru (defensive cyberspace operations)

Multinacionalni crveni tim, a sačinjavali su ga latvijski, američki, poljski, estonski i španjolski vojnici specijalizirani u kibernetičkoj obrani koji su oponašali ruske organizacije kao kibernetičke napadače za testiranje sustava obrane pomoću UNIX Operativnog Sistema (Hammock, 2017:81). Pošto se uspješnost kibernetičkih vježbi temelji na uočavanju potencijalnih prijetnji i njihovom uvrštavanju u kibernetičke sisteme, može se reći da je ključni čimbenik u kibernetičkoj nadogradnji upravo ljudska spoznaja, koja s napretkom tehnologije prelazi u automatizam kojim sistemi na osnovu algoritama sami identificiraju nedostatke i potencijalna rješenja za nastale probleme.

Treba napomenuti da se u kibernetičkom prostoru gubi klasično državno–centrični pogled jer je teško identificirati izvršitelja napada koji ne mora biti država već može biti i određena organizacija ili pojedinac, što otežava pripisivanje krivnje za izvršeni napad, odnosno napad se odvija neovisno o kontroli granica (Hammock, 2017:80). Ne postoji suverenitet nad internetskim prostorom, kao što postoji suverenitet države nad određenim teritorijem. Također, u posthladnoratovskom razdoblju dolazi do suvremenih izazova koji uključuju postupak deteritorijalizacije s kojime se NATO mora suočiti (Yost, 2010:490). Karakteristika kibernetičkog prostora u kojemu ne postoje granice nacionalnoga tipa, otežava pripisivanje krivnje za kibernetički napad. Stoga se zajednički vojni napad koji je propisan člankom 5 Sjevernoatlantskog saveza ne može aktivirati na temelju neidentificiranog izvršitelja napada. Prema NATO–u kolektivna obrana ne uključuje samo pozivanje na vojne snage u slučaju agresije, već i pružanje pomoći. Članak 5 Sjevernoatlantskog saveza je pokrenut samo jednom tijekom terorističkih napada u SAD–u 2001. godine (Ccdcoe.org, 2022). Što se tiče kibernetičkih napada, iako su 2014. godine prepoznati kao potencijalni pokretači kolektivnog odgovora propisanog člankom 5 Sjevernoatlantskog saveza, ni jedan nije rezultirao pokretanjem kolektivnog odgovora primjenom konvencionalnih oružja do danas (Ccdcoe.org, 2022). Nije propisano koji intenzitet štete uzrokovan kibernetičkim napadima bi bio dovoljan za pokretanje kolektivnog odgovora. Proklamirano je da bi kibernetički napadi intenziteta onih koji su se dogodili u Estoniji 2007. godine, mogli potencijalno dovesti do zazivanja kolektivnog odgovora (Ccdcoe.org, 2022). Pošto je ranije naznačeno da kolektivni odgovor ne podrazumijeva samo napad vojnih snaga, već i pružanje pomoći i solidarnost, nije jasno je li se zazivanje na kolektivni odgovor u slučaju sličnoga napada kao napada na Estoniju odnosi na spremnost upotrebe konvencionalnog naoružanja.

## 4.2 **Razvoj promjene kibernetičke obrane od 1999. do 2006. godine**

Uvod u kibernetički svjestan NATO je označen donošenjem Strateškog koncepta Saveza iz 1999. godine. Ključne promjene u razdoblju od 1999. do 2006. godine u NATO kibernetičkoj obrani su potaknute konfliktom u Kosovu, odnosno 'Prvim web ratom' tijekom operacije Allied Force u kojemu su se srpski, ali i ruski hakeri infiltrirali u komunikacijsku infrastrukturu NATO–a uskraćujući DDoS usluge[32] kao odgovor na NATO–ovu umiješanost u rat na Kosovu. Kao rezultat tog incidenta i događanja jedanaestoga rujna 2001. godine u SAD–u na inicijativu američkog predsjednika Busha dolazi do izgradnje institucionalnih kapaciteta kibernetičke obrane NATO–a formiranjem NCIRC–a. U Pragu se 2002. godine održava summit, na osnovi kojega dolazi do formacije NCSA[33] 2004. godine. Kibernetički napadi kao prijetnja se po prvi put spominju u Deklaraciji iz 2002.[34] godine sa summita u Pragu (Mad'ar, 2019:9). Napadi na informacijske infrastrukture NATO–a, otkrili su ranjivost kibernetičkih sigurnosnih kapaciteta organizacije što je dovelo do promjena istih; što potvrđuje hipotezu broj dva koja navodi da sigurnosne prijetnje kao rezultat potiču stvaranje kibernetičkih sposobnosti NATO–a. Nakon sigurnosne prijetnje dolazi do donošenja političkih odluka u Pragu što slijedi hipotezu broj jedan koja navodi da političke implementacije imaju direktan učinak na brzinu razvoja kibernetičkih sposobnosti u NATO–u. Summit u Pragu je doprinio razvoju kibernetičke sigurnosti u NATO–u stvaranjem ACT[35]–a (Savezničkog zapovjedništva za transformaciju) i stvaranjem ACO[36]–a (Savezničkog zapovjedništva za operacije) koji se nalazi u Belgiji (Efthymiopoulos, 2009:63). Jedna od odluka donesenih u Pragu je i uspostava NCIRC–a, odnosno sposobnosti za tehničku i zakonodavnu podršku za 24–satnu kibernetičku obranu i podršku kao odgovor na kibernetičke prijetnje (Mad'ar, 2019:9). No, političku odluku iz Praga ne treba precijeniti, pošto je

[32] Napad distribuiranim onemogućivanjem pružanja usluge (DDoS) označava napad u kojemu dolazi do ometanja mrežnih stranica zbog preplavljivanja mreže prometom; to znači da dolazi do izbacivanja ciljanih korisnika iz mreže kao rezultat pretrpanosti prometa zbog napada na računalo. To može rezultirati izbacivanjem s mreže ili lošom funkcionalnošću web mjesta.

[33] NATO Agencija za usluge komunikacijskih i informacijskih sustava - NCSA (NATO Communication and Information Systems Services Agency) je bila pružatelj usluga svojim NATO i nacionalnim klijentima. Gdje god je NATO bio raspoređen u operacijama ili vježbama, NCSA je pružala usluge komunikacijskih i informacijskih sustava (CIS) kao potporu misiji. Godine 2012. NCSA se ukorporirala u novostvorenu agenciju NCIA.

[34] NATO Prague Summit Declaration

[35] Allied Command Transformation (Savezničko zapovjedništvo za transformaciju) vodi vojnu prilagodbu Saveza, koordinira nacionalne pothvate kako bi se osigurala koherentnost i osigurala interoperabilnost. Njegovo sjedište se nalazi u Norfolku u Virginiji.

[36] Savezničkog zapovjedništva za operacije (Allied Command Operations) odgovoran je za planiranje i izvođenje svih vojnih operacija NATO-a.

kibernetička obrana spomenuta samo u članku 4f kao precizno izražena odluka o jačanju sposobnosti za obranu od kibernetičkih napada (Mad'ar, 2019:9).

Godine 1999. osim incidenta hakiranja NATO mreže od strane srpskih i ruskih hakera, kibernetičkim napadima se pridružuju kineski hakeri zbog greškom bombardiranog kineskog veleposlanstva u Beogradu (Mad'ar, 2019:9). Napadi su rezultirali obaranjem servera i web stranica kojima upravlja Savez (Mad'ar, 2019:9). Strateški koncept iz 1999. godine je potaknuo razvoj kibernetičke obrane, ali i šire sigurnosne obrane u NATO–u zbog svoga značaja u određenju fundamentalnih sigurnosnih zadataka.

Pet sigurnosnih zadataka su spomenuti u Strateškom konceptu; 1. Osiguravanje sigurnosti koja je temeljena na demokratskim institucijama i stabilnosti okruženja, 2. Konzultacije kao forum za razgovor o vitalnim interesima i mogućim rizicima, 3. Odvraćanje i obrana od agresije propisana člancima 5 i 6 Washingtonskog ugovora, 4. Upravljanje kriznim situacijama u skladu sa člankom 7 ugovora, uključujući operacije odgovora na krizne situacije i 5. Partnerstvo s ciljem povećanja povjerenja, te povećanja zajedničkog i transparentnog djelovanja (Yost, 2010:491). Godine 2003. dolazi do potpisivanja sporazuma o razmjeni informacija o kibernetičkoj sigurnosti. Ugovor potpisuje devet članica Saveza (Velika Britanija, SAD, Kanada, Francuska, Njemačka, Italija, Norveška i Nizozemska). Nedugo nakon potpisivanja sporazuma, 2004. godine dolazi do uspostavljanja NCSA, donosno agencije koja pruža informacijske i komunikacijske usluge kao podršku u NATO–vim misijama (NCIA, 2020). Godine 2006. se održava summit u Rigi na kojemu se ponovno naglašava važnost razvoja kibernetičke obrane i brzine razmjene podataka, kao i važnost prilagodbe NATO–ove mreže novim sigurnosnim prijetnjama (Mad'ar, 2019:12).

