UDK: 005:004.738.5
Biblid: 0025-8555, 73(2021)
Vol. LXXIII, br. 2, str. 235–258

Pregledni rad
Primljen 24. marta 2021.
Odobren 14. juna 2021.
DOI: https://doi.org/10.2298/MEDJP2102235V

Problemi i izazovi upravljanja internetom na međunarodnom nivou

Dejan VULETIĆ, Branislav ĐORĐEVIĆ[1]

Apstrakt: U radu su razmatrani subjekti upravljanja internetom, aktivnosti Ujedinjenih nacija kao najznačajnije međunarodne organizacije ali i napori određenih regionalnih i nacionalnih organizacija. Posebna pažnja u radu je posvećena „internet stvarima", čija sve masovnija upotreba uzrokuje nastanak novih, opasnijih i ozbiljnijih pretnji, čime se dodatno komplikuje problem upravljanja Internetom. Iskazani predmet istraživanja je u direktnoj vezi sa ciljem rada koji se odnosi na prikaz i analizu aktivnosti različitih subjekata, međunarodnih, regionalnih i nacionalnih institucija i organizacija kao i vodećih država, pre svih Sjedinjenih Američkih Država i Rusije, i dokumenata kojima pokušavaju da urede aktivnosti u sajber prostoru. Osnovna hipoteza je da suprotstavljeni nacionalni interesi ne dozvoljavaju postizanje koncenzusa oko osnovnih principa upravljanja internetom u okviru međunarodnih tela, pre svih u Organizaciji ujedinjenih nacija, što ima za posledicu povećanje nebezbednosti u smislu sve učestalijih, raznovrsnijih i ozbiljnijih pretnji na Internetu i sajber prostoru uopšte. Na osnovu iznete argumentacije u radu, mogu se videti brojni pokušaji regulisanja upravljanja internetom koji nisu materijalizovani kroz konkretne odluke koje se mogu implementirati u nacionalna zakonodavstva i praksu. Usled sve veće zavisnosti od informaciono-komunikacionih tehnologija problem nepostojanja regulative u ovoj oblasti čini informaciono društvo dodatno ranjivim.

Ključne reči: internet, sajber prostor, internet stvari, ranjivosti, upravljanje, bezbednost.

---

[1] Dr Dejan Vuletić je naučni saradnik u Institutu za strategijska istraživanja Univerziteta odbrane, Beograd.

E-pošta: dejan.vuletic@mod.gov.rs

Dr Branislav Đorđević je redovni profesor u Institutu za međunarodnu politiku i privredu, Beograd.

Rad je nastao u okviru naučnoistraživačkog projekta „Srbija i izazovi u međunarodnim odnosima 2021. godine", koji finansira Ministarstvo prosvete, nauke i tehnološkog razvoja Republike Srbije, a realizuje Institut za međunarodnu politiku i privredu tokom 2021. godine.

Subjekti upravljanja internetom

Napredak u razvoju informaciono-komunikacione tehnologije doneo je revolucionarne promene širom sveta. Informaciono-komunikaciona tehnologija utiče na svaki aspekt života pojedinaca i zajednica, na odnose između država ali i njihovu bezbednost. Internet (međunarodna mreža, eng. *INTERnational NETwork*) kao najveća svetska računarska mreža („mreža svih mreža") nastao je kao posledica tehnološkog napretka. Usled sve većeg značaja interneta za moderno društvo, privilegovana uloga Sjedinjenih Američkih Država po pitanju upravljanja internetom sve je češće predmet sporenja u međunarodnih zajednici. U različim pokušajima da se promeni način upravljanja internetom najaktivniju ulogu u međunarodnim i regionalnim organizacijama imala je Rusija, a u poslednje vreme sve češće i Kina. Upravljanje internetom postaje sve više ekonomsko, bezbednosno, političko, socijalno odnosno pitanje od nacionalnog interesa.

Od nastanka interneta do danas, američka vlada uključena je u upravljanje preko raznih ministarstava i agencija – Ministarstva odbrane, kasnije Nacionalne fondacije za nauku, a u novije vreme Ministarstva trgovine (Kurbalija 2011, 167–168). U praksi se često kao sinonim za internet, ali i digitalni svet uopšte, koristi sintagma „*cyber* prostor" (Tipton and Krause 2004, 3171). Upravljanje internetom podrazumeva razvoj i primenu zajedničkih principa, normi, pravila i postupaka pri donošenju odluka i programa koji oblikuju promene i upotrebu interneta, od strane vlada, privatnog sektora i civilnog društva (UN WGIG Rep. 05.41622/2015).

Postoji više subjekata upravljanja internetom, na globalnom nivou, kao što su:

- Države (vlade) – pitanja javne politike u vezi interneta;
- Privatni sektor (kompanije) – razvoj Interneta u tehničkoj i ekonomskoj oblasti;
- Civilno društvo (nevladine organizacije) – zastupanje interesa svih pripadnika internet zajednice;
- Međuvladine organizacije – koordinacija pitanja državne politike vezano za internet;
- Internet organizacije – upravljanje i razvoj tehničkih standarda i politika vezano za internet;
- Akademske organizacije – naučno-istraživački aspekt tehničkog i administrativnog upravljanja internetom.

Najvažnije globalno telo koje se bavi pitanjima upravljanja internetom je Forum za upravljanje internetom (*Internet Governance Forum* – IGF). Forum je uspostavljen na Svetskom samitu o informacionom društvu 2005. godine u Tunisu i saziva ga generalni sekretar Ujedinjenih nacija. Od formiranja Foruma, održano

je više sastanaka posvećenih problemima upravljanja internetom, prevazilaženju digitalnih podela, informacionoj bezbednosti i drugim srodnim temama.

Jedna od glavnih tema trinaestog sastanka Foruma za upravljanje internetom, održanog u Parizu novembra 2018. godine, bila je „Evolucija upravljanja internetom". U izveštaju se navodi da je upravljanje internetom dostiglo fazu u kojoj se suočavamo sa sve većim brojem nacionalnih zakona ili regionalnih pravnih instrumenata koji se primenjuju na javnu politiku interneta (IGF 2018). Te fragmentirane regulatorne politike među državama mogu se odraziti negativno na internet kao globalnu mrežu. Istaknuto je da postoji potreba da globalna zajednica, uključujući Forum za upravljanje internetom, osmisli niz univerzalnih vrednosti i standarda kao i globalno priznati okvir koji će podržati harmonizaciju individualnih nacionalnih pristupa. Pored toga, pružaoci usluga na mreži moraju da poštuju principe o neutralnosti mreže. Za Forum za upravljanje internetom je imperativ da internet ostane slobodan, otvoren i siguran za sve. S obzirom na kompleksnost problematike, uključivanje svih sektora je od naročite važnosti za pronalaženje efikasnih rešenja. To je razlog zašto je model više zainteresovanih strana još važniji za diskusiju o upravljanju internetom (IGF 2018).

U kontekstu proširenja učešća zainteresovanih strana u upravljanju internetom, na tom sastanku Foruma za upravljanje internetom je konstatovano sledeće:

- Postoji potreba za standardizovanim setom principa primenljivih na upravljanje internetom radi unapređenja ljudskih prava i postizanja održivog razvoja;
- Menjaju se načini na koji dobavljači i operatori internet usluga mogu uticati na upravljanje internetom i na njegove osnovne principe;
- Izraz „internet upravljanje" se smatra neprivlačnim i teško ga je smisleno prevesti na neke jezike. Od zainteresovanih strana se zahteva da pojasne korišćenu terminologiju i prilagode je aktivnostima;
- Zainteresovane strane imaju različite uloge na internetu. Za povećan angažman zainteresovanih strana važno je objasniti različitim akterima da priroda interneta zahteva da se uključe sve discipline i da će svi imati koristi od razvoja dobrih internet politika;
- Procesi angažovanja zainteresovanih strana moraju se sprovoditi na nacionalnom, regionalnom i globalnom nivou kako bi se postiglo uključivanje svih relevantnih subjekata;
- Izgradnja kapaciteta može se izvršiti i kroz edukaciju o upravljanju internetom;
- Forum za upravljanje internetom treba da obuhvati subjekte koji tradicionalno nisu bili uključeni u upravljanje internetom;

- Saradnju među nacionalnim, regionalnim i drugim forumima treba poboljšati deljenjem najboljih praksi i koordinacijom vremena održavanja sastanaka i drugih događaja;
- Model više zainteresovanih strana mora da uključi mnoge subjekte, uzimajući u obzir brzi rast korisnika interneta gde se procenjuje da će dve trećine korisnika u budućnosti biti iz zemalja u razvoju. Ti korisnici moraju biti uključeni u postojeće procese, jer će se eventualni dogovoreni model odnositi i na njih;
- Potrebno je koristiti i razviti efikasne alate kako bi se olakšale interakcije na internetu;
- Pojačan dijalog i saradnja između relevantnih aktera neophodni su za diskusiju o neutralnosti mreže na globalnom nivou;
- Pitanja upravljanja internetom odražavaju ljudska prava. Sloboda govora dovodi do brojnih lažnih informacija na internetu. Zaključeno je da bi trebalo da postoji harmonizovan skup rešenja za borbu protiv te prakse, a ne sporadične mere;
- Nacionalni zakoni o internetu su sve brojniji. Trebalo bi uspostaviti međunarodni okvir i skup dogovorenih principa da se izbegne nedosledna praksa.

Glavne teme četrnaestog sastanka, održanog u martu 2019. godine u Berlinu, bile su upravljanje podacima, digitalna inkluzija i bezbednost, stabilnost i otpornost. Na sastanku je, između ostalog, konstatovano da postojeći model upravljanja internetom povlašćuje nekoliko velikih tehnoloških kompanija. Konstatovano je da su pojedinci, kao i manje kompanije i zemlje u razvoju, isključeni iz deljenja i koristi od velike količine podataka, a istovremeno su ranjivi na različite zloupotrebe i napade na njihovu privatnost (IGF 2019). Sastanak Foruma za upravljanje internetom, petnaesti po redu, realizovan je *online*, i na njemu je, pre svega, bilo reči o prevazilaženju digitalnih podela i upotrebi interneta za veću solidarnost i podršku očuvanju zdravlja i života ljudi u vreme pandemije izazvane virusom COVID-19 (IGF 2020).

Rad Foruma za upravljanje internetom podržale su vodeće sile i pojedine regionalne organizacije. Rezolucijom Evropskog parlamenta se poziva Generalna skupština Ujedinjenih nacija da osnaži resurse i kapacitete Foruma za upravljanje internetom i očuva model upravljanja internetom sa više subjekata. Države članice i relevantne institucije Evropske unije se pozivaju da nastave sa podrškom Forumu za upravljanje internetom. Takođe, od članica Evropske unije i Komisije se očekuje da ulože više napora u podršci modela upravljanja internetom koji uključuje više subjekata. Pravna zaštita otvorenog interneta i ideja neutralnosti mreže su od izuzetne važnosti kada se razmatra upravljanje internetom (EP Res. 2015/2526[RSP]).

Forum za upravljanje internetom se smatra jedinstvenom platformom pod pokroviteljstvom Ujedinjenih nacija, što omogućava pojedincima i zainteresovanim

grupama da razgovaraju o pitanjima upravljanja internetom. Međutim, Forum za upravljanje internetom trebalo bi da ide u korak sa tehnološkim inovacijama kako bi ostao relevantan u današnjim trendovima brzog razvoja i prihvatanju novih tehnologija. Zbog toga, Forum za upravljanje internetom mora da nastavi da radi na poboljšanju svojih procesa, jačanjem zajednica više zainteresovanih strana na nacionalnom i regionalnom nivou i uspostavljanjem saradnje među njima na globalnom nivou, kao i sa drugim srodnim forumima i institucijama (IGF 2018).

Vodeća organizacija u upravljanju internetom, u tehničkom smislu, jeste Internet korporacija za dodeljene nazive i brojeve (*Internet Corporation for Assigned Names and Numbers* – ICANN). Njena uloga je često osporavana od određenih svetskih i regionalnih sila, pre svih Rusije. Internet korporacija za dodeljene nazive i brojeve je odgovorna za rukovođenje globalnom strukturom interneta (IP adresama, nazivima domena, numeričkim oznakama protokola i glavnim DNS serverima).[2] Funkcionalna ovlašćenja Internet korporacije za dodeljene nazive i brojeve počivala su na Memorandumu o razumevanju sa Ministarstvom trgovine Sjedinjenih Američkih Država, koji je potpisan 1998. godine i dva puta produžavan. Od 1. oktobra 2009. godine formalni osnov za funkciju Internet korporacije za dodeljene nazive i brojeve predstavlja Izjava o obavezama koju su potpisali Internet korporacija za dodeljene nazive i brojeve i Ministarstvo trgovine Sjedinjenih Američkih Država. Taj dokument predstavlja dobru osnovu za nezavisnost i samostalnost u radu Internet korporacija za dodeljene nazive i brojeve (Kurbalija 2011, 175–176). Internet korporacije za dodeljene nazive i brojeve rukovodi strukturom interneta, ali nema ovlašćenja nad drugim aspektima upravljanja internetom, kao što su sajber bezbednost, politika sadržaja, zaštita autorskih prava, zaštita privatnosti, održavanje kulturne raznolikosti ili prevazilaženje digitalnih podela.

Internet korporacija za dodeljene nazive i brojeve se smatra – sa stanovišta Rusije, Kine i još nekih država – američkom organizacijom, odnosno institucijom pomoću koje Sjedinjene Američke Države ostvaruju svoje interese kroz tehnička rešenja, pravila i norme koje se tiču interneta. Rusija zagovara ideju da mnoge aspekte koje danas reguliše Internet korporacija za dodeljene nazive i brojeve treba da preuzme Međunarodna unija za telekomunikacije (*International Telecommunication Union* – ITU) kao specijalizovana agencija Ujedinjenih nacija. Rusija svoje ideje nastoji da realizuje kroz aktivnosti u okviru Ujedinjenih nacija i regionalne organizacije kao što su Šangajska organizacija za saradnju, Organizacija Ugovora o kolektivnoj bezbednosti (ODKB) i grupacija BRIKS.

---

[2] *Domain Name System* (DNS) u osnovi predstavlja sistem koji pretvara imena računara u logičke, IP adrese. DNS je zasnovan na hijerarhijskom principu i jedna je od osnovnih komponenti interneta.

Inicijative u Ujedinjenim nacijama

U Rezoluciji Ujedinjenih nacija A/RES/74/197 se navodi da bi upravljanje internetom trebalo da bude u skladu sa odredbama Samita o informacionom društvu, održanog u dve faze, u Ženevi i Tunisu. U dokumentu se naglašava potreba za većim učešćem vlada i relevantnih subjekata iz svih zemalja u razvoju, posebno manje razvijenih zemalja, na svim sastancima Foruma za upravljanje internetom i pozivaju se države članice, kao i drugi relevantni subjekti, da uzmu učešće u radu Foruma i na pripremnim sastancima (UNGA Res. A/RES/74/197).

Dijalog u Ujedinjenim nacijama o kontroli naoružanja i informaciono-komunikacionoj tehnologiji datira iz kraja devedesetih godina prošlog veka. Usled sve veće upotrebe informaciono-komunikacionih tehnologija, Rusija je 1998. godine odlučila da pitanje pretnji miru i bezbednosti informaciono-komunikacionih tehnologija postavi Prvom komitetu Generalne skupštine Ujedinjenih nacija (*First Committee of the UN General Assembly*), čiji je delokrug rada razoružanje i međunarodna bezbednost. To je na kraju rezultiralo formiranjem Grupe vladinih eksperata (*Group of governmental experts* – GGE) iz oblasti informacija i telekomunikacija u kontekstu međunarodne bezbednosti (Eneken 2019).

Posle više od dve decenije razmatranja malo je zajedništva između država po pitanju stavova o prirodi pretnji i merama potrebnim za njihovo rešavanje. Rasprave u Ujedinjenim nacijama karakterišu različiti pristupi o upotrebi i regulaciji upotrebe interneta i informaciono-komunikacionih tehnologija uopšte. Dva najuticajnija stanovišta su iz Rusije i Sjedinjenih Američkih Država, koje toj problematici pristupaju iz različitih perspektiva. Rusija želi da kontroliše protok informacija unutar državnih granica i zalaže se za multilateralni regulatorni postupak radi upotrebe informaciono-komunikacionih tehnologija u vojne, terorističke i kriminalne svrhe. Sjedinjene Američke Države zastupaju stanovište da na međunarodnom nivou nema potrebe za dodatnom regulacijom, jer je upotreba informaciono-komunikacionih tehnologija od strane država regulisana međunarodnim pravom. Udaljenost ruskog i američkog stanovišta predstavlja prepreku napretku na nivou Ujedinjenih nacija i odražava se na podele u pozicijama različitih država (Nocceti 2015, 122–126).

Nedvosmisleno sagledavanje obima i karakteristika sajber napada sponzorisanih od strane države mogu biti teški jer većini zemalja nedostaju nezavisne sposobnosti za efikasno otkrivanje i dokazivanje. Situaciju dodatno komplikuje činjenica da su informaciono-komunikacione tehnologije dostupne svima, a mreže su većim delom u vlasništvu i upravljanju privatnog sektora, što otežava vladama kontrolu nad njihovom upotrebom. U velikom broju slučajeva se

upravo ta činjenica koristi kao izgovor odgovornih državnih autoriteta u slučaju incidenata u sajber prostoru (UNGA Rep. A/66/152). Rusija i Sjedinjene Američke Države nisu spremne da daju bilo kakve garancije da neće izvoditi sajber operacije koje ostaju ispod praga upotrebe sile. To ostavlja ogromnu većinu sajber operacija između država, poput špijunaže, uskraćivanja usluga i uništavanja podataka, bez dijaloga. Sajber kriminal, upotreba informaciono-komunikacionih tehnologija u terorističke svrhe, upravljanje internetom, nadzor, privatnost i druga pitanja ljudskih prava isključeni su iz fokusa dijaloga Sjedinjenih Američkih Država i Rusije.

Na sastancima Grupe vladinih eksperata razmatrano je 2016. i 2017. godine kako se međunarodno pravo primenjuje na upotrebu informaciono-komunikacionih tehnologija od strane država. Međutim, nespojivi nacionalni interesi onemogućili su postizanje konsenzusa i kao rezultat toga nije mogao da se objavi zajednički izveštaj.

U 2018. godini usvojene su dve nove rezolucije Generalne skupštine Ujedinjenih nacija. Rezolucija Generalne skupštine Ujedinjenih nacija iz 2018. godine sadrži izbor normi, pravila i principa koje preporučuje Grupa vladinih eksperata. Formirana je Radna grupa otvorenog tipa (*Open-Ended Working Group* – OEWG) koja se bazira na radu ranijih Grupa vladinih eksperata. Radna grupa otvorenog tipa je sazvala diplomatske predstavnike kako bi se razmotrila mogućnost uspostavljanja redovnog institucionalnog dijaloga sa širokim učešćem pod okriljem Ujedinjenih nacija (UNGA Res. A/73/27). Rusija je bila pokrovitelj tog procesa. Opredeljenje Rusije je da pregovarački proces Ujedinjenih nacija o bezbednosti upotrebe informaciono-komunikacionih tehnologija učini demokratičnijim i transparentnijim. Cilj Rusije je formiranje međunarodnog sistema bezbednosti informacija (Doctrine RF No. 646/2016). Rusija zastupa stanovište da sistem bezbednosti informacija mora biti formiran na osnovu opštepriznatih principa i pravila međunarodnog prava, kao što su poštovanje nacionalnog suvereniteta, sprečavanje upotrebe ili pretnja silom u međunarodnim odnosima i pravo država na individualnu i kolektivnu odbranu.

Sjedinjene Američke Države su bile strogo protiv sadržaja i formata rezolucije. U skladu sa tim, Sjedinjene Američke Države su pokrenule posebnu rezoluciju Generalne skupštine o Unapređenju odgovornog ponašanja države u sajber prostoru u kontekstu međunarodne bezbednosti (*Advancing responsible state behaviour in cyberspace in the context of international security*). Ta rezolucija predstavlja nadogradnju procena i preporuka ranijih izveštaja Grupe vladinih eksperata. U rezoluciji se preporučuje da se nastavi sa iznalaženjem modela saradnje u informacionoj sferi. Takva zajednička razumevanja mogu da uključuju

> (...) norme, pravila i principe odgovornog ponašanja država, mere za izgradnju poverenja i izgradnju kapaciteta, kao i primenu međunarodnog prava po pitanju

upotrebe (zloupotrebe) informaciono-komunikacionih tehnologija od strane država (UNGA Res. 73/266).

U Sjedinjenim Američkim Državama se posebno naglašava pravo na kontramere i samoodbranu u slučaju sajber napada (U.S. S/CCI Recommendations).

Na sastanku Grupe vladinih eksperata su pokrenuta brojna pitanja kao što su nedostatak nacionalnog kapaciteta, nedostatak otpornosti i odsustvo zajedničkog razumevanja, potencijala i prednosti informaciono-komunikacionih tehnologija. Na taj način je okupljena međunarodna zajednica oko dijaloga, jer su mnoge države izražavale zabrinutost zbog mogućeg negativnog uticaja informaciono-komunikacionih tehnologija na njihovu nacionalnu bezbednost.

Izveštaji Grupe vladinih eksperata su značajni i po tome što sadrže dva različita pogleda vezano za upotrebu informaciono-komunikacionih tehnologija. Prvi, sa Zapada, veću upotrebu informaciono-komunikacionih tehnologija posmatra kao pozitivnu činjenicu, da je postojeće međunarodno pravo dovoljno i ne zahteva posebne regulative. Drugi stav, iz grupe zemalja predvođenih Kinom i Rusijom, digitalizaciju smatra pretnjom i preferira nove normativne smernice o razvoju i upotrebi informaciono-komunikacionih tehnologija. Već dugi niz godina izveštaji Grupe vladinih eksperata su uokvireni i formulisani na takav način da su se mogla prihvatiti oba pogleda. Kao rezultat toga, izveštaji su pružili malo normativnih smernica međunarodnoj zajednici (UNGA Res. A/RES/74/197; UNGA Res. A/73/27; UNGA Res. 73/266).

Sajber bezbednost je postala vitalno polje koje utiče na sve aspekte svakodnevnog života ali i na bezbednost kritične infrastrukture svake države. Usvajanje međunarodnih standarda zasnovanih na konsenzusu, kako bi se osiguralo da se sajber prostor ne koristi u destruktivne svrhe koje narušavaju međunarodni mir i bezbednost, jedno je od najvažnijih pitanja sa kojima se Ujedinjene nacije danas suočavaju. Strategija generalnog sekretara Ujedinjenih nacija za nove tehnologije (*The UN Secretary-General's Strategy on New Technologies*) ističe povećan obim i rasprostranjenost pretnji i aktera na međunarodnom nivou u sajber prostoru. Cilj Strategije je da definiše kako će Ujedinjene nacije da podrže upotrebu novih tehnologija kako bi se ubrzalo postizanje Agende održivog razvoja 2030 (*2030 Sustainable Development Agenda*) i olakšalo njeno usklađivanje sa vrednostima sadržanim u Povelji Ujedinjenih nacija, Univerzalnoj deklaraciji o ljudskim pravima kao i drugi međunarodnim normama i standardima (UNGA SG Strategy).

Političke i tehničke poteškoće u pripisivanju odgovornosti za sajber napade podstiče aktere da zauzmu ofanzivan stav, ne samo kada su države u pitanju, već i nedržavni akteri, kriminalne grupe i pojedinci. Takva situacija bi mogla da oslabi i ugrozi savremenu međunarodnu bezbednosnu arhitekturu. U pomenutoj Strategiji

se ističe da su mnoge tehnologije dizajnirane, razvijane i implementirane u infrastrukturi i oblastima koje su u nadležnosti pojedinačnih država. Primarna odgovornost vlada i njihovih društava je kako da maksimalno iskoriste nove tehnologije uz minimiziranje rizika (UNGA SG Strategy). Panel o digitalnoj saradnji na visokom nivou (*High-level Panel on Digital Cooperation*), koji je Generalni sekretar Ujedinjenih nacija Antonio Gutereš (Antonio Guterres) osnovao u julu 2018. godine, mogao bi da postane glavna platforma međunarodnog dijaloga o odnosu novih tehnologija i međunarodnog razvoja, mira, stabilnosti i bezbednosti (UNGA SG Strategy).

Bez obzira na nivo operativnih sposobnosti i interesa, postoji snažan argument da odgovornost za sajber bezbednost u državi ostaje u potpunosti na toj državi. Primarna odgovornost za bezbednost je na državama odakle je napad izvršen kao i na preduzimanju mera zaštite od takvih napada. Bez nacionalnih strategija, vlade ostavljaju svoje stanovništvo i informaciono-komunikacione sisteme „širom otvorenim" za strani uticaj. Do sada je preko sto država usvojilo nacionalne politike i strategije informacione ili sajber bezbednosti koje se fokusiraju na razvoj nacionalnih kapaciteta (pravni i institucionalni okviri), sposobnosti i mehanizama koji, između ostalog, štite kritičnu infrastrukturu i regulišu suprotstavljanje sajber kriminalu, razvijaju veštine i kompetencije (Kerttunen and Tikk 2019, 1–14).

Svetski samit o informacionom društvu (*World Summit on the Information Society* – WSIS) WSIS+10, koji je koordinisala Međunarodna unija za telekomunikacije Ujedinjenih nacija, odvijao se u saradnji sa svim organima i agencijama Ujedinjenih nacija u okviru svojih mandata, u skladu sa Rezolucijom 1334 Saveta Međunarodne unije za telekomunikacije. Deset godina ranije, na Svetskom samitu o informacionom društvu, u njegove dve faze (Ženeva 2003. i Tunis 2005. godine), usvojena je zajednička vizija o informacionom društvu, identifikujući njegove glavne principe i izazove. Osnovni cilj Svetskog samita o informacionom društvu bio je podsticanje upotrebe tehnologije za poboljšanje života ljudi i premošćavanje digitalne razlike.

Kao prioritetno područje koja treba rešiti u sprovođenju Ženevskog akcionog plana posle 2015. godine (*Geneva Plan of Action Beyond 2015*) je „pomoć zemljama u razvoju da prošire širokopojasnu infrastrukturu i preduzmu mere za poboljšanje kvaliteta, povezanosti i otpornosti računarskih mreža, podstiču konkurenciju i smanjuju troškove lokalnih, nacionalnih, regionalnih i međunarodnih komunikacija, uključujući pružanje lokalnog sadržaja i lokalnih elektronskih usluga u tim zemljama u većoj meri". Efikasno učešće vlada i svih drugih zainteresovanih strana je od vitalnog značaja za razvoj informacionog društva kroz inkluzivni angažman i saradnju, čime se obezbeđuje održiva, sveobuhvatna i bezbedna upotreba informaciono-komunikacionih tehnologija (UN-ITU WSIS+10 2014).

Inicijative regionalnih i međunarodnih organizacija

Pojedine regionalne organizacije, kao što su Evropska unija, Savet Evrope, OEBS, NATO i Savez država jugoistočne Azije realizuju brojne aktivnosti i usvajaju regulative sa ciljem da se unapredi bezbednost interneta (sajber prostora).

U Strategiji sajber bezbednosti Evropske unije (*Cybersecurity Strategy of the European Union*) ističe se da je internet bez granica i višeslojni internet postao jedan od najmoćnijih instrumenata za globalni napredak. U Strategiji se naglašava da privatni sektor i dalje treba da igra vodeću ulogu u izgradnji i upravljanju internetom. Potreba za transparentnošću, odgovornošću i sigurnošću postaje sve izraženija kao i zahtev da digitalnim svetom ne upravlja niti jedan entitet, već da ga karakteriše demokratsko i efikasno upravljanje više zainteresovanih subjekata. Trenutno ima nekoliko zainteresovanih subjekata, od kojih su mnogi komercijalni i nevladini, koji su svakodnevno uključeni u upravljanje internet resursima, protokolima i standardima interneta. Evropska unija naglašava važnost svih aktera na trenutnom modelu upravljanja internetom (EC CSEU 2013).

Uredba o sajber bezbednosti Evropske unije ima za cilj da ojača sposobnost Agencije Evropske unije za mrežu i informacionu bezbednost (*European Union Agency for Cybersecurity* – ENISA) kako bi se pomoglo državama članicama da se izbore sa pretnjama u sajber prostoru i da se uspostavi okvir sajber bezbednosti u okviru Evropske unije u kojem će Agencija Evropske unije za mrežu i informacionu bezbednost imati ključnu ulogu (Regulation [EU] No. 2019/881). Direktiva o bezbednosti mreža i informacionih sistema (*Directive on security of network and information systems* – NIS Directive) je deo zakonodavstva o sajber bezbednosti u Evropskoj uniji. Predstavlja pravni okvir za povećanje opšteg nivoa sajber bezbednosti u Evropskoj uniji. Članom 23. se zahteva od Evropske komisije da se periodično vrši evaluacija i procena efikasnosti primene Direktive (Directive [EU] No. 2016/1148). Direktiva predviđa zakonske mere za povećanje nivoa sajber bezbednosti u Evropskoj uniji obezbeđujući:

Spremnost država članica od kojih se zahteva da budu adekvatno opremljene i da imaju odgovarajuće timove, npr. računarski tim za odgovor na incidente (*Computer Incident Response Team*);

Kooperativnost svih država članica osnivanjem grupe za saradnju u cilju podrške i olakšavanja strateške saradnje i razmene informacija između država članica. Na taj način obezbediće se brza i efikasna operativna razmena informacija o određenim incidentima u vezi sa sajber bezbednošću i aktuelnim rizicima;

Bezbednosnu kulturu u sektorima koji su od vitalnog značaja za ekonomiju i društvo i koji se u velikoj meri oslanjaju na informaciono-komunikacione

tehnologije, poput energije, transporta, vode, bankarstva, infrastrukture finansijskog tržišta, zdravstvene zaštite i digitalne infrastrukture. Kompanije iz sektora koje su države članice identifikovale kao operatore najvažnijih usluga u društvu moraće da preduzmu odgovarajuće mere zaštite i da o ozbiljnim incidentima prijave relevantnim nacionalnim organima. Takođe, ključni dobavljači digitalnih usluga moraće da se pridržavaju propisanih bezbednosnih mera i imaće obavezu izveštavanja, prema navedenoj Direktivi.

U Strategiji Saveta Evrope o upravljanju internetom (*Internet governance – Council of Europe strategy 2016–2019*) navodi se da svaki građanin treba da bude zaštićen od kriminala i nesigurnosti na mreži kao i od nezakonitog nadzora nad njihovim aktivnostima. Građani treba da budu slobodni da komuniciraju bez cenzure ili ometanja, da se osećaju sigurno u deljenju ličnih podataka, kreiranju sadržaja i *online* aktivnostima. Internet treba da ostane univerzalan, inovativan i da dalje služi interesima korisnika. To je globalni resurs koji treba zaštititi i njime upravljati u javnom interesu (CoE IGS 2016). Strategija naglašava pitanja koja se tiču sadržaja, usluga i uređaja povezanih na internet, uključujući relevantne aspekte njegove infrastrukture i funkcionisanja koji mogu uticati na ljudska prava i slobode. Strategija identifikuje mnoge izazove vezane za internet i pruža smernice za vlade i ostale zainteresovane strane, uključujući civilno društvo, privatni sektor, tehničku i akademsku zajednicu.

Evropski dijalog o upravljanju internetom (*European Dialogue on Internet Governance* – EuroDIG) otvorena je platforma više zainteresovanih strana za razmenu mišljenja o upravljanju i drugim aspektima vezanim za internet. Osnovan je 2008. godine od strane nekoliko organizacija, predstavnika vlada i eksperata. Podstiče dijalog i saradnju sa brojnim subjektima o javnoj politici interneta. Održava se jednom godišnje, u nekom od glavnih gradova različitih država. Poruke se pripremaju i predstavljaju na Forumu za upravljanje internetom pod vođstvom Ujedinjenih nacija. *EuroDIG* je podržan od strane grupe institucionalnih partnera: Saveta Evrope, Evropske komisije (*European Commission*), Internet društva (*Internet Society* – ISOC), Evropske regionalne organizacije (*European Regional At-Large Organization* – EURALO), Evropske radiodifuzne zajednice (*European Broadcasting Union* – EBU), Koordinacionog mrežnog centra (*RIPE Network Coordination Centre* – RIPE NCC) i Saveznog ureda za komunikacije Švajcarske (*Federal Office of Communications of Switzerland* – OFCOM) (CoE IGS 2016).

Organizacija za evropsku bezbednost i saradnju (OEBS) usvojila je tokom 2013. i 2016. godine skup mera (*Confidence-Building Measures* – CBMs) radi smanjenja rizika nastalih upotrebom informaciono-komunikacionih tehnologija (OSCE Decision No. 1106/2013). Analizom implementacije mera od strane država za 2016. godinu utvrđena je visoka stopa implementacije mera u nordijskim zemljama i

naglašena je uloga timova za reagovanje na incidente u izgradnji poverenja (OSCE Decision No. 1202/2016). Naglašena je važnost mera kao što su razmena informacija o pretnjama, saradnja između državnih organa za sajber bezbednost, konsultacije o riziku, deljenje informacija, zajedničko jačanje kapaciteta i transparentnost u nacionalnim politikama i zakonodavstvu.

NATO je preduzeo odlučan potez u razvoju sposobnosti za sajber operacije jer sajber prostor posmatra kao jedan od domena sukoba, sa izazovima i pretnjama iz svih strategijskih pravaca. NATO je formirao Operativni centar za sajber prostor u Monsu u Belgiji (NATO Cyber Defence 2020). Imajući u vidu razlike u primeni međunarodnog prava u sajber prostoru među državama članicama, NATO će se suočiti sa izazovima međusobnog usklađivanja regulative zemalja članica. Sajber bezbednost je takođe područje saradnje NATO i Evropske unije (NATO Declaration No. 095/2018).

Savez država jugoistočne Azije (*Association of Southeast Asian Nations* – ASEAN) preduzeo je brojne korake za poboljšanje sajber bezbednosti u regionu i naročito za poboljšanje nacionalnih resursa. U kontekstu razvoja normi, Singapur je preuzeo vodeću ulogu u sprovođenju preporuka Grupe vladinih eksperata i u razvoju specifičnih normi. U 2018. godini čelnici Saveza država jugoistočne Azije pojačali su napore da sarađuju u vezi sve većeg broja sajber incidenata (ASEAN 2018).

Pored napora regionalnih organizacija, značajan doprinos bezbednosti interneta daju i određene nacionalne i korporativne aktivnosti. Londonski proces je serija globalnih konferencija o sajber prostoru koji se održavaju dvogodišnje, počev od 2011. godine. Na tim događajima se okupljaju predstavnici vlada, privatnog sektora i civilnog društva kako bi razgovarali i promovisali praktičnu saradnju u sajber prostoru, unapredili izgradnju sajber kapaciteta i razmotrili norme za odgovorno ponašanje u sajber prostoru. Značajan doprinos bezbednosti interneta pružaju i svetske konferencije posvećene internetu koje se periodučno održavaju u Vuženu u Kini. Globalni forum o sajber ekspertizi (*The Global Forum on Cyber Expertise*), osnovan u Hagu, globalna je platforma za države, međunarodne organizacije i kompanije iz privatnog sektora radi razmene najboljih praksi i ekspertiza o izgradnji sajber kapaciteta.

Francuska promoviše svoj međunarodni program sajber bezbednosti. Od novembra 2018. godine, više od 60 država, uključujući sve države članice Evropske unije obećalo je podršku novom međunarodnom sporazumu o uspostavljanju standarda za sajber oružje i upotrebu interneta, potpisivanjem Pariškog poziva za poverenje i bezbednost u sajber prostoru (*Paris Call for Trust and Security in Cyberspace*) (Paris Call 2018). Rusija, Kina i Sjedinjene Američke Države nisu među potpisnicama navedenog sporazuma.

Američka tehnološka kompanija *Microsoft* sponzorisala je proces promocije Digitalne ženevske konvencije (*Digital Geneva Convention*). Konvencijom se pozivaju države da „u vreme mira štite civile na internetu" i da se države obavezuju da neće napadati civilnu infrastrukturu. Iako ova inicijativa nije dobila podršku američke vlade, privukla je pažnju nekih država i dovela do istrage određenih incidenata u sajber prostoru (Jeutner 2019, 158-170).

„Internet stvari"

Napredak u razvoju informaciono-komunikacionih tehnologija, uz smanjenje troškova i povećanje performansi različitih uređaja doveli su do pojave „internet stvari" (*Internet of Things*). Uređaji spojeni na internet nisu nova pojava. Ta ideja stara je koliko i sam internet. Prvi takvi uređaji počeli su se pojavljivati osamdesetih godina prošlog veka. Ipak, prošlo je dosta vremena do početka masovnog povezivanja određenih, manje važnih, uređaja poput sistema za kontrolu garažnih vrata, na internet. Ovu promenu omogućila su dva značajna tehnološka napretka u području mrežnih tehnologija, to jest, samog interneta: širokopojasni (*Broadband*) pristup internetu i internet protokol verzije 6 (*Internet Protocol version 6 - IPv6*). Problem brzine, odnosno slanja velike količine podataka preko interneta rešen je uvođenjem širokopojasnog interneta. Drugi važan napredak, koji je omogućio razvoj „internet stvari" je postepeni prelazak na *IPv6*. Prethodna verzija internet protokola nije omogućavala povezivanje velikog broja uređaja na internet (Filipović i dr. 2019, 809–810). Za početak razvoja „internet stvari" veliku ulogu ima upotreba tehnologije radio-frekventne identifikacije (*Radio-Frequency Identification* – RFID).[3]

„Internet stvari" se sastoje se od hardvera i softvera koji mogu da komuniciraju bez ljudske intervencije odnosno komunikacija se ostvaruje od mašine do mašine (*machine to machine* – M2M). Ljudski faktor je svakako uključen, tako da pouzdanost hardvera nije vezana samo za pouzdanost softvera već i za pouzdanost ljudstva. Elektronska minijaturizacija, troškovi elektronskih komponenata i trend ka bežičnoj komunikaciji su tri glavna pokretačka faktora „internet stvari" (Filipović i dr. 2019, 809–810). Zbog izuzetno velike količine podataka (*Big Data*) koje senzori prikupljaju, oni se u velikom broju slučajeva skladište i obrađuju u oblaku (*Cloud*). *Cloud computing* ili „računarstvo u oblaku" je platforma koja putem interneta korisnicima isporučuje različite podatke i aplikacije koje se ne nalaze na njihovom računaru, sa bilo koje lokacije i sa bilo kog na internet povezanog uređaja.

[3] RFID je sistem daljinskog slanja i prijema podataka pomoću posebnih kartica tj. odašiljača.

„Internet stvari" se definišu kao mreža fizičkih uređaja, vozila, građevina i drugih objekata, sa ugrađenom elektronikom, softverom, senzorima i mrežnim interfejsima, koja omogućava svim tim entitetima da prikupljaju, razmenjuju, obrađuju i koriste podatke. „Internet stvari" predstavljaju sistem međusobno povezanih računarskih uređaja, mehanički i digitalnih mašina, predmeta, životinja ili ljudi koji su opremljeni jedinstvenim identifikatorima i koji mogu da prenose podatke preko mreže bez potrebe interakcija čovek-čovek ili čovek-računar (Mahlyanov 2018, 176). *Things* u kovanici *Internet of Things* predstavlja bilo koji uređaj koji je povezan na internet i kojem je dodeljena IP adresa.[4] Internet stvari se mogu posmatrati kao globalna infrastruktura za informaciono društvo koja omogućava napredne usluge međusobnim povezivanjem (fizičke i virtuelne) stvarnosti zasnovane na postojanju i razvoju, interoperabilne informaciono-komunikacione tehnologije (Pokorni 2019, 590). U poslednje dve decenije došlo je do značajnog približavanja fizičkog (realnog) i digitalnog (virtuelnog) sveta. U početku je internet igrao presudnu ulogu u povezivanju ta dva sveta. Danas postoje brojne aplikacije vezane za „internet stvari", uređaji raspoređeni u raznim sektorima, uključujući zdravstvenu zaštitu, transport, pametne kuće, proizvodnju i slično (Zeadally and Tsikerdekis 2019, 1). „Internet stvari" uključuju gotovo sve aspekte života građana.

Evropska komisija je 2015. godine formirala Savez za inovacije „internet stvari" (*Alliance for Internet of Things Innovation* – AIOTI) kako bi stvorila platformu razmene podataka između različitih sektora (industrija). Misija Saveza za inovacije „internet stvari" je saradnja sa Evropskom komisijom za primenu i izvršenje evropskog okvirnog programa za istraživanje i inovacije (*European framework programs for research and innovation*), saradnja i koordinacija sa drugim evropskim inovacionim platformama i organizacijama vezanim za „internet stvari", identifikovanje i pokušaj rešavanja tržišnih prepreka za primenu i drugo. Članovi Saveza za inovacije „internet stvari" su široko zastupljeni u različitim industrijama i sektorima (AIOTI n.d.).

Kontinuirani brzi tehnološki napredak je od ključne važnosti za ekonomski prosperitet i socijalno blagostanje, ali takođe predstavlja potencijalne nove pretnje. Više desetina milijardi „internet stvari" je u novije vreme povezano na internet što proširuje potencijal napada zlonamernih pojedinaca i organizacija na internetu (Trautman and Ormerod 2017, 761–764). Aplikacije koje se tiču „internet stvari" su tako često povezane sa osetljivim podacima, mrežnom infrastrukturom i

[4] IP broj ili IP adresa je jedinstvena brojčana oznaka računara ili bilo kog drugog uređaja koji je povezan na Internet.

sredstvima što ih čini ranjivim (Picone et al. 2021, 1–4). Povećanje upotrebe „internet stvari" u poslednjoj deceniji, prouzrokovalo je prikupljanje velikih količina podataka i brojne poteškoće, kao što su npr. selekcija i upravljanje podacima. Poseban izazov leži u činjenici da broj uređaja povezanih na mrežu raste svaki dan. Očekuje se da će broj „internet stvari" narasti na više od 70 milijardi do 2025. godine (Alvarez et al. 2021, 1). „Internet stvari" imaju ograničene resurse kao što su memorijski prostor i procesorska moć, što utiče na performanse i bezbednost upotrebe (Botta et al. 2016, 684–700). Mnoge aplikacije su poboljšane integrisanjem „internet stvari" i računarstva u oblaku. Primeri takvih primena su u zdravstvu, pametnim gradovima, pametnim zgradama, pametnim merenjima, pametnog urbanog nadzora itd. (Petrolo et al. 2015, 1–3).

Trenutno stanje zaštite „internet stvari" je veoma loše (Rytel et al. 2020, 22). Mnogi proizvođači često zanemaruju aspekt bezbednosti. Prema rezultatima pojedinih istraživanja, „internet stvari" se prodaju sa malim stepenom ili bez zaštite (Dhanjani 2015, 296). Istraživanje Fondacije za bezbednost „internet stvari" (*IoT Security Foundation*), sprovedeno 2018. godine, pokazalo je da je samo deset odsto od ukupno 331 kompanije koje proizvode „internet stvari" svesno ranjivosti svojih proizvoda (IoT Security Foundation n.d.). Veliki broj proizvođača ignoriše čak i ozbiljne, identifikovane, bezbednosne propuste koji se nalaze u njihovim proizvodima (Rytel et al. 2020, 2).

Najčešće ranjivosti kada su u pitanju „internet stvari" jesu slabe lozinke, problem ažuriranja propusta, nedostatak kriptovanja komunikacije i autentifikacije korisnika, zastarela verzija operativnog sistema i drugih softvera, kodirane lozinke bez mehanizama za promenu, „rupe" za ubacivanje zlonamernog koda kao i otvoreni Telnet portovi (Anand et al. 2020, 2).[5] Nedostatak mehanizama za ažuriranje „internet stvari" je posebno opasan, jer ometa sposobnost daljinskog ublažavanja otkrivenih ranjivosti. Često se ranjivosti nalaze u hardveru uređaja i mogu se popraviti samo modifikovanjem samog hardvera, što je skupo i ponekad nemoguće. Ranjivost „internet stvari" je već eksploatisana više puta. Najpoznatiji detektovan problem kojim je kompromitovan veliki broj „internet stvari" je *Mirai botnet* kojim je realizovan distribuirani napad uskraćivanja usluga (*Distributed Denial of Service* – DDoS) velikih razmera. *Botnet* (*roBOT NETwork*) predstavlja mrežu zaraženih računara (*zombies*) kojima mogu pristupiti neovlašćeni korisnici i na taj način ostvariti daljinsku kontrolu svakog pojedinačnog računara, najčešće radi izvršavanja određenih komandi (Rytel et al. 2020, 2).

[5] Telnet je mrežni protokol koji omogućava korisniku jednog računara sesiju za korišćenje komandne linije na drugom računaru tj. povezivanje i rad na drugom računaru putem interneta.

Ukoliko se komunikacija odvija bežičnim sredstvima onda je povećana osetljivost i verovatnoća napada. Još jedna karakteristika „internet stvari" je njihova otvorenost i fleksibilnost. „Internet stvari" se često postavljaju na fizički neobezbeđena područja tako da im napadači u tom slučaju mogu lako pristupiti. Dok neki napadi ugrožavaju samo nekoliko „internet stvari", drugi mogu kompromitovati celu mrežu (Khan and Herrmann 2019, 2). Najčešći napadi na „internet stvari" su DDOS, spufing napadi, napad malicioznim programima radi kompromitovanja, prikupljanja informacija i preuzimanje kontrole.[6] Istraživanja određenih organizacija i kompanija pokazuju porast broja malicioznih programa koji ugrožavaju „internet stvari". Broj malicioznog softvera koji ugrožava „internet stvari" u prvoj polovini 2018. godine je bio trostruko veći u odnosu na celu 2017. godinu, u kojoj je pak zabeleženo deset puta više napada na „internet stvari" u odnosu na celu 2016. godinu (Filipović i dr. 2019, 813–815). Najčešće napadana usluga je *Telnet* za koju se vezuje 75,4% napada. Prema podacima Laboratorije Kasperski (*Kaspersky Lab*) kao maliciozni programi otkriveni su: *Backdoor.Linux.Mirai.c* (15,9% od ukupnog broja napada), *Trojan-Downloader. Linux.Hajime.a* (5,8%), *Trojan-Downloader.Linux.NyaDrop.b* (3,3%), itd. *Mirai botnet* je najzastupljeniji u napadima na „internet stvari" (15,9%). IP nadzorne kamere su takođe izložene napadima, pa je tako primera radi u jednoj sedmici kompromitovano 57.000 *GoAhead* kamera (Kaspersky Laboratory n.d.).

Mehanizmi zaštite računarskih sistema obično nisu primenljivi za „internet stvari" zbog ograničenja resursa uređaja i decentralizovane prirode arhitekture „internet stvari" (Picone et al. 2021, 1). Trenutna rešenja koja omogućavaju ublažavanje rizika vezano sa „internet stvari" fokusirana su na obezbeđivanje osnovnih atributa bezbednosti informacija: tajnost (poverljivost), integritet (celovitost) i raspoloživost (dostupnost) (Alvarez et al. 2021, 4). Zbog ogromnog rasta, veličine i složenosti sistema „internet stvari", zaštita elemenata i mreže preko kojih su uređaji povezani veoma su složen problem. Rešenje bi trebalo da započne zaštitom pojedinačnog elementa, a zatim da se osigurava mreža na koju su „internet stvari" priključene (Mahlyanov 2018, 179). Istraživačka zajednica i tela za standardizaciju trenutno rade na definisanju novih metodologija i standarda zaštite (Sicari et al. 2018, 59–74).

Jedan od mehanizama zaštite je *blockchain*.[7] Podrazumeva postavljanje fizičkog dodatka na uređaje i sadrži odgovarajuće zapise, čineći informacije jedinstvenim (Villamil et al. 2020, 2320–2327). *Blockchain* je digitalno distribuiran sistem

[6] Spufing (*spoofing*) je obmana tj. prevara kojom se stvara utisak da prenos vrši ovlašćeni korisnik. To je prefinjena tehnika provere autentičnosti jednog uređaja prema drugom.

[7] *Blockchain* je kompjuterski fajