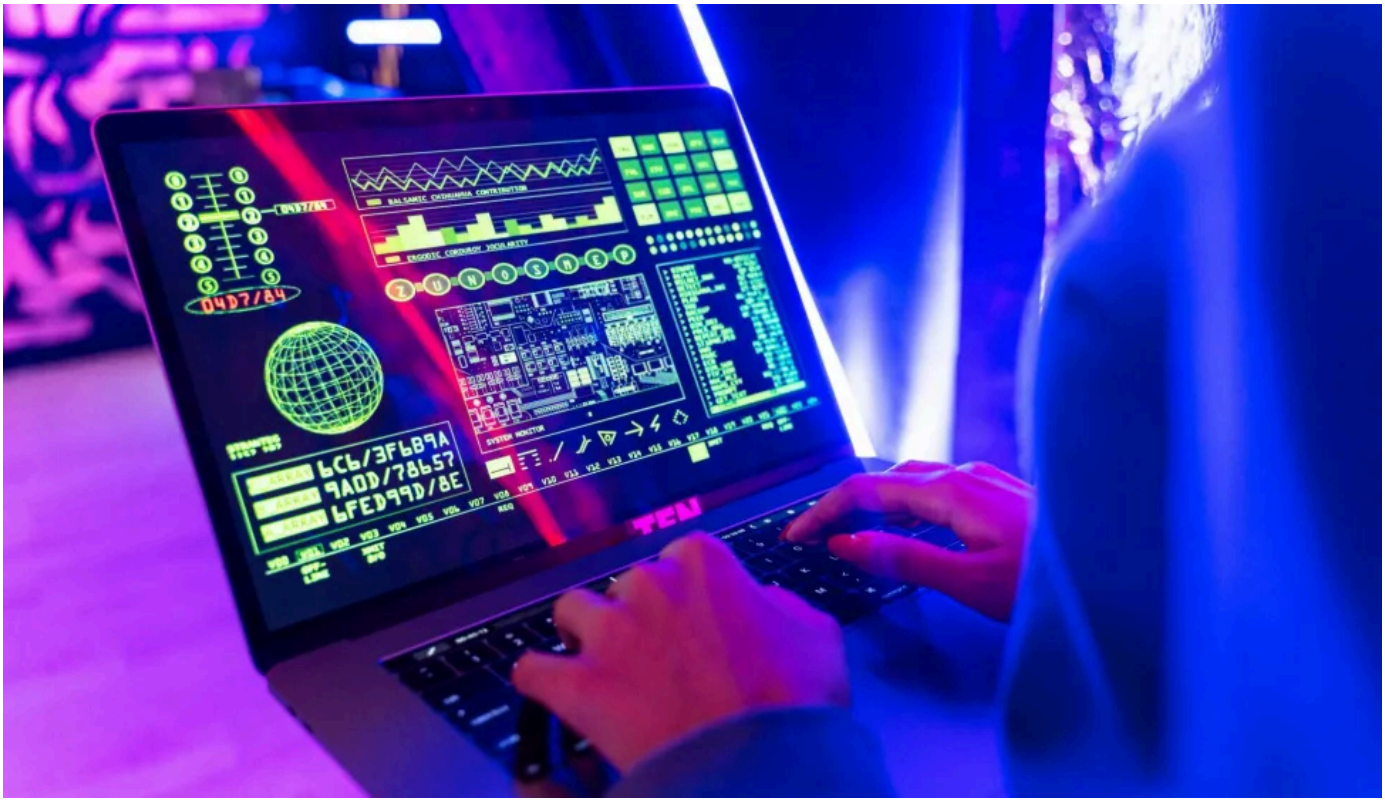
Glas Slavonije



PEXELS

1.11.2025., 13:00

Ivica MANDIĆ

SIGURNOSNE UGROZE U EUROPI

Hibridnim ratovanjem udara se na temelje liberalne demokracije

ŠIRENJE PODRUČJA BORBE: HIBRIDNO RATOVANJE DANAS VIŠE NIJE SAMO TEORIJSKI POJAM...

U drugom nastavku feljtona, ekskluzivno za Magazin Glasa Slavonije, **Ivica Mandić**, vojni komentator, umirovljeni načelnik Centra za obrambene i strateške studije Hrvatskog vojnog učilišta u Zagrebu, opsežno elaborira najvažnije aspekte kompleksnog područja kakvo je hibridno ratovanje danas te upozorava na ozbiljnu razinu prijetnji s kojima se suočava Europa/Europska unija.

- Hibridno ratovanje danas više nije samo teorijski pojam; ono je praktičan okvir koji objašnjava kako autoritarni akteri, prije svega Rusija nakon 2014. i naročito od 2022. godine, kombiniraju vojna,

Glas Slavonije

IVICA MANDIĆ

i ostvarivali geostrateške ciljeve u Europi. Europska unija i države članice pod stalnim su pritiskom upravo zato što su otvorene, međusobne povezane i snažno oslonjene na digitalnu, energetsku i trgovačku infrastrukturu. **[20]**

SVI POSTAJU IZLOŽENI

Koliko ozbiljno hibridno ratovanje ugrožava sigurnost EU?:

Opći odgovor glasi - ozbiljno i višeslojno, ali heterogeno po intenzitetu i učinku. Hibridne akcije ne moraju dovesti do otvorenog oružanog sukoba da bi proizvele znatne strateške posljedice - cilj često nije okupacija, nego erozija odlučnosti, razdor u društvu i onesposobljavanje ključnih sustava. Time se stvara trajna "siva zona", u kojoj se političke odluke i javno povjerenje postupno potkopavaju. Takvu ocjenu podupiru temeljne institucionalne procjene EU-a i NATO-a: hibridne prijetnje obuhvaćaju koordinirane napade s pomoću dezinformacija, cyber-napada, ekonomske ucjene i ciljane sabotaže kritične infrastrukture. **[21]**

Dva praktična razloga zašto je učinak velik:

Povezanost i ovisnost: Europski sustavi (energetski, financijski, transportni, telekomi) visoko su međusobno povezani - kvar u jednom lancu lako prelijeva učinak u druge domene.

Teškoća atribucije i "uvjerljivo poricanje": Kad se napad ne može brzo i jednoznačno pripisati državnom nalogodavcu, politički odgovor postaje fragmentiran i usporen, što daje napadaču stratešku prednost. **[22]**

Tko je najizloženiji (države, regije, institucije):

Izloženost varira po geografskoj i institucionalnoj ranjivosti:

- predugi istočni i baltički rub EU/NATO (Poljska, baltičke države, Rumunjska, Bugarska) - zbog blizine Rusiji, povijesnih tenzija i velikog interesa Moskve za utjecaj u tim državama, te su članice često u fokusu hibridnih pokušaja destabilizacije (dezinformacije, politički utjecaji, cyber-napadi). **[23]** (Atlantic Council+1)

Glas Slavonije

društva i napade na kritičnu infrastrukturu. Njemačka je javno identificirala veću izloženost informacijskim i cyber-pritiscima **[24]**

- manje/ranjivije članice s ograničenim kapacitetima za cyber-obranu i javnu otpornost - države s manje razvijenom digitalnom sigurnosnom infrastrukturom te slabijim regulatornim i medijskim okvirom bit će ranjivije na sve vrste hibridnih pritisaka. **[25]**

VRSTE I RANJIVOST

Koji su segmenti društva najizloženiji i kakvim prijetnjama?

Državne institucije i uprava: vlade, ministarstva, vojska, obavještajne agencije:

- vrste prijetnje: hakerski upadi u mreže, kompromitacija komunikacija, krađa podataka, sabotaža IT sustava, kompromitiranje lanaca opskrbe

- zašto ranjivost: državni sustavi često su integrirani s privatnim dobavljačima; kompromitirani softver ili usluge imaju učinak "jedan za sve". ENISA i NATO identificiraju državne kapacitete kao prioritetne mete cyber i informacijskih kampanja. **[26]**

Kritična infrastruktura: energetika, transport, vodovod, telekomi, financije...:

- vrste prijetnje: fizičke sabotaže (npr. podvodne komunikacijske kabele, energetske instalacije), napadi na dostupnost (DDoS, ransomware), ometanje opskrbe energijom kao oblik ucjene

- zašto ranjivost: privatni operatori, međuzavisnost i troškovna osjetljivost otežavaju brzu redundancu. ENISA i izvještaji o incidentima 2024. - 2025. stavljaju prijetnje dostupnosti i ransomwarea u vrh liste. **[27]**

Mediji, društvene mreže i javni informacijski prostor:

- vrste prijetnje: koordinirane kampanje dezinformacija, "astroturfing", botovi, manipulacija viralnim pričama, ciljano mikroprofiliranje birača

- zašto ranjivost: pluralizam medija i platformi znači da se lažne naracije brzo šire, a retroaktivno je ispravljanje teško; polarizacija društva pogoršava učinak. Atlantic Council i Chatham House ističu da informacijske kampanje imaju cilj smanjiti društvenu koheziju i povjerenje u institucije. **[28]**

Civilno društvo, nezavisne organizacije, akademija i think-tankovi:

- vrste prijetnje: ciljana kompromitacija, diskreditacijske kampanje, hakiranje i iznošenje povjerljivih podataka, financijski pritisci

Glas Slavonije

Privatne kompanije, posebno sektor visokih tehnologija i opskrbni lanci:

- l vrste prijetnje: krađa intelektualnog vlasništva, kompromitacija dobavljačkih lanaca, ucjene i širenje zlonamjernog softvera kroz industrijske platforme. ENISA i analize incidenta pokazuju rast napada usmjerenih na lance opskrbe i pružatelje usluga. **[30]**

Javne usluge ključne za društvenu stabilnost: zdravstvo, obrazovanje, hitne službe...:

- vrste prijetnje: *ransomware* koji paralizira bolnice, dezinformacije oko javnog zdravlja koje potkopavaju povjerenje, opstrukcija obrazovnih napora

- zašto ranjivost: ove institucije kritične su za održavanje svakodnevnog reda - njegov prekid ima neposredne društvene i političke efekte. **[31]**

SOA zabrinuta...

Što službeni izvori i analize kažu o stanju u Hrvatskoj? Sigurnosno-obavještajna agencija (SOA) i povezani nacionalni centri posljednjih godina sve više identificiraju rastuće kibernetičke prijetnje, špijunažu i pokušaje utjecaja koji se uklapaju u definiciju hibridnih prijetnji. U javno objavljenim izvješćima SOA je naglasila povećani broj ozbiljnih kibernetičkih napada na državne institucije i uspostavu Nacionalnog centra za kibernetičku sigurnost unutar SOA-e, kao odgovora na tu dinamiku. To pokazuje da državne institucije prepoznaju aktivnu prijetnju i rade na institucionalnoj konsolidaciji odgovora. **[42]** (ncsc.hr) Istodobno, europske i regionalne analize (ENISA, HybridCoE, razne studije) upozoravaju da je Hrvatska, kao članica EU-a i NATO-a povezana energetskim i informacijskim tokovima, izložena sličnim obrascima napada kao i druge članice: cyber-kampanje, manipulacija informacijama i pokušaji utjecaja kroz mrežu lokalnih i transnacionalnih medija i platformi. Hrvatska se, također, formalno uključuje u mehanizme suradnje protiv hibridnih prijetnji (npr. članstvo u HybridCoE), što pokazuje želju za kolektivnim odgovaranjem. (enisa.europa.eu)

METODE UGROŽAVANJA

Posebni obrasci/operativne metode koje pogoduju prijetnji:

- korištenje privatnim i kriminalnim mrežama kao “force multiplier” (npr. suradnja države s cyber-kriminalnim grupama ili toleriranje njihova djelovanja), što komplicira atribuciju i pravni odgovor **[32]**

- kombinacija malih, sinkroniziranih incidenata (manji cyber-upadi + viralna dezinformacija + lokalna sabotaža), koji zajedno proizvode neproporcionalan učinak - to je “hibridni efekt”: mala

- napadi na vjerodostojnost izvora: hakiranje novinara, curenje selektivnih dokumenata i njihovo obnavljanje kroz dezinformacijske mreže da se stvori narativ kompromitacije institucija. **[34]**

Kolika je vjerojatnost i koji su mogući učinci u kratkom i srednjem roku?