### 4.3 **Ključne promjene kibernetičke obrane 2007. i 2008. godine**

Kibernetički napadi izvedeni u Estoniji 2007. godine rezultirali su odobrenjem prve politike NATO–a o kibernetičkoj obrani, premještanju fokusa počinitelja kibernetičkih napada i uspostavljanju CDMA, ICTM[37]–a i CCD COE–a. Godine 2008. u Tallinn–u dolazi do uspostavljanja NATO–vog CCD COE–a, koji iako nije dio formalne zapovjedne strukture,

[37] NATO–vo tijelo za upravljanje informacijskim komunikacijama i tehnologijom (Information Communications and Technology Management-ICTM) pruža podršku i usluge u područjima upravljanja informacijskim komunikacijama i tehnologijom i upravljanja arhivima i informacijama.

preuzima ulogu u poboljšanju doktrine kibernetičke sigurnosti i razvoju sposobnosti kibernetičke sigurnosti (Burton, 2015:307). Kroz inicijativu 'Pametna obrana' smanjuje transakcijske troškove, a Savez stvara resurse koji djeluju kao stabilizatori organizacije čak i kada se sigurnosno okruženje mijenja (Burton, 2015:307). Nakon napada u Estoniji 2007., u siječnju 2008. godine dolazi i do odobrenja prve politike NATO–a o kibernetičkoj obrani, što zajedno sa summitom u Bukureštu 2008. predstavlja stvarni temelj političkog pristupa kibernetičkoj obrani u Savezu (Mad'ar, 2019:13). Iako je NATO imao osam godina da se pripremi, nije uspio spriječiti napade na estonske javne i privatne institucije, te je zbog toga u Bukureštu naglašena potreba zaštite kibernetičkih sustava i potreba za sposobnostima pomoći savezničkim državama (Hasanov, Iskandarov, Sadiyev, 2019:96). Do napada u Estoniji dolazi nakon premještanja memoriala 'Bronze Soldier' od glavnog grada Estonije do vojnog groblja; što rezultira dvadesetdvodnevnim napadima na web stranice banki i političkih institucija (Joubert, 2012:1). Premještanju memorijala se protivila Rusija, koja je zbog političkih implikacija započela kibernetičke napade. Najbrojniji napadi su bili DDoS napadi koji su uzrokovali milijune zahtjeva za informacijama koje su preplavile mrežni promet što je dovelo do zastoja u radu servera (Joubert, 2012:1). Takvi napadi mogu uzrokovati veliku štetu za stabilnost funkcioniranja mnogih sektora unutar države bitnih za cjelokupnu nacionalnu sigurnost, zavisno o ovisnosti društva o informacijskim strukturama. Estonija, iako ne raspolaže pretjeranim teritorijalnim kapacitetima, uvelike ovisi o internetu. Estonija sve aktivnosti bitne za svakodnevno funkcioniranje, od održavanja izbora, obrazovanja, upravljanja bankovnim transakcijama i slično obavlja putem interneta, stoga je vrlo osjetljiva na kibernetičke napade koji su u mogućnosti paralizirati svakodnevne radnje (Joubert, 2012:1). Učinak napada na funkcioniranje države ovisi o destrukcijskoj razini napada. Napadi u Estoniji nisu uzrokovali previše štete jer nisu bili dovoljno sofisticirani, te su kibernetički stručnjaci brzo reagirali i uspješno koordinirali svoje aktivnosti, čemu je u prilog išao mali teritorij države (Joubert, 2012:1). NATO je uočio da države koje uvelike ovise o IT infrastrukturama mogu kibernetičkim napadima biti onemogućene u izvršavanju vitalnih zadaća. Unatoč uočenim prijetnjama, kibernetičke prijetnje su u Deklaraciji nedovoljno spominjane, sugerirajući da tema još nije postala glavnim prioritetom Saveza (Mad'ar, 2019:13). U skladu s člankom četiri Washingtonskog ugovora NATO se obvezao u pružanju pomoći, preporuka i jačanju koordinacije NATO–a i nacionalnih vlasti. Kao rezultat, stvoreno je Upravno tijelo za kibernetičku obranu, kasnije zamijenjenog CDMB–om (Mad'ar,

2019:13). CDMB kontrolira CDMA–om koji je uspostavljen 2008. godine od strane NAC–a. Godinu dana ranije je uspostavljen ICTM za sjedište NATO–vog zapovjedništva (NCIA, 2020). Deklaracijom u Bukureštu NATO je podržao zahtjeve za Akcijski plan za članstvo Ukrajine i Gruzije, što je uzrokovalo rusku kampanju napada u kibernetičkom prostoru. Takve okolnosti su zajedno s zamrznutim sukobom s Abhazijom i Južnom Osetijom usporile postupak članstva Ukrajine i Gruzije u NATO (Mad'ar, 2019:13). Godine 2008. na summitu u Bukureštu NATO potiče pridruživanje Ukrajine i Gruzije Savezu, što je jedan od razloga za rusko – gruzijski rat koji uključuje kibernetičku komponentu; i hibridne ratove u Ukrajini, što će detaljnije biti opisano u sljedećem poglavlju.

## 4.4 **Ključne promjene kibernetičke obrane od 2008. do 2010. godine**

Devedesetih godina 20. stoljeća dolazi do sukoba u Gruziji koji rezultira građanskim ratom. Dolazi do stvaranja Južne Osetije i Abhazije. Ruska Federacija se miješa u sukob jer smatra da su povrijeđena prava njezinih građana, te se Gruzija zbog straha od ruskog napada povlači. Godine 2002. dolazi do prelaska Čečena preko Gruzije na ruski teritorij. Ponovno se pojavljuju tenzije između Rusije i Gruzije, koje se kasnije pojačavaju odobrenjem Gruzije za prisustvo NATO–ovih zrakoplova za elektronsko djelovanje AWACS na gruzijskom teritoriju (Ogorec, 2009:14). Gruzija (uz pomoć SAD–a) promiče zatvaranje ruskih vojnih baza na teritoriju Gruzije. Godine 2008. Gruzija napada Južnu Osetiju: u sklopu napada također dolazi do okršaja s ruskim postrojbama. Ruske snage uz opravdanje da žele zaštititi Južnu Osetiju, napadaju Gruziju. U sklopu napada 2008. godine, osim konvencionalnog oružja, koriste se i kibernetički napadi. Kibernetički napadi od strane ruskih hakera su u funkciji množitelja snage i zbunjivanja gruzijskih vojnih jedinica i vladinih ministarstava 2008. godine, uspješno spriječili koordiniran odgovor na sigurnosnu prijetnju. Kibernetički napad nije uzrokovao znatnu štetu Gruziji. Gruzija nije članica NATO–a, te joj zbog toga NATO nije pružio izravnu pomoć, ali je poslana skupina stručnjaka na inicijativu estonske vlade što je rezultiralo ubrzanom normalizacijom informacijskih sustava Gruzije (Hasanov, Iskandarov, Sadiyev, 2019:96). Zbog rusko–gruzijskog rata i Stuxnet virusa[38] dolazi do brojnih političkih promjena, odnosno do kibernetičkih promjena koje su većinom vojne orijentacije. Zbog održavanja sigurnosti informacijskih sustava, Pentagon

[38] Iranski program nuklearnog razvoja je bio pod udarom izraelskog kibernetičkog napada (uz pomoć SAD–a)

je 2008. godine u studenom zabranio upotrebu vanjskih tvrdih diskova nakon što je strana obavještajna agencija na računalima Ministarstava obrane upotrijebila USB za učitavanje softvera za eksfiltraciju podataka (Burton, 2015: 307). Sukob između Rusije i Gruzije pokazao je da su kibernetički napadi potencijalno glavna sastavnica konvencionalnog ratovanja (Hasanov, Iskandarov, Sadiyev, 2019:96). Kibernetički napadi na Gruziju su organizirani i iz drugih država u svijetu, ne samo iz Rusije, a glavna metoda napada je bilo distribuirano uskraćivanje usluga i otkrivanje ranjivosti informacijske infrastrukture gruzijske vlade kao glavne mete (Hasanov, Iskandarov, Sadiyev, 2019:96).

Kao reakcija na rat u Gruziji 2009. godine se u Strasbourg–Kehlu održava summit Saveza. Deklaracija iz Strasbourg–Kehla spominje da kibernetička obrana treba postati dio NATO vježbi. Godine 2010. dolazi do ponovnih kibernetičkih napada od strane Rusije, ovaj puta u Ukrajini. Kampanja ruskog hibridnog ratovanja u Ukrajini je uključivala zlonamjerno preusmjeravanje prometa, DDoS napade, kibernetičku špijunažu, manipulaciju informacijama, propagandu i oštećenje web stranica (Ducaru, 2016:17). Zlonamjerni softver korišten u Ukrajini, poznat pod imenom 'Snake' je alat korišten za špijunažu računalnih sustava vlade (Ducaru, 2016:17). Kibernetički napadi su se događali istovremeno s vojnim i političkim akcijama vezanim za krizu na Krimu (Ducaru, 2016:17). Valja uočiti da se kibernetički napadi dešavaju simultano s političkim i vojnim akcijama. Kao reakcija na kibernetičke napade i osvještavanje da država može biti napadnuta i izvan tradicionalnih okvira; zemlje, zraka, vode i svemira, u Lisabonu se 2010. godine održava summit. Najvažniji rezultat summita je donošenje novog Strateškog koncepta. Izmjene u Strateškom konceptu, između ostaloga, uključuju i preformulaciju stupnja informacijske obrane sustava i vojne komunikacije (Kovács, 2018:21). Kao rezultat summita, Strateški koncept je uključio zaštitu informacijskih i komunikacijskih sistema kao značajan zadatak zbog sve sofisticiranije prirode kibernetičkih napada (Kovács, 2018:21). Kao nastavak pitanja kibernetičke sigurnosti dolazi do revidiranja Politike kibernetičke obrane NATO-a od strane ministra obrane u lipnju 2011. godine, što se obrađuje u sljedećem poglavlju.

### 4.5 **Ključne promjene kibernetičke obrane od 2011. do 2013. godine**

Zbog nedovoljne informacijske koordinacije između članica Saveza, dolazi do potrebe usvajanja revidirane politike kibernetičke obrane. Dana 8. lipnja 2011. godine novousvojena politika za izgradnju otpornosti informacijskih sustava i sprječavanje kibernetičkih napada rezultira

stvaranjem tima za brzo reagiranje na kiberincidente[39](Hasanov, Iskandarov, Sadiyev, 2019:97). Tim za brzo reagiranje je uspostavljen 2012. godine i reagira na kibernetičke napade dok su u tijeku. Rad na konceptu tima za brzo reagiranje je već započet 2011. godine, a koncipiran je tako da su stručnjaci za kibernetičku obranu adekvatno raspoređeni u slučaju da se dogodi kibernetički napad od nacionalnog značaja (Ccdcoe.org, 2014). Međutim, izostala je jednoglasna podrška unutar NATO–a, stoga je napredak u tom trenutku izostao. U usporedbi s tradicionalnim sredstvima ratovanja, u kibernetičkom prostoru timu za brzu reakciju treba vrijeme da istraži informacijske sustave što otežava ubrzano reagiranje na napad u tijeku, što je i sama bit tima za brzo reagiranje (Ccdcoe.org, 2014). Jedno od rješenja je predviđanje uloge posrednika koordinatora NATO–a kako bi saveznici pružali potporu jedni drugima, umjesto da on služi kao pružatelj izravne pomoći, kako tijekom napada, tako i tijekom preventivnih priprema od napada (Ccdcoe.org, 2014). Pravovremeno reagiranje koje se postiže većom razinom pripravnosti, znatno smanjuje rizik od napada. Rad u kibernetičkom prostoru u određenoj mjeri i dalje izaziva konvencionalni obrazac strateškog razmišljanja, a ključni faktor u suzbijanju kibernetičkih prijetnji je poznavanje sposobnosti i vještina drugih država do kojih se većinom dolazi bilateralnim dijeljenjem informacija između država koje djeluju na temelju povjerenja, a ne putem posrednika (Ccdcoe.org, 2014). Do pozamašnih problema dolazi kad nacije koje su otkrile ograničenja nacionalnih sposobnosti, a raspolažu razvijenim kibernetičkim sposobnostima, nisu voljne dijeliti korisne informacije s NATO–om. Kada je 2012. godine napokon došlo do uspostave tima za brzo reagiranje, tim od šest stručnjaka je angažiran u odgovaranju na napade, ponovnom uspostavljanju funkcionalnosti mreže ili odgovaranju u slučaju eksploatacije mreže (Burton, 2015:308).

Novi pristup kibernetičkoj obrani se temeljio na; shvaćanju da je kibernetička obrana ključna za upravljanje krizama i ključna u kolektivnoj obrani, zatim na pretpostavci da je prevencija, otpornost i obrana kibernetičke imovine od vitalnog interesa za Savez i da mora doći do centralizacije zaštite NATO–vih mreža i naprednijih kibernetičkih sposobnosti (Hasanov, Iskandarov, Sadiyev, 2019:97). Za učinkovitiju politiku, potrebno je uspostaviti mjerila i minimalne zahtjeve kibernetičke sigurnosti. Nova politika se temeljila i na zahtjevu za definiranjem minimalnih kriterija za kibernetičku obranu nacionalnih mreža koje su presudne u

[39] NATO's cyber Rapid Reaction Team (RRT): stručnjaci za kibernetičku obranu odgovorni su za pomoć državama članicama koje zatraže pomoć u slučaju napada od nacionalnog značaja.

temeljnim zadaćama Saveza, te na pomoći saveznicima u postizanju smanjene razine ranjivosti kritične infrastrukture, kao i kooperaciji s drugim međunarodnim organizacijama (Hasanov, Iskandarov, Sadiyev, 2019:97). Nedugo nakon usvajanja Akcijskog plana 2011. godine, 2012. godine je započeta uspostava ćelije za procjenu kibernetičke prijetnje NATO–a (Kovács, 2018:22). Politika kibernetičke obrane iz 2011. godine je naglašavala potrebu ispunjavanja minimalnih zahtjeva za kibernetičku obranu nacionalnih mreža i potrebu da s NAC–om kao krajnjim pokretačem politike u području kibernetičke obrane, stvori integriran sustav kibernetičkog upravljanja unutar Saveza (Burton, 2015: 307).

Nadalje, dolazi do održavanja summita Saveza u Chichagu godine 2012. gdje je uočeno da postoji diskrepancija u koordinaciji NATO–a u kibernetičkom prostoru, stoga je godine 2013. pokrenut projekt razvoja multinacionalne kibernetičke obrane od strane Nizozemske, Danske, Kanade, Norveške i Rumunjske (Hasanov, Iskandarov, Sadiyev, 2019:98). Međutim, zbog nedovoljne podrške projektu koja je bila pružena od strane maloprije spomenutih pet članica NATO–a, projekt je bio neučinkovit. Godine 2012., održana je i 'Smart Defence i budućnost NATO–a': konferencija koja je trajala dva i pol dana. Od ukupno 143 projekta koja su rezultat Smart Defence–a, tri su uključivale kibernetičku obranu. Prvi projekt, MNCD2[40] za cilj postavlja bolje sposobnosti otkrivanja zlonamjernih aktivnosti, dijeljenje osjetljivih informacija i poboljšanje svijesti o situaciji, dok drugi projekt u obliku platforme za dijeljenje informacija o zlonamjernim softverima olakšava dijeljenje i razmjenu tehničkih informacija unutar pouzdane zajednice bez potrebe za dijeljenjem pojedinosti o napadu (Pernik, 2011:7). Treći projekt (Transatlantska obrambena tehnološka i industrijska suradnja[41]) je projekt koji nastoji stvoriti ili unaprijediti partnerstvo s industrijom (Pernik, 2011:7). Godine 2012. također dolazi do uspostave NCIA, agencije koja nastaje kao sinteza NCSA–a, NC3A–a[42], NACMA–a[43], ICTM–a i ALTBMD–a[44] (NCIA, 2020). Što se tiče daljnjih političkih odluka koje su doprinijele

[40] Multinacionalni projekt razvoja sposobnosti kibernetičke obrane (Multinational Cyber Defence Capability Development Project)
[41] Transatlantic Defence Technological and Industrial Cooperation
[42] NATO agencija za konzultacije, zapovijedanje i kontrolu (NATO Consultation, Command and Control Agency – NC3A) je agencija osnovana sa zadatakom središnjeg planiranja, integracija sistema, sistem inženjeringa i tehničke podrške za C3 sisteme.
[43] NATO Agencija za upravljanje sustavom zračnog zapovijedanja i kontrole (NATO Air Command and Control System Management Agency) je bila je odgovorna za upravljanje programom NATO-ovog sustava za zračno zapovijedanje i kontrolu (ACCS).
[44] ALTBMD (Programme Office for NATO's Active Layered Theatre Ballistic Missile Defence) je program koji je dizajniran za zaštitu trupa od balističkih prijetnji dometa do 3000 km.

kibernetičkom razvoju u NATO–u, posebno se ističe dokument iz 2013. godine: Priručnik iz Tallinn–a o međunarodnom pravu primjenjivom na kibernetičko ratovanje[45]. Objavljen u ožujku, taj dokument je rezultat rada pravnih i tehničkih stručnjaka koji surađujući zajedno s CCDCOE–om nastoje razjasniti i kodificirati sve moguće odgovore na pravne i strateške dileme koje se tiču kibernetičkih napada, uzimajući u obzir primjenu već postojećeg međunarodnog prava u domeni kibernetičke sigurnosti (Burton, 2015:308). Dokument je unaprijedio NATO–vo pravno i strateško razmišljanje o ključnim pitanjima kibernetičke sigurnosti, uključujući problem pripisivanja, gdje se tvrdi da bi države trebale snositi dio odgovornosti za kibernetičke napade koji proizlaze iz njihove jurisdikcije (Burton, 2015:308). Suradnja stručnjaka iz tehničkih i pravnih područja unijela je određenu razinu fleksibilnosti u razmišljanju o kibernetičkoj obrani, ali i unaprijedila pitanje pripisivanja odgovornosti, za koju se tvrdi da odgovornost država proizlazi iz njihove jurisdikcije, te stoga dio odgovornost za kibernetičke napade moraju snositi države. Kao sljedeći korak u razvoju kibernetičke obrane je usvajanje poboljšane politike 2014. godine u Walesu koja utvrđuje da je jedna od središnjih zadaća NATO–ve kolektivne obrane upravo kibernetička obrana, što će biti obrađeno u sljedećem poglavlju.

### 4.6 **Ključne promjene kibernetičke obrane 2014. i 2015. godine**

Kriza u Ukrajini 2014. godine, ponovno je ponukala raspravu o ruskim hakerima i o potencijalnim kibernetičkim implikacijama ruskog djelovanja na ovom području za NATO savez. Pošto su se kibernetički napadi na NATO događali za vrijeme napetosti u Ukrajini, ponovno možemo uočiti da se kibernetički napadi događaju istovremeno s političkim, ali i vojnim događanjima. Simultano odvijanje se uočava u kampanji proruskih hakera još od Estonije zbog političkih implikacija, i nanovo u Ukrajini 2014., ali i 2022. godine. Tijekom ukrajinske krize izveden je niz DDoS napada, navodno od strane moderno organizirane skupine proruskih haktivista pod nazivom Cyber Berkut (Jensen, Maness i Valeriano 2019:13).

Otkako je Rusija okupirala Krim, na Ukrajinu je izvedeno više od 2000 kibernetičkih napada, a poremećaji su se odrazili i na mrežne rezervacije za transportne linije, u sustavu glasovanja i u obliku uništavanja poreznih i financijskih računovodstvenih podataka putem softvera NotPetya (Shea, 2017:19). Te sigurnosne prijetnje su dovele do promjena u članku 5 kolektivne obrane

[45] The Tallinn Manual on the International Law Applicable to Cyber Warfare: je neobvezujuća studija koja identificira načela međunarodnog prava primjenjivana na kibernetičko ratovanje. Nabraja 25 pravila koja reguliraju kibernetičke sukobe.

NATO–a. Kao rezultat NATO summita u Walesu, kibernetička obrana je postala dio središnje zadaće kolektivne obrane, što znači da u slučaju kibernetičkog napada, NATO je spreman odgovoriti konvencionalnim oružjem, što implicira da je internet prepoznato kao novo bojno polje (Hasanov, Iskandarov, Sadiyev, 2019:98). Prema članku 5 Sjevernoatlantskog ugovora, kibernetički napad može potaknuti kolektivni odgovor (Burton, 2015:297). Kada se radi o kibernetičkom ratovanju, članak 5 Sjevernoatlantskog ugovora je nedorečen jer ne nudi jasne kriterije koji bi u slučaju kibernetičkog napada izazvali kinetički odgovor u stvarnome prostoru. Odgovor na kibernetičke napade se odražava na geopolitičkom planu, što možemo vidjeti iz ukrajinskog odgovora na kibernetičke napade. Ukrajinska reakcija na kibernetičke napade primjer je mijenjanja politike i donošenja strateških političkih odluka, koje su u ovom slučaju dovele do daljeg približavanja Kijeva Zapadu, što je Rusija htjela spriječiti. Zbog kibernetičkih napada na ukrajinsku mrežu, predsjedničkim dekretom 744/2014 na snagu stupa odluka Vijeća za nacionalnu sigurnost i obranu donesena 28.8.2014. (odluka stupa na snagu 24.9.2014. godine) koja ističe poduzimanje hitnih koraka za unaprjeđenje obrambene sposobnosti Ukrajine, i da je prioritetni nacionalni interes ukrajinske vanjske politike uspostavljanje partnerstva s NATO–om, SAD–om i Europskom unijom (Cherneha, Marchenkov i Shypovsky, 2020:14). Nakon usvajanja dekreta broj 287/2015 donesenog odlukom Vijeća za nacionalnu sigurnost i obranu Ukrajine, donesena je odluka uspostavljanja uvjeta za ukrajinsko članstvo u Savezu (Cherneha, Marchenkov i Shypovsky, 2020:14). Kao odgovor na kibernetičke napade, osnovan je Nacionalni centar za kibernetičku sigurnost u Ukrajini 1.7.2015. godine koji podržava CERT–UA[46] i koji surađuje s NATO–om (Cherneha, Marchenkov i Shypovsky, 2020:14). Novostvoreni centar služi kao koordinator; jedinica lokalne samouprave, organizacija, vojnih agencija, državnih uprava i poduzeća za otklanjanje kibernetičkih prijetnji, kao i način za jačanje suradnje s NATO–om i poboljšanje ukrajinske sigurnosne infrastrukture (Cherneha, Marchenkov i Shypovsky, 2020:14). Ta odluka je podržana dekretom broj 96/16 koji je usvojen 15.1.2016. godine (Cherneha, Marchenkov i Shypovsky, 2020:14).

NATO Politika o kibernetičkoj obrani iz 2014. vrijedi za 'čiste' kibernetičke napade, ali i kibernetičke napade kao dio hibridnog ratovanja (Ducar 2016: 21 – 22). Uz to CIICS, razvijen od strane Nizozemske, Norveške, Rumunjske, Kanade i Danske, unaprjeđuje NATO–ove ‘Cyber

[46]Ukrajinski tim za odgovor na računalne hitne slučajeve (Computer Emergency Response Team of Ukraine) je strukturna jedinica Državnog centra za kibernetičku sigurnost i Državne službe za posebne komunikacije i zaštitu informacija Ukrajine.

Coalition' vježbe održane 2014. godine (Pernik, 2011:7). Politika iz 2014. godine se ne aktivira kao reakcija na svaki kibernetički napad. NATO je u Cardiff–u izjavio da će pozivanje na kibernetički napad određen člankom 5 ovisiti od 'slučaja do slučaja', odnosno pozivanje je ovisno o zasebnom kibernetičkom napadu, no međutim u Deklaraciji summita u Walesu je pojašnjeno da se svaka vrsta kibernetičkog napada smatra vrstom agresije (Limnéll i Salonius-Pasternak, 2016:2). To podrazumijeva mogućnost članicama da odgovore na kibernetičke prijetnje korištenjem sile kako bi se postigla sigurnost. Kao posljedica deklaracije se još navodi potreba za razvijanjem zasebne kibernetičke doktrine i njezina integracija u strateške dokumente i cjelokupno planiranje (Limnéll i Salonius-Pasternak, 2016:2). To dovodi do realizacije da je kibernetička domena, smatrana više binarnom domenom, u konačnici politička, a to dovodi do stvaranja koncepta kiberpolitike[47]. S nastankom kibernetičkog prostora, nastaje i novi prostor za vođenje politike, a anonimnost i sveprisutnost kiberprostora dovode u pitanje tradicionalne koncepte diplomacije, odvraćanja i nacionalne sigurnosti u međunarodnim odnosima (Limnéll i Salonius-Pasternak, 2016:2). Zatim, napadi na kompaniju Sony Pictures 2014. godine dodatno zahvaćaju pozornost NATO–a na kibernetičku sigurnost i izazivaju sankcije protiv sjevernokorejskih dužnosnika (Burton, 2015:298). Činjenica je da su kao odgovor na političke sporove, ruski i kineski hakeri redovito napadali NATO–ve mreže s ciljem istjerivanja vitalnih, pa i povjerljivih informacija. Postojali su pokušaji poboljšanja suradnje s Rusijom u sferi kibernetičke sigurnosti, kao što je dijalog na razini Vijeća NATO–Rusija, no kriza u Ukrajini je poremetila znatniji napredak u toj sferi (Burton, 2015:310).

### 4.7 **Ključne promjene kibernetičke obrane od 2015. do 2017. godine**

Do ponovnog sukobljavanja Rusije s Ukrajinom dolazi u prosincu 2015. godine, kada zbog napada na ukrajinsku elektrodistribucijsku mrežu 230. 000 stanovnika ostaje bez struje do 6 sati. Taj incident potvrđuje rastuću prijetnju ruskih kibernetičkih napada europskoj sigurnosti i potrebu za novim pristupom konceptu sukoba koji kibernetičku i kinetičku prijetnju čini neodvojivima (Cilluffo, Evans, Ilves i Nadeau 2016:128). Važno je napomenuti da Sjeverna Koreja, Iran i Kina također imaju kapacitete i namjeru ugroziti sigurnost NATO–a i Europske unije putem kibernetičkih sredstava (Cilluffo, Evans, Ilves i Nadeau, 2016:128). Zbog toga se

[47] Kiberpolitika je područje istraživanja uloge novih informacijskih tehnologija u suvremenom političkom životu.

2015. godine razvija  Memorandum o razumijevanju o kibernetičkoj obrani.

Zbog sigurnosnih prijetnji, 8.–9.–og srpnja 2016. godine se održava NATO summit u Varšavi. Sastanak u Varšavi je iznimno bitan jer je NATO tada službeno priznao kiberprostor kao operativnu vojnu domenu, odnosno operativno područje ratovanja (uz zemlju, more, zrak i svemirski prostor), te tvrdi da je spreman odgovoriti na kibernetičke napade tradicionalnim oružjem, no izostaju jasni kriteriji prema kojima bi se takav odgovor pokrenuo (Ruiz i Winter, 2017:78). To je promijenilo fokus NATO–a od zaštite informatičkih mreža NATO–a (information assurance) do kibernetičke obrane u okviru vojnih aktivnosti Saveza (mission assurance) (Shea, 2017:20-21). Uloga NATO–a u kibernetičkoj sigurnosti se može podijeliti u dvije komponente; prva je sigurnost informatičkih mreža koja je bila fokus summita u Newportu 2014. godine, a ona uključuje potrebu osiguranja ključnih informacijskih i komunikacijskih sustava za operacije NATO–a u kibernetičkom prostoru (Cherneha, Marchenkov i Shypovsky, 2020:13). Drugi cilj je potpora državama članicama u unaprjeđenju njihovih kibernetičkih sposobnosti što uključuje dvogodišnju metodu definiranja zajedničkih ciljeva kibernetičke sigurnosti i provedbu strategije kibernetičke obrane (Cherneha, Marchenkov i Shypovsky, 2020:13). Još jedan rezultat NATO summita u Varšavi je usvajanje 'Cyber Defence Pledge – a[48]' koji obvezuje saveznike da polože dodatno ulaganje u poboljšanje nacionalne kibernetičke obrane (Shea, 2017:22). Godine 2017. dolazi do ažuriranja Akcijskog plana kibernetičke obrane, kao i plana za implementaciju kibernetičkog prostora kao domene operacija. U lipnju 2017. godine dolazi do kompromisa oko novih ciljeva kibernetičke obrane. Godine 2016. i 2017. su obilježene boljom suradnjom NATO–a i Europske unije u području kibernetičke sigurnosti.

### 4.8 **Ključne promjene kibernetičke obrane od 2018. do 2021. godine**

Posljednje analizirano razdoblje uključuje period od 2018. do 2021. godine. Taj period je obilježen sve češćim kibernetičkim napadima, uključujući učestalije napade na zdravstvene institucije tijekom pandemije COVID–a 19 i istraživačke institute. Ovakva situacija se odražava i na NATO. Godine 2021. dolazi do zlonamjernih kibernetičkih aktivnosti usmjerenih na kritičnu infrastrukturu i usmjerenih na iskorištavanje lanaca opskrbe. NATO se također suočava sa sve

[48] Cyber Defence Pledge (Obveza (zavjet) kibernetičke obrane) je popis izjava o kibernetičkoj sigurnosti s kojima se slažu svi potpisnici.

češćim kibernetičkim napadima. Zbog tih sigurnosnih prijetnji se 2018. godine održava summit u Bruxellesu. U sklopu tog summita, NATO po prvi puta donosi odluku da u okviru snažnoga političkog nadzora upotrijebi niz kibernetičkih sposobnosti u svojim misijama, a to je u suprotnosti s prijašnjim tvrdnjama da Savez reflektira striktno obrambeni stav za kibernetičke operacije (Maďara, 2019:18). Stavak 20 Deklaracije iz Bruxellesa, naglašava potrebu za jačanjem situacijske svijesti predvođene obavještajnim podatcima, uključujući primjenjivost i prikladnost pripisivanja uzroka kibernetičkim napadima i primjenjivost međunarodnog humanitarnog prava i zakona o ljudskim pravima (s upozorenjem) na kibernetički prostor (Maďara, 2019:18). U Bruxellesu su se saveznici složili uspostaviti novi centar za operacije u kibernetičkom prostoru kao dio ojačane zapovjedne strukture Saveza koji će olakšati korištenje kibernetičkih sposobnosti u NATO–vim misijama (NATO, 2021). Donesena je odluka da NATO može koristiti nacionalne kibernetičke sposobnosti za provođenje svojih operacija (NATO, 2021). Do ponovnog dogovora u vezi kibernetičke sigurnosti između saveznika dolazi 2019. godine. Saveznici prihvaćaju vodič koji postavlja niz alata za daljnje jačanje sposobnosti NATO–a da odgovori na kibernetičke prijetnje.

Europska unija i NATO surađuju kroz Tehnički aranžman o kibernetičkoj obrani[49] koji je potpisan 2016. godine, no zbog zajedničkih interesa i izazova jačaju suradnju posebice u područjima istraživanja, vježbi i razmjene informacija (NATO, 2021). NATO intenzivira svoju suradnju s privatnim poslovnim subjektima kroz NATO Industry Cyber Partnership[50]. Saveznici se ponovno sastaju na summitu u Bruxellesu 2021. godine, kada se donosi nova Sveobuhvatna politika kibernetičke obrane koja za cilj ima stvaranje veće otpornosti NATO–a na kibernetičke prijetnje (NATO, 2021). Sveobuhvatna politika kibernetičke obrane[51] utjelovljuje sinergiju obrane, kriznog menadžmenta i kooperativne sigurnosti. Godine 2021. NATO imenuje svoga prvoga glavnog direktora za informiranje (CIO[52]), Manfred Boudreaux-Dehmer–a.

[49] Technical Arrangement on Cyber Defence pruža okvir za razmjenu informacija i razmjenu najboljih praksi između timova za hitne slučajeve

[50] NICP obuhvaća 12 ciljeva koji uključuju: poboljšanje kibernetičku obranu u NATO-ovom obrambenom lancu opskrbe, olakšanje sudjelovanja industrije u multinacionalnim projektima Smart Defence–a i doprinos obuci i vježbama kibernetičke obrane.

[51] Sveobuhvatna politika kibernetičke obrane iz 2021. (Comprehensive Cyber Defence Policy) uključuje priznanje da priroda kibernetičkog prostora zahtijeva sveobuhvatan pristup kroz jedinstvo napora na političkoj, vojnoj i tehničkoj razini. Sveobuhvatna politika kibernetičke obrane i njezin odgovarajući akcijski plan potaknut će aktivnosti na ove tri razine. Prepoznato je da NATO mora aktivno odvraćati, braniti se i suprotstavljati cijelom spektru kibernetičkih prijetnji u svakom trenutku–tijekom mira, krize i sukoba.

[52] Chief Information Officer

Za bolje provođenje Sveobuhvatne politike kibernetičke obrane potrebno je promicanje integracije informacijskih i komunikacijskih tehnologija i usklađivanje s ciljevima NATO–a. NATO se koristi kao platforma za političke konzultacije o kibernetičkim prijetnjama, razmjenu zabrinutosti i nacionalnih pristupa kibernetičkim prijetnjama, kao i platforma za razmatranje potencijalnih kolektivnih odgovora na kibernetičke prijetnje (NATO, 2021). Izgradnjom normi za odgovorno ponašanje u kibernetičkom prostoru, kao i podupiranjem međunarodnog prava, smanjuju se rizici od sukoba i povećava se stabilnost informacijskih struktura, kao i funkcioniranje i stabilnost samih država.

# 5. IZAZOVI RAZVOJA KBERNETIČKE OBRANE I POLITIČKE ODLUKE

## 5.1 **Potencijalni problemi u razvoju kibernetičke obrane**

Dinamičnost promjena koje su nepredvidljive dovode do potrebe za što fleksibilnijom prilagodbom na kibernetičke prijetnje i ugroze. Dolazi do neizvjesnosti, odnosno do poteškoća u predviđanju daljnjega tijeka događanja, što dovodi do nedostatka mogućnosti planiranja i reagiranja na prijetnje. Neizvjesnost, kada se radi o kibernetičkim sukobima, uglavnom proizlazi iz poteškoća u identifikaciji neprijateljskih snaga i odluka koje su donijeli u izvođenju napada. Pripisivanje odgovornosti za napade i regulacija odgovora na iste često izostaje. Prepoznavanje uzroka je otežano. Kompleksnost okolnosti dovodi do poteškoća u određivanju uzroka i posljedica, te je stoga kibernetički prostor okruženje s visokom razinom apstrakcije i dolazi do poteškoća identificiranja događaja i utvrđivanja njihova značenja u kinetičkom (fizičkom) prostoru (Ruiz i Winter, 2017:78). Zbog sve veće količine informacija dolazi do poteškoća filtriranja istih. Mogućnost anonimnog izvođenja napada i njegovih globalnih dosega smanjuju učinkovitost kibernetičke obrane. Nove klase protivnika, asimetrične prijetnje i poteškoće u utvrđivanju proporcionalne prijetnje predstavlja izazov za manevriranje u kibernetičkom prostoru.

Prijetnje, zajednički pristupi interesima koji se tiču kibernetičke sigurnosti približavaju Ameriku i Europu. Obje strane Atlantika zagovaraju otvoreno globalno kibernetičko djelovanje s minimalnim vladinim ograničenjima. Pristupačnost interneta obje strane smatraju ključnim za

gospodarski rast nakon financijske krize 2008. godine, te su također jedinstveni u svom pristupu osiguravanja kritične infrastrukture i borbe protiv kibernetičkog kriminala (Burton, 2015:310). Pristup NATO–a je u suprotnosti ruskog i kineskog pristupa, koji su više zabrinuti s kontroliranjem informacija što se može iščitati iz njihovog zalaganja za ograničavanje i cenzuru internetskog prometa u međunarodnom pravu: što ujedno dovodi i do većega ujedinjena Amerike i Europe oko pristupa informacijama (Burton, 2015:312). Pernik ističe da postoji smanjena volja za razvoj NATO–vih ofenzivnih ili defenzivnih kapaciteta, ponajprije zbog dodatnog opterećenja sve skromnijeg obrambenoga proračuna članica i činjenice da samo tri europske članice NATO–a (Velika Britanija, Grčka i Estonija) ispunjavaju zahtjev razine obrambenih izdataka u iznosu od 2% BNP–a godišnje (Pernik, 2011:9). Prema novijim NATO–vim izvorima, devet članica zadovoljavaju zahtjev od 2%, a glavni tajnik NATO-a Jens Stoltenberg je najavio i povećanje do 19 članica do 2024. godine (NATO, 2022).

Problemi se ne javljaju samo zbog nedovoljnog izdavanja članica za razvoj sposobnosti kibernetičke obrane, nego i zbog neučinkovite koordinacije. Problemi koordinacije se javljaju kada nacije koje razvijaju ozbiljne kibernetičke sposobnosti negiraju dijeliti informacije o tom procesu s NATO–om, što treba imati na umu u svim političkim razmatranjima (Ccdcoe.org, 2014). Još jedna od prepreka je NATO–ov fokus na obrambenoj kibernetičkoj sigurnosti, u odnosu na ofenzivne kibernetičke sposobnosti. Ofenzivne kibernetičke sposobnosti uglavnom ostaju u djelokrugu nacionalnih obavještajnih i sigurnosnih institucija pojedinih članica.

NATO–va kibernetička sigurnosna doktrina usmjerena je na uskraćivanje mogućnosti da protivnička strana postigne svoje ciljeve zbog poteškoća u prisiljavanju od odustajanja od napada i otežanoj mogućnosti odmazde (Burton, 2015:310). Problemi rješavanja izazova koji predstavljaju kočnicu u razvoju kibernetičke sigurnosti su posljedica ograničenih kibernetičkih dostignuća, preklapanja kibernetičkog područja kroz različite domene, odnosno njegova kompleksnost i problem učinkovitosti i zajedničkog usuglašavanja kao odgovora na sigurnosne prijetnje. Dolazi do usporenog odgovora na napade zbog nemogućnosti brzoga otkrivanja prijetnji i zbog asimetrične prirode konflikta. DBIR[53] izvještava da od prikupljenih incidenata koji su se zbili u 91 državi, u 60% slučajeva napadači su uspjeli kompromitirati organizaciju za par minuta, a prosječno vrijeme za otkrivanje zlonamjernog softvera je brojeno u mjesecima

[53] Data Breach Investigations Report, odnosno izvješće od američkog operatera bežične mreže Verizon sa sjedištem u New York–u.

(Ducaru, 2016:7). Zbog učinkovitosti i dostupnosti kibernetičkog oružja, ono postaje sve češće sredstvo kompromitiranja protivničke strane, te se zbog toga treba pratiti njegov razvoj. Treba naglasiti da rekcije na kibernetičke napade, koje se mogu iščitati iz političkih odluka NATO–a, se ne poklapaju u potpunosti s legalnim okvirom, zbog nedovoljne koordinacije, nedostatka prijava prijetnji i drugih faktora (Tikk, 2011:120). Zbog toga treba uzeti u obzir ograničenost istraživanja na osnovu pravnih dokumenata koji su ujedno i najdostupniji izvori.

## 5.2 Politički procesi, politička tijela i njihova relevantnost u razvoju kapaciteta kibernetičke obrane i odgovaranja na sigurnosne prijetnje u NATO–u

Od 2014. godine prema Unaprijeđenoj politici kibernetičke obrane NATO–a, okvir kolektivne obrane uključuje kibernetičku obranu čija je struktura pojednostavljena maloprije spomenutom politikom iste godine (Mad'ar, 2019:8). NATO stvara razvojne politike kroz koje s NCIRC–om poboljšava djelovanje strategija kibernetičke obrane. Tijela koja se koriste za implementaciju i provedbu kibernetičkih politika su CDMB koje je glavno tijelo za nadgledanje aktivnosti kibernetičke obrane, zatim CCD COE koji služi kao centar za istraživanje i edukaciju, koji nije formalno dio NATO–a, ali je u uskoj kooperaciji s organizacijom (Fidler, Pregent i Vandurme, 2013:6). Važnu ulogu imaju i sastanci ministara obrane NATO–a posvećeni kibernetičkoj obrani, kao i vježbe kibernetičke obrane s članicama NATO–a (Fidler, Pregent i Vandurme, 2013:6). Za efektivan razvoj kibernetičke obrane, nije dovoljno samo stvaranje novih tijela za tu svrhu, već i uklapanje kibernetičke obrane u već postojeće političke procese. CDMB, zajedno s DPPC–om[54], nadzire Koncept politika i akcijski plan kibernetičke obrane iz 2011. godine (Fidler, Pregent i Vandurme, 2013:6). U studenom 2003. godine, devet članica NATO–a (Kanada, Francuska, Njemačka, Italija, Nizozemska, Norveška, Španjolska, Velika Britanija i SAD) potpisuju sporazum o razmjeni više informacija o kibernetičkoj sigurnosti (Hasanov, Iskandarov, Sadiyev, 2019:96). Kasnije, iste godine, NATO je odobrio Program kibernetičke obrane i sposobnost odgovora na računalne incidente za sprječavanje, otkrivanje i odgovor na kibernetičke prijetnje (Hasanov, Iskandarov, Sadiyev, 2019:96). Dolazi do učestale revizije dogovorenih ciljeva.

[54] Odbor za obrambenu politiku i planiranje (Defence Policy and Planning Committee)–nadležan je za unaprjeđenje politike obrambenog planiranja i cjelokupnu koordinaciju aktivnosti NDPP-a (NATO Defence Planning Process).

Za postizanje dogovorenih ciljeva, NATO kroz obrazovno–istraživačke institucije poput NATO škole u Oberammergau i Cyber akademiju koja je osnovana u Portugalu, pruža programe obuke (Cherneha, Marchenkov i Shypovsky, 2020:13). Škole u Oberammergau i Oeiras–u pružaju edukaciju u vezi kibernetičke obrane, zajedno s NATO Obrambenim fakultetom u Rimu koji promiče strateško razmišljanje u vezi političko–vojnih predmeta (NATO, 2021a). To je bitno jer hipoteza dva upravo implicira da je prepoznavanje nedostataka kibernetičke obrane podloga za razvoj same obrane, a ukoliko ne dođe do prepoznavanja kibernetičkih prijetnji, ne dolazi ni do strukturalne promjene organizacije kroz političke procese. Prema tome, ne radi se samo o postojanju sigurnosnih prijetnji kao takvih, već i o prepoznavanju njihovog postojanja, u čemu pomažu NATO edukacijske ustanove smještene diljem Europe. Pošto kibernetičke sposobnosti značajno ovise o kapacitetima kibernetičke obrane svake članice, važno je spomenuti Kooperativni centar za izvrsnost kibernetičke obrane koji se nalazi u Estoniji, Tallinn–u. Radna podskupina za kibernetičku obranu osnovana je 2008. godine na inicijativu Službe sigurnosti Ukrajine, a upravo ta podskupina je dala poticaj za uspostavu konceptualnih mehanizama za suradnju između Ukrajine i NATO–a u konzultacijama i razmjeni informacija o kibernetičkoj sigurnosti (Cherneha, Marchenkov i Shypovsky, 2020:13).

Odgovornost implementacije kibernetičke obrane preuzimaju autoriteti na svim razinama Saveza, kao i njegove članice. NAC preuzima najveću odgovornost jer ima glavne ovlasti donošenja odluka u vezi s upravljanjem kibernetičkim krizama i ulogu nadziranja političkih aspekata njezine provedbe (Pernik, 2011:17). NAC osigurava Međunarodnom osoblju i IM–u[55] nadzor na visokoj razini nad provedbom politike, te prima informacije i daje političke smjernice o svakom većem kibernetičkom incidentu (Mad'ar, 2019:8).

Na političkoj razini savjetnika za obranu iz nacionalnih izaslanstava, Odbor za kibernetičku obranu[56] kroz NDPP[57] ocjenjuje procese planiranja kibernetičke obrane te pruža nadzor i savjete NAC–u u vezi kibernetičke obrane (Pernik, 2011:17). Odbor za kibernetičku obranu se sastoji od Međunarodnog osoblja, predstavnika savezničkih zemalja i Međunarodnog vojnog stožera, te on razvija političke smjernice i politiku kibernetičke obrane.

[55] Međunarodni vojni stožer (International Military Staff) je izvršno tijelo Vojnog odbora. IMS se sastoji od osoblja od približno 500 zaposlenika, sastavljenog isključivo od vojnog i civilnog osoblja iz zemalja članica NATO-a. IMS također osigurava da NATO odluke i politike o vojnim pitanjima, provode odgovarajuća vojna tijela NATO-a.
[56] Cyber Defence Committee (CDC), koji je do 2014. postojao kao Odbor za obrambenu politiku i planiranje
[57] NATO proces obrambenog planiranja (NATO Defence Planning Process): kroz njega NATO identificira sposobnosti koje mu trebaju i promiče njihov razvoj i stjecanje od strane saveznika.

Na operativnoj razini, već spomenuti CDMB koordinira političke, tehničke aktivnosti i aktivnosti dijeljenja informacija (Pernik, 2011:17). Većina država članica NATO–a je potpisala memorandume s CDMB–om koji definiraju razmjenu informacija i dogovore o ranom upozoravanju te mehanizme za primanje pomoći. CDMB je glavno savjetodavno tijelo NAC–a; savjetuje države članice o kibernetičkoj obrani i usmjerava i upravlja kibernetičkom obranom u svim civilnim i vojnim tijelima NATO–a (Pernik, 2011:17).

Na tehničkoj razini NCIA zajedno s NMA[58] dijeli odgovornost za provedbu sposobnosti kibernetičke obrane NATO–a. NCIRC vrši nadzor nad NATO mrežama, obrađuje incidente, izvješćuje o incidentima i dijeli informacije o incidentima (Pernik, 2011:17). NCIRC koordinira kibernetičke aktivnosti kako unutar Saveza tako i između Saveza i drugih organizacija. NCIRC je sačinjen od dvije podcjeline; Euroatlantskog centra za koordinaciju[59] i Tehničkog centra koji se nalazi u Monsu: koji pruža tehničke usluge u slučaju kibernetičkog napada na NATO (Pernik, 2011:17). NATO–ov NC3[60] se također bavi implementacijom kibernetičke obrane, on daje tehničke i provedbene smjernice, a planiranje i provođenje NATO kibernetičkih vježbi je pod okriljem ACT–a koje je odgovorno za kontinuiranu prilagodbu NATO–a novim izazovima (Pernik, 2011:17). ACT je također odgovoran za organizaciju vježbe Cyber Coalition (Mad'ar, 2019:8). Za kibernetičku obranu, ali i nacionalnu sigurnost, ključna je brza procjena i donošenje odluka. Za procjenu NATO koristi CDDSS[61], odnosno sistem za podršku kibernetičkoj obrani, kao i informiran i brz proces donošenja odluka u suzbijanju kibernetičkih napada: za koje je ključno učestalo usavršavanje postupaka i sposobnosti kroz obuku i vježbe (Ducaru, 2016:20).

Nakon što NAC donese odluku o kibernetičkoj obrani, njegova se odluka smatra izrazom volje svih država članica budući da se odluke donose konsenzusom. Kako bi se spriječili sukobi, NATO promiče političke ciljeve i izgradnju povjerenja koje se stječe kroz učestale konzultacije. U slučaju da diplomatski napori ne uspiju, NATO provodi upravljanje krizom vojnim sposobnostima koje se organiziraju na temelju članka 5 Washingtonskog ugovora ili pod mandatom UN–a (Mad'ar, 2019:8). Vojne sposobnosti NATO–a se nadograđuju kibernetičkim sposobnostima. Zbog proširivanja sigurnosnih izazova dolazi do inkorporiranja različitih

[58] Vojne vlasti NATO–a (NATO Military Authorities)
[59] Centar za koordinaciju se nalazi u Bruxellesu: on je zaslužan za pripremu procjene prijetnji i vježbe planiranja
[60] NATO Consultation, Control and Command
[61] CDDSS (Cyber Defence Decision Support System) je integrirani sustav za procjenu stanja kibernetičke sigurnosti, analizu i podršku u odlučivanju. Proširuje situacijsku svijest predstavljanjem slike kibernetičke sigurnosti računalnih mreža i pruža podršku donositeljima odluka kroz rezultate analize.

dimenzija vježbi u vojne pripreme NATO–a. Simulacije kibernetičkih napada su uključene u sve vježbe NATO–a, ne samo u kibernetičke vježbe (kao primjer se može navesti godišnja vježba Cyber Coalition) (Ducaru, 2016:20). Za provođenje kibernetičkih vježbi NATO se služi komunikacijskim i informacijskim sustavima, odnosno CIS[62] servisima koji se pružaju putem agencije NCSA. Postupak dobro informiranog procesa donošenja odluka i odgovora na krize su ključni u suzbijanju kibernetičkih napada.

# 6. ZAKLJUČAK

Potencijalni problem koji se javlja je tipičan problem analize koji se temelji na činjenici da zbog pretrpanosti informacija dolazi do poteškoća filtracije najbitnijih, a najočitije informacije su posljedica medijske pozornosti i objavljivanja informacija motiviranih partikularnim interesima kao što su postizanje političkih ciljeva. Ključne kritične infrastrukture su sve kompleksnije i ovisnije o informacijskoj tehnologiji, a za političku militantnost ne postoje geografske barijere uslijed demokratizacije informacija putem medija (Ducaru, 2016:9). Zbog dostupnosti i profitabilnosti korištenja informacijske tehnologije, organizirane skupine i države koriste kibernetički prostor za traženje prava i provođenje ratnih aktivnosti (Ducaru, 2016:9).

NATO dostupnost određenih informacija ograničava: što opravdava pozivanjem na zaštitu nacionalnih interesa. Prema tome dostupnost informacija je ograničena razinom neotkrivanja klasificiranih podataka. Stoga se istraživanje temelji na objavljenim i dostupnim podacima izvučenih od utjecajnih autora u području kibernetičke sigurnosti i podacima objavljenim na NATO–vim službenim stranicama. Do skrivanja podataka dolazi i zbog onemogućavanja potencijalnih protivničkih snaga da analiziraju ranjivost kibernetičkih sustava ili da koriste znanje u nadogradnji za vlastite potrebe: koje se potom mogu koristiti za ugrožavanje protivničke stranke u obliku napada ili ucjenjivačkog potencijala. Prema tome istraživanje kibernetičkog razvoja NATO–a ostaje ograničeno. Kibernetička sigurnost dotiče pitanje kompleksnosti reguliranja i održivosti sustava koje se temelji na međuovisnosti. Održivost se odnosi na stanje sustava u kojemu se zadovoljavaju potrebe sadašnjosti bez ugrožavanja sposobnosti zadovoljavanja budućih potreba. O tome uvelike ovisi rad sustava. Adekvatna

[62] Komunikacijski i informacijski sustavi

procjena kapaciteta regulacije i razina u kojemu sustav ugrožava okolinu, mogu dati uvid u učinkovitost i isplativost samoga sistema.

Istraživanje stavlja fokus na tri glavne varijable, a to su: političke odluke, sigurnosne prijetnje i kibernetički razvoj, a kompleksnost međunarodnih odnosa uključuje enorman niz faktora koji objašnjavaju razvoj donošenja odluka. Istraživanje daje uvid u utjecaj političke scene na razvoj informacijskih razmjena koji je često zanemaren zbog primarne fokusiranosti javnosti na tehničke aspekte informacijske razvijenosti, stoga je jedan od ciljeva rada naglasiti bitnost političkih inicijativa u sferi informacijske implementacije u kompleksne organizacijske sisteme. Kibernetički razvoj kao ovisna varijabla ne ovisi samo o znanstvenim postignućima, već i o privatnim i političkim interesima koji dovode do motiviranosti ulaganja u iste, bilo u obliku profita ili utjecaja. Rad može poslužiti kao podloga i poticaj drugim akterima akademske zajednice da razmišljaju u terminima međunarodnih odnosa. Suvremeni tijek događanja potvrđuje sve veću isprepletenost različitih ekonomskih, vojnih, geopolitičkih, tehnoloških i ekoloških sfera što zahtjeva promišljanje u terminima njihove zajedničke sintetizacije za pronalaženje uzročno–posljedičnih veza zbivanja: što je bitno pošto stupanj izoliranosti sfera postaje sve manji, odnosno uzroci događaja sve zamagljeniji.
Zbog neizvjesnosti koja dovodi do manjka predvidljivosti, zbog složenosti i volatilnosti promjena, identifikacija napadača postaje sve teža u asimetričnim sučeljavanjima (Ruiz i Winter, 2017:78), a uočavanje motiva putem analize političkih događanja može potencijalno dovesti do kristalizacije aktera s najvećom koristi u provođenju određenih kibernetičkih napada. Raštrkanosti i inter–povezanost, te različita tolerancija rizika narušava sposobnost odvraćanja kibernetičkih napada (Burton, 2015:303). Teorijski okvir kojim se NATO kao organizacija vodi, uvelike se može iščitati iz članka 5 Sjevernoatlantskog ugovora koji govori o kolektivnoj obrani. Može se reći da ukoliko ne dođe do ozbiljnih sigurnosnih prijetnji koje mijenjaju strukturu same organizacije, razvoj kibernetičke obrane izostaje.

Postavlja se pitanje relevantnosti daljnjega djelovanja NATO–a ako unatoč sigurnosnim prijetnjama ne razvije prikladne sposobnosti za suzbijanje istih. Stoga treba naglasiti bitnost tih promjena kao reakciju na vanjske čimbenike. Reakcije na te vanjske čimbenike se mogu jasno iščitati iz političkih odluka same organizacije, iako treba naglasiti opažanje Eneken Tikk koja

napominje da se ukupnost prijetnji ne poklapa u potpunosti s legalnim okvirom, zbog nedostatka koordinacije i nedostatka prijava prijetnji (Tikk, 2011:120).

Najdostupniji izvori koji nam govore o tome kako se struktura NATO–a prilagođava novonastalim prijetnjama su upravo summiti i javno dostupni dokumenti koji sadržavaju ishode političkih odluka. Taj obrazac razvoja možemo pratiti kroz ovo istraživanje. Možemo ga pratiti od konflikta u Kosovu koji rezultira Strateškim konceptom 1999., summitom u Pragu 2002. godine i formiranjem kibernetičkih tijela za suzbijanje kibernetičkih prijetnji, pa sve do summita u Bruxellesu 2021. godine koji također rezultira promjenama u kibernetičkoj obrani NATO–a. Možemo pratiti različite uzroke poboljšanja kibernetičke obrane NATO–a. Multidisciplinarni timovi su glavni čimbenik poboljšanja provođenja učinkovitosti i uspješnosti kibernetičkih ratovanja zbog volatilnosti i dinamičnosti prirode sigurnosnih prijetnji, koja dovodi do partnerstva privatne industrije, Saveza i akademske zajednice (Ducaru, 2016:9). Možemo primijetiti da recipročna razmjena informacija i suradnja poboljšavaju učinkovitost odgovora na kibernetičke prijetnje. Izuzev kooperacije na tehničkoj i taktičkoj razini, ključni oblik suradnje čini razmjena podataka, kao npr. NATO–vo dijeljenje podataka o prijetnjama s državnim i privatnim tvrtkama, kao i s Europskom unijom 2017. godine tijekom kampanja NotPetya i WannaCry (Mad'ar, 2019:17). Sve češće korištenje kibernetičkih sposobnosti, veća povezanost terorizma i kibernetičkog prostora i razvoj ‘kibernetičkog piratstva’: koji se očituje u okretanju državnih aktera prema digitalnom kriminalnom podzemlju za nabavu kibernetičkih alata i izvršenju kibernetičkih napada, navode na sve veću važnost kibernetičkih prijetnji u međunarodnim odnosima (Ducaru, 2016:9). Upravo usvajanje političkih odluka i njihova efektivna implementacija rezultira stvaranjem poboljšanih kibernetičkih sposobnosti. Prema tome, potrebno je kontinuirano analizirati sve izraženije sigurnosne prijetnje za održavanje nacionalne sigurnosti i funkcionalnog međunarodnog poretka.

# 7. LITERATURA


Burton, Joe (2015) NATO's cyber defence: strategic challenges and institutional adaptation. *Defence Studies* 15(4): 297–319.

Cherneha, Volodymyr, Marchenkov, Serhiy, and Shypovskyi, Volodymyr (2020) Analysis of the ways of improvement of Ukraine – NATO cooperation on cybersecurity issues. *Journal of Scientific Papers 'Social development and Security'* 10(2): 11–15. DOI: 10.33445/sds.2020.10.2.2.

Cilluffo, Frank J., Evans, Timothy J., Ilves, Luukas K., et al. (2016) European Union and NATO Global Cybersecurity Challenges: A Way Forward. *Prism: A Journal of the Center for Complex Operations* 6: 126.

Ducaru, Sorin Dumitru (2016) THE CYBER DIMENSION OF MODERN HYBRID WARFARE AND ITS RELEVANCE FOR NATO. *Europolity: Continuity and Change in European Governance* 10: 7–23.

Efthymiopoulos, M.P. (2009) NATO's Security Operations in Electronic Warfare. *Journal of Information Warfare* 8(3). Peregrine Technical Solutions: 61–70.

Fidler, David P, Pregent, Richard and Vandurme, Alex (2013) NATO, cyber defense, and international law. . *John's J. Int'l & Comp. L.* 4(1). HeinOnline: 1-25.

Hammock, CJ (2017) Enabling the Development and Deployment of NATO Cyber Operations. *Journal of Information Warfare* 16(3). Peregrine Technical Solutions: 79–94.

Hasanov, Arif Hasan, Iskandarov, Khayal Ibrahim and Sadiyev, Sadi Saleh (2019) THE EVOLUTION OF NATO'S CYBER SECURITY POLICY AND FUTURE PROSPECTS. *Journal of Defense Resources Management* 10(1). ' Carol I' National Defence University: 94–106.

Jensen, Benjamin, Maness, Ryan and Valeriano, Brandon (2019) Fancy bears and digital trolls: Cyber strategy with a Russian twist. Journal of Strategic Studies 42(2). Routledge: 1–23. DOI: 10.1080/01402390.2018.1559152.

Joubert, V., NATO Defense College, and North Atlantic Treaty Organization (2012) *Five Years After Estonia's Cyber Attacks: Lessons Learned for NATO?.* Research paper. Research Division, NATO Defense College. NATO Defense College, Research Division. Available at: https://books.google.hr/books?id=kb_iwAEACAAJ.

Kovács, László (2018) Cyber Security Policy and Strategy in the European Union and Nato. *Land Forces Academy Review* 23(1): 16–24.

Limnéll, J. and Salonius-Pasternak, C. (2016) *Challenge for NATO: Cyber Article 5*. Center for Asymmetric Threat Studies (CATS) briefing paper. Center for Asymmetric Threat Studies. Available at: https://books.google.hr/books?id=wgaozgEACAAJ.

Maďar, Tomáš (2019) LAGGING COLOSSUS OR A MATURE CYBER-ALLIANCE? 20 Years of Cyber Defence in NATO. *Obrana a strategie (Defence and Strategy)* 19(1): 5–22. DOI: 10.3849/1802-7199.19.2019.01.005-022.

Nagy, Károly and Sherifi, Shkendije G. (2013) Small Countries and Cyber Defence. *Academic and Applied Research in Military and Public Management Science* 12(2): 329–342. DOI: 10.32565/aarms.2013.2.14.

Ogorec, Marinko (2009) NOVA REFORMA RUSKIH ORUŽANIH SNAGA: ISKUSTVA IZ RUSKO - GRUZIJSKOG SUKOBA. *Polemos* 7(24): 11-32.

Pernik, Piret (2014) Improving Cyber Security: NATO and the EU. International Centre for Defence Studies: 1–18.

Ruiz, Natasha and Winter, Rogerio (2017) CYBERSECURITY, CYBER WEAPONS AND CYBER-ATTACKS: RESPONSIBILITY AND DIFFERENT REFLECTIONS ON THE SUBJECT. *Critical Infra Structure Protection Review ISSN 2516-0087*: 77–82.

Shea, Jamie (2017) How is NATO meeting the challenge of cyberspace? *Prism* 7(2). JSTOR: 18–29.

Tikk, Eneken (2011) Ten Rules for Cyber Security. *Survival* 53(3): 119–132. DOI: 10.1080/00396338.2011.571016.

Yost, David S. (2010) NATO's evolving purposes and the next Strategic Concept. *International Affairs* 86(2): 489–522.

Carnegieendowment.org (2021) A Brief Primer on International Law and Cyberspace https://carnegieendowment.org/2021/06/14/brief-primer-on-international-law-and-cyberspace-pub-84763 Pristupljeno: 25. kolovoza 2022.

Ccdcoe.org (2022) Cyber attacks and Article 5 – a note on a blurry but consistent position of NATO https://ccdcoe.org/library/publications/cyber-attacks-and-article-5-a-note-on-a-blurry-but-consistent-position-of-nato/ Pristupljeno: 27. kolovoza 2022.

Ccdcoe.org (2014) NATO on Its Way Towards a Comfort Zone in Cyber Defence https://ccdcoe.org/library/publications/nato-on-its-way-towards-a-comfort-zone-in-cyber-defence/ Pristupljeno: 8. ožujka 2022.

Cybersecforum.eu (2017) https://cybersecforum.eu/wp-content/uploads/2021/06/ECJ-VOLUME-3-2017-ISSUE-2.pdf Pristupljeno: 30. svibnja 2022.

NATO (2021) NATO Cyber defence https://www.nato.int/cps/en/natohq/topics_78170.htm?fbclid=IwAR3cbP3KbuelrqaZKtNvw5QlEXrwh7Dq-S-UmPgQilINE2hP0LwewpCbAkQ Pristupljeno: 30. svibnja 2022.

NATO (2021a) NATO Cyber defence https://www.nato.int/nato_static_fl2014/assets/pdf/2021/4/pdf/2104-factsheet-cyber-defence-en.pdf Pristupljeno: 30. svibnja 2022.

NATO (2022) Press conference https://www.nato.int/cps/en/natohq/opinions_197288.htm?selectedLocale=en Pristupljeno: 27. srpnja 2022.

NCIA (2020) NATO Communications and Information Agency https://www.ncia.nato.int/about-us.html Pristupljeno: 27. srpnja 2022.

# 8. SAŽETAK I KLJUČNE RIJEČI

Razvoj kibernetičke obrane u NATO–u nastaje kao ishod sve većih sigurnosnih prijetnji i potrebe za obranom sigurnosti kritične infrastrukture. Promjene unutar organizacije se mogu promatrati kao svojevrsna refleksija promjena međunarodnih odnosa, tehnološkog napretka, političkih inicijativa i sustavnog provođenja aktivnosti koje poboljšavaju koordinaciju u donošenju odluka. Razvoj kibernetičkih sposobnosti unutar NATO–a smanjuje stupanj uspješnosti nadolazećih kibernetičkih napada na kritične infrastrukture; odnosno povećava uspješnost pronalaska točaka ranjivosti sistema; što dovodi do nadogradnje u dijelovima strukture u kojima je došlo do identifikacije nedostataka. Rad se bavi međusobnim utjecajem sigurnosnih prijetnji i političkih promjena na kibernetički razvoj, stoga istraživačko pitanje glasi: kako su političke odluke donesene zbog nastalih sigurnosnih prijetnji utjecale na razvoj kibernetičke obrane u NATO–u?

*Ključne riječi*: nacionalna sigurnost, kibernetička obrana, NATO, političke odluke, sigurnosne prijetnje, međunarodni odnosi

## 9. SUMMARY AND KEYWORDS

The development of cyber defence in NATO is the result of increasing security threats and the need to defend critical infrastructure security. Changes within the organisation can be seen as a reflection of changes in international relations, technological progress, political initiatives and systematic implementation of activities that improve coordination in decision – making. The development of cyber capabilities within NATO reduces the degree of success of upcoming cyber attacks on critical infrastructures; namely, it increases the success rate of finding system vulnerability points; which leads to upgrades in parts of the structure where defects have been identified. This paper addresses the mutual influence of security threats and policy changes on cyber development, therefore the research question is: how have policy decisions made in response to emerging security threats affected NATO's cyber defence development?

*Keywords*: national security, cyber defence, NATO, policy decisions, security threats, international relations