Hybrid Warfare Research Institute

Udruga Sv. Jurja St. George Association

ZAKLJUČCI 4. ZAGREBAČKOG SIGURNOSNOG FORUMA (2019)

PREPOZNAVANJE I SUOČAVANJE S NOVIM HIBRIDNIM I CYBER SIGURNOSNIM IZAZOVIMA - STVARANJE OTPORNE KRITIČNE INFRASTRUKTURE

Jačanje demokracije, zaštita sloboda i društva

U suočavanju s hibridnim prijetnjama prevladavaju tri pristupa:

I. Znanstveno-tehnološki, koji se temelji na mišljenju o učinkovitosti tehnologije i pretpostavci da se bolje tehnologije mogu učinkovito suočavati s prijetnjama. Tehnologije pak mogu biti, a što u većini slučajeva i jesu, razvojne. Međutim njihov glavni problem je da i najbolja tehnološka rješenja ovise o ljudima koji ih stvaraju, koriste i tumače. Ljudski je čimbenik vrlo često previše siguran u vlastite sposobnosti i mogućnosti, ponekad nedovoljno iskusan i obučen, zbog čega nije u stanju prepoznati nesavršenost sustava ili jednostavno nije u stanju donositi točne i pravodobne odluke.

II. Teoretski se razvio između strateškog i taktičkog koncepta i pristupa ovom problema ističući stav da bolje planiranje znači bolju i učinkovitiju obranu.

Bar-Ilan University

Tri ključne stavke teoretskog koncepta su: Prevencija, Imenovanje i Odgovor.

- **PREVENCIJA**

  Klasični oblici preventivnog djelovanja temelje se na mogućnosti, sposobnosti i spremnosti uporabe konvencionalnih obrambeno-napadnih vojnih sredstava u slučaju potrebe. Danas je pak većina klasičnih vojnih sredstava kojima neka

NATO OTAN This workshop is supported by: The NATO Science for Peace and Security Programme

država raspolaže vrlo irelevantna za moderne sukobe ili pak njena uporaba nije rješenje većine nesporazuma (je li npr., bilo Ujedinjeno Kraljevstvo, bilo Španjolska, spremno ući u oružani sukob zbog teritorijalnih voda oko Gibraltara ili Gibraltara samog?). Danas je bitno postaviti pitanje: kako organizirati učinkovitu preventivnu zaštitu u digitalnom svijetu? Možemo li odvratiti pojedince, grupe, države od napada na naše pojedinačne ili zajedničke interese i ciljeve u digitalnom svijetu? Je li prevencija dovoljna sama po sebi?

- **IMENOVANJE**

U prethodnim desetljećima bilo je lako odrediti izvor agresije kao i njihove pokretače. Napadnuti je znao, jer je vidio i osjetio, tko ga napada, kako, s čim, i gdje. Danas je pitanje napada u cyber svijetu izuzetno dobro prikriveno (posebno kad govorimo o institucionalnim napadačima) i sakriveno. Vrlo često se dogodi da onaj tko je napadnut hibridnim (ili cyber) napadima da toga nije niti svjestan. Čak i kad je napadnuti svjestan da je izložen hibridnim napadima, vrlo često ne može pouzdano odrediti tko uistinu stoji iza napada, odnosno tko je stvarni napadač, planer i/ili organizator napada. Stoga je neophodno usmjeriti aktivnosti koje napadnutima stoje na raspolaganju s primarnim ciljem identificiranja napadača, njegovog pouzdanog i nedvojbenog imenovanja kao izvora prijetnje.

U tom je cilju nužno snažno raditi, integriranjem sposobnosti i znanja koja se nalaze u državnom, javnom, privatnom i akademskom sektoru, na iznalaženju načina, modela, metoda i sredstava s ciljem pouzdanog imenovanja izvora hibridnih napada. Postojanje takvog sustava jedan je od najboljih načina prevencije napada.

NATO OTAN This workshop is supported by: The NATO Science for Peace and Security Programme

- **ODGOVOR**

U vremenu kad je imenovanje napadača bilo nedvojbeno, i odgovor korištenjem odgovarajućih sredstava mogao je biti prilagođen identificiranom napadaču. Danas je, sagledavajući odličnu prikrivenost hibridnih napada i napadača, uistinu vrlo zahtjevno, a ponekad i gotovo nemoguće uobičajenim metodama i sredstvima, odrediti tko stoji iza napada, a time i prema kome, kojim sredstvima, gdje i kako odgovoriti na napad. A na napad se mora, na neki način, odgovoriti.

Razgovori o potrebi postojanja i razvoja posebno obrambenih a posebno napadnih efektiva posebno u cyber svijetu, postaju izuzetno nepotrebni, neproduktivni, čak i štetni za organiziranje učinkovite obrane. Razvoj integriranih sustava i modela aktivne obrane te prigodnih tehnoloških rješenja ukazuje na novu stvarnost.

Nova stvarnost iziskuje raspravu o novim etničkim pitanjima kao i potrebu definiranja pravila hibridnog, posebno onog u cyber prostoru, ratovanja. Naime, koja je to razina izvjesnosti u pouzdanost imenovanja stvarnog napadača koja može pokrenuti odgovarajući odgovor u vidu aktiviranja vlastitih napadnih efektiva; treba li na cyber napad na neku instituciju ili tvrtku (pa i onu privatnu) na vlastitom teritoriju odgovoriti sredstvima aktivne obrane koja državi stoje na raspolaganju; kako se ponijeti u slučaju napada na neku osobu? Kako zaštiti vlastiti informacijsko-komunikacijski prostor i vlastitu i asocijacijsku informacijsku i digitalnu suverenost zadržavajući dostignute vrijednosti demokratskog društva te prava i sloboda pojedinca i zajednica?

Čak i ako se pouzdano imenuje napadač, koja je to razina odgovora koja se treba primijeniti i prema kojim ciljevima? Treba li na napad digitalnim pištoljem,

pokrenuti odgovor korištenjem digitalnog nosača zrakoplova i cijele digitalne flote?

Ono što je jasno jest da još ne postoje takva pravila jer su izazovi s kojima se susrećemo više tehnološki revolucionarnije nego evolucijske naravi (primjer složenih računalnih malicioznih programa kao što su STUXNET i FLAME).

III. Praktički naglašava potrebu izgradnje pouzdanog sustava učinkovitog upravljanja krizama, te razvoj prilagodljivih struktura i postupaka u upravljanja krizama. Postojanje učinkovitih struktura za upravljanje krizom, a koje prolaze redovne, kvalitetne i stvarne procese obuke i uvježbavanja, znači da se čak i na najmanje očekivane (ili pak i na one neočekivane) krize može pripremiti kvalitetan i pouzdan odgovor. Jedna od ključnih potreba ovog sustava je i potreba razvoja modela učinkovitog kriznog komuniciranja.

Problemi, sigurnosna područja, naučene lekcija, preporuke

1. Hibridne su prijetnje stvarna i prisutna prijetnja. Hibridne prijetnje i krize iziskuju i hibridne odgovore, ne samo one temeljene na tehničkim i tehnološkim mogućnostima nego i uključivanjem sustava za upravljanje krizama.

2. Upravljanje krizama mora biti planiran, izvježban i redovno, u što stvarnijim uvjetima, uvježbavan proces. Samo oslanjanje na tehnologiju ne jamči uspjeh nego neuspjeh. Ljudski je čimbenik važan kao i tehnološko rješenje.

3. Međunarodna suradnja nije luksuz nego nužnost. Ona je nerazdvojiv dio odgovora s obzirom da su hibridne prijetnje stvarnost, ne samo na lokalnoj i regionalnoj, nego i globalnoj razini. Stoga i odgovor mora biti takav.

4. Samostalna rješenja otežavaju i onemogućavaju međunarodnu suradnju. Isto kao i rascjepkanost i neuvezanost institucija unutar pojedinih država i

zajednica. Ukazujemo na povećanu potrebu standardizacije i zajednički prihvaćenih sigurnosnih postupaka, protokola i certifikata.

5. Tehnološki razvoj mora staviti naglasak na četiri temeljne sposobnosti: međusobnu kompatibilnost, interoperabilnost, obuku i certificiranje.

6. Državne institucije, ministarstva i agencije, natječu se za proračunska sredstva s ciljem razvoja vlastitih efektiva u domeni hibridnih djelovanja. U stvarnosti se pak oko 80% sektora kritičnih infrastruktura u razvijenom svijetu nalazi u rukama privatnih vlasnika i štićeno od strane privatnih zaštitarskih tvrtki. Stoga privatni sektor treba biti shvaćen i prihvaćen kao, u najmanju ruku, jednakopravan partner u razvoju i primjeni strategija i taktika za suočavanje s hibridnim prijetnjama. U tom smislu, i u tom spektru aktivnosti, obvezatno treba uključiti i akademsku zajednicu s njenim znanjima i sposobnostima.

7. Sustav obuke ne smije biti ograničen unutar nacionalnih okvira. Izgradnju prekogranične obuke treba razvijati na sličan način kao što je već uspostavljen sustav za suočavanje s katastrofama.

8. Hibridne prijetnje u obliku operacija utjecaja na demokratska društva, posebno u domeni zlonamjernih utjecaja na izbore, iziskuju razvoj društvene otpornosti. Ona mora biti temeljena na osobnom, ali i zajedničkom pristupu akademskog, državnog, javnog i privatnog sektora.

9. Dezinformacijske aktivnosti, kako bi bile učinkovite, iziskuju određeno vrijeme za pripremu. Kao što je već naglašeno u točkama 3. i 6., pozitivni učinak suradnje treba biti vidljiv u razvoju učinkovite i pouzdane alate umjetne inteligencije s posebnim naglaskom na suočavanje s hibridni prijetnjama koje koriste mogućnosti društvenih mreža. Cilj je prepoznavanje hibridnih prijetnji i napada, kao i imenovanje napadača, u ranoj fazi planiranja i djelovanja. Ti alati, razvijani i podržani na nacionalnoj i asocijacijskoj (međunarodnih

NATO OTAN This workshop is supported by: The NATO Science for Peace and Security Programme

organizacija kojih je zemlja država članica) razini trebaju služiti kao sustav za rano upozoravanje prijetnji.

10. Združeno djelovanje državnog, javnog, privatnog i akademskog sektora na području razvoja informacijske i digitalne pismenosti te kritičkog razmišljanja neophodan je uvjet za postizanje stanja informacijskog i digitalnog suvereniteta na nacionalnoj i međunarodnoj (asocijacijskoj) razini. Cilj je očuvanje demokracije te zadržavanje i razvoj dostignutih prava i sloboda pojedinca i društava.

11. Neophodno je razviti model i sustav međunarodno priznatih i prihvaćenih pravila, odnosno konvencija o sukobima u digitalnom prostoru koje će biti moguće primijeniti, a po potrebi i nametnuti njihovu primjenu i pridržavanje. Hibridne sukobe, s naglaskom hibridnih napada na kritičnu infrastrukturu od životne važnosti, treba tretirati kao uporabu sredstava za masovno uništavanje.

NATO OTAN This workshop is supported by: The NATO Science for Peace and Security Programme

13.-14. ožujka 2020. Zagreb

NATO OTAN

This workshop is supported by: The NATO Science for Peace and Security Programme

This workshop is supported by: The NATO Science for Peace and Security Programme