Kratki rok (0 - 2 godine): Nastavak dnevnih ili tjednih cyber-incidenata (DDoS, ransomware), intenzivirane kampanje dezinformacija u kriznim razdobljima (izbori, energetska kriza) te izolirani incidenti sabotaže - sve s ciljem podizanja političkog troška i polarizacije. ENISA-ini trendovi iz 2024. upućuju na rast napada usmjerenih na dostupnost i ransomware. **[35]**

Srednji rok (2 - 5 godina): Sustavni pritisci koji polako erodiraju povjerenje u institucije, mogućnost da suptilne, ali trajne mjere slabe kolektivnu obrambenu volju EU; razvoj novih oblika hibridnih alata (UI-generirane dezinformacije, napadi na satelitsku/svemirsku infrastrukturu). NATO i EU planovi upućuju da se upravo takve prijetnje anticipiraju u obrambenim strategijama. **[36]**

SURADNJA I ZAŠTITA

Kako smanjiti ranjivost - preporuke (kratko, konkretno)?

Povećati otpornost kritične infrastrukture: Zahtjevi za redundanciju, segmentaciju mreža, obvezne provjere sigurnosti dobavljača i obvezne planove oporavka. (ENISA/EU strategije). **[37]**

Jačanje institucionalne koordinacije: Jedinstveni nacionalni mehanizmi za rano upozorenje i koordinirani odgovori na hibridne incidente (civilno-vojna-privatna suradnja). NATO i EU već grade takve kapacitete. **[38]**

Otpornost informacijske sfere: Medijska pismenost, transparentnost financiranja i oglašavanja na društvenim mrežama, regulacija automatiziranih kampanja i bolji monitoring manipulacija bez zadiranja u slobodu govora. (Preporuke iz analize Atlantic Council/Chatham House.) **[39]**

Zaštita ranjivih društvenih segmenata: Financijska i sigurnosna pomoć manjim državama članicama za jačanje vlastitih kapaciteta; programi za jačanje civilnog društva. **[40]**

Međunarodna suradnja i sankcije režimu: Brži i precizniji mehanizmi za atribuciju i proporcionalan odgovor (uključujući javno izlaganje odgovornosti zlonamjernih aktera). **[41]**

Zaključak: Hibridno ratovanje za Europu znači ozbiljnu, višedimenzionalnu i trajnu prijetnju upravo zato što efikasno iskorištava ranjivost otvorenih, povezanih društava. Učinci variraju: od otežanih političkih procesa i erozije povjerenja do izravnih kvarova u kritičnoj infrastrukturi.

Najizloženiji su oni koji su istovremeno visoko vrijedni za napadača i slabo zaštićeni - istočni rub Europske unije, ključne državne i privatne infrastrukture, medijska i civilna sfera. Odgovor mora biti

Glas Slavonije

Linkovi i objašnjenja

[20] Hybridthreats - Consilium
[21] 241007-hybrid-threats-and-hybrid-warfare.pdf
[22] ENISA Threat Landscape 2024 | ENISA
[23] Russian hybrid warfare: Ukraine’s success offers lessons for Europe - Atlantic Council
[24] Hybrid threats - Consilium
[25] 241007-hybrid-threats-and-hybrid-warfare.pdf
[26] ENISA Threat Landscape 2024 | ENISA
[27] ENISA Threat Landscape 2024 | ENISA
[28] Russian hybrid warfare: Ukraine’s success offers lessons for Europe - Atlantic Council
[29] 241007-hybrid-threats-and-hybrid-warfare.pdf
[30] ENISA Threat Landscape 2024 | ENISA
[31] 241007-hybrid-threats-and-hybrid-warfare.pdf
[32] Russian cyber-attacks against Nato states upby 25% in a year, analysis finds | Nato | The Guardian
[33] 241007-hybrid-threats-and-hybrid-warfare.pdf
[34] Russian hybrid warfare: Ukraine’s success offers lessons for Europe - Atlantic Council
[35] ENISA Threat Landscape 2024 | ENISA
[36] 241007-hybrid-threats-and-hybrid-warfare.pdf
[37] ENISA Threat Landscape 2024 | ENISA
[38] 241007-hybrid-threats-and-hybrid-warfare.pdf
[39] Russian hybrid warfare: Ukraine’s success offers lessons for Europe - Atlantic Council
[40] 241007-hybrid-threats-and-hybrid-warfare.pdf
[41] 241007-hybrid-threats-and-hybrid-warfare.pdf
[42] Objavljeno javno izvješće SOA-e za 2025. godinu | NCSC-HR

#HIBRIDNO RATOVANJE #IVICA MANDIĆ