Senka bezbednosti i digitalne linije fronta: Izazovi savremenog geopolitičkog poretka

April 2025.

Autor: Centar za strateške prognoze

I. Uvod: Poremećaj poretka

Početak 21. veka obeležen je iluzijom o globalnoj međuzavisnosti kao garantu stabilnosti. Danas, ravno četvrt veka kasnije, ta iluzija je urušena. Umesto svetskog poretka zasnovanog na jasno definisanim pravilima (engl. *rules-based order*), međunarodni sistem sve više liči na mozaik paralelnih zona uticaja, tehnoloških blokova i ideoloških linija razgraničenja. Bezbednost više nije pojam koji se isključivo vezuje za teritoriju, oružje ili ekonomiju, već za podatke, algoritme, infrastrukturu i kontrolu nad digitalnim prostorima.

„Senke bezbednosti" koje se nadvijaju nad svetom ove 2025. godine nisu samo metafora, već vrlo konkretna politička realnost. Naime, sajber napadi, sajber operacije, kampanje plasiranja dezinformacija, manipulacije tržištima energenata, zloupotrebe veštačke inteligencije i erozija poverenja u institucije predstavljaju novi skup instrumenata geopolitičke konkurencije. Savremeni sukobi današnjice ne vode se samo oko granica ili resursa ' već oko kontrole nad percepcijama, protokom informacija i digitalnim suverenitetom.

II. Novi oblik moći: Tehnologija kao geopolitička valuta

Tehnologija je postala najvrednija valuta geopolitike. Kontrola nad mikro-čipovima, satelitima, komunikacionim kablovima i podacima sada su osnova političke moći današnjice. Sjedinjene Američke Države, Kina i Evropska unija vode trku za tehnološku dominaciju, dok se srednje i manje sile bore za digitalnu otpornost i stratešku autonomiju.

Sjedinjene Američke Države nastoje da očuvaju svoju prednost kroz koncept „tehno-demokratije", oslanjajući se na saveze poput *Chip 4 Alliance* i inicijative za osiguravanje bezbednih lanaca snabdevanja. Kina, s druge strane, gradi sopstveni digitalni svet kroz *Digital Silk Road*, u okviru kojeg infrastruktura, telekomunikacije i veštačka inteligencija postaju instrumenti uticaja. Evropska unija nastoji da balansira, pozicionirajući se kao „normativna sila" koja teži regulaciji, etici i očuvanju i poštovanju standarda.

Ali u praksi, tehnologija više nije neutralna. Ona je postala instrument politike i sredstvo prinude. Kada Sjedinjene Američke Države ograniče izvoz naprednih poluprovodnika Kini, ili kada Peking uslovljava pristup svojim tehnološkim tržištima lojalnošću stranih partnera, mi ne govorimo o ekonomskom, već o čisto bezbednosnom činu. Geopolitika tehnologije, u tom kontekstu, postala je novi sistem hladnog rata – bez ideoloških blokova, ali sa dubokim digitalnim zidovima.

III. Sajber prostor kao nova zona sukoba

U 20. veku, tenkovi, rakete i flote predstavljali su glavne simbole moći; u 21. veku, to su serveri, algoritmi i podaci. Sajber prostor je postao novi teatar operacija u kojem se države nadmeću, bez formalnog objavljivanja rata.

Rusija i Iran koriste sajber operacije kao alate za pružanje asimetričnog odgovora na ekonomske i vojne sankcije. Severna Koreja finansira svoj nuklearni program hakovanjem tržišta kriptovalutama. Kina razvija i izvodi vrlo kompleksne operacije u sajber prostoru, bazirane na alatima iz spektra veštačke inteligncije, usmeravajući svoje napade na akademske i industrijske centre Zapada. Istovremeno, Sjedinjene Američke Države i evropski saveznici sprovode preventivne, ili pak odbrambene napade i kompleksnije i dugoročnije operacije sa ciljem neutralisanja postojećih pretnji.

Međutim, sajber prostor je suštinski nekontrolisam. Međunarodno pravo ne poznaje jasne norme kojima bi se eventualno definisao sajber suverenitet, a privatni tehnološki akteri, poput *Microsoft*, *Google*, *Palantir* ili *Huawei*, danas poseduju veću digitalnu moć nego neke države. Taj „digitalni vestfalijanski vakuum" omogućava državama i korporacijama da deluju u sivim zonama, gde granica između odbrane i agresije postaje nejasna.

Napad na evropsku energetsku infrastrukturu 2023. godine, sajber sabotaža u Iranu 2024. godine, te iznenadni prekidi komunikacionih kablova u Baltičkom i Arktičkom moru pokazali su da digitalni front zaista još uvek nije virtuelan – već ima realne ekonomske i bezbednosne posledice.

IV. Informacija kao oružje: Veštačka inteligencija i arhitektura propagande

Paralelno sa rastom sajber pretnji, odvija se i evolucija informacionog rata. Veštačka inteligencija postala je ključni alat u oblikovanju javnog mnjenja i kreiranju „stvarnosti po meni" (engl. *tailored reality*).

Sistemi zasnovani na velikim količinama podataka i obradi prirodnog jezika (engl. *natural language processing*) omogućavaju brzu i kvalitetnu izradu dezinformacionih sadržaja, sintetičkih materijala (engl. *deepfakes*) i lažnih medijskih narativa. Time se ruši granica između stvarnog i simuliranog. U aktuelnim konfliktima, poput onih koji se trenutno odvijaju u Gazi, Ukrajini, pa čak i u Sudanu, algoritmi diriguju emocijama miliona korisnika targetiranih ovim propagandnim materijalima, dok državni akteri koriste digitalne platforme kao produženu ruku strategije.

Alati iz spektra veštačke inteligencije omogućili su „masovnu personalizaciju propagande", te svaka publika dobija svoju verziju istine. To predstavlja novu vrstu strateškog rizika: društva koja izgube sposobnost da diferenciraju istinu od manipulacije postaju izrazito ranjiva iznutra, zbog čega je informaciona bezbednost postala neraskidivi deo nacionalne odbrane.

V. Energetika, infrastruktura i digitalni suverenitet

Tradicionalni pojam „energetske bezbednosti" više se ne odnosi samo na naftu i gas, već i na struju, optičke kablove, centre za zaštitu podataka (engl. *data centres*) i *cloud* sisteme. Energetska infrastruktura postala je istovremeno i fizički i digitalni cilj.

Ruski napadi na ukrajinsku elektroenergetsku mrežu, iranski pokušaji sabotaže u Saudijskoj Arabiji, kao i pojava sajber kriminala koji se izvodi protiv evropskih terminala za LNG, ukazuju načinjenicu da je integrisanost sistema i njihova ranjihost postala globalni problem.

Istovremeno, Evropa i Azija ulaze u novu fazu „digitalne infrastrukturne diplomatije". Svaka zemlja nastoji da kontroliše svoje *cloud* kapacitete, lance podataka i satelitske mreže. Ujedinjeni Arapski Emirati, Singapur i Južna Koreja razvijaju koncept „digitalnih slobodnih zona" – prostora u kojima državni nadzor i korporativna bezbednost koegzistiraju radi osiguravanja ekonomske stabilnosti.

U tom kontekstu, digitalni suverenitet postaje novi oblik energetske nezavisnosti. Onaj ko kontroliše tokove podataka, ujedno kontroliše i tokove kapitala, energije i informacija.

VI. Svet posle poretka: Povratak strategije

Globalni sistem 2025. godine ne karakteriše ni rat ni mir – već stalna nestabilnost. Svet funkcioniše u stanju strateške dvosmislenosti (engl. *strategic ambiguity*), gde konflikti nisu dovoljno otvoreni da izazovu rat, ali ni dovoljno rešivi da bi se obezbedio dugoročni mir.

U tom kontekstu, strategija se vraća u prvi plan. Međunarodni akteri pokušavaju da definišu nove ose stabilnosti, pri čemu se ističu tri ose: tehnološka, energetska i informaciona. Po pitanju tehnološke ose, prisutne su dve suprotstavljene grupe, i to osa SAD-Japan-EU, koja deluje naspram saveza na nivou Kine-Rusije-Irana. S druge strane, po pitanju grupisanja duž energetske ose, primetno je približavanje na liniji Persijski zaliv-Indija-Kina. Na kraju, formiranje informacione ose ponajviše podseća na nekadašnje blokovske podele, imajući u vidu primetno grupsanje zapadnih demokratija nasuprot autoritarnih digitalnih sistema.

Iako deluje da je čitav svet fragmentisan, indikativno je da se u njemu postepeno oblikuje nova ravnoteža – ne ona zasnovana na pravilima, već na sposobnostima. Države koje uspeju da kombinuju tehnološku inovaciju sa institucionalnom otpornošću biće pobednici novog doba.

VIII. Zaključak: Svet u senci algoritama

Globalni poredak više ne počiva na geografiji, već na podacima. Bezbedost se ne brani više samo na granicama, već i serverima, kodovima i percepcijama (ili kreiranjem istih!). Digitalni suverenitet je postao ključni preduslov političkog opstanka.

Ali svaka epoha nesigurnosti ujedno u sebi nosi i potencijal za transformaciju. Kao što je nuklearna era stvorila mehanizme kontrole naoružanja, tako bi i digitalna era mogla nametnuti novu kulturu odgovornosti – zasnovanu na transparentnosti, verifikaciji i zajedničkoj otpornosti.

Izazov leži u tome što vreme radi protiv tog procesa: tehnologija se razvija brže nego što se uspostavljaju institucije. Zbog toga će naredna decenija biti presudna – ne za kraj jednog poretka, već za definisanje novog, u kojem će algoritmi i ljudi zajedno oblikovati granice slobode i bezbednosti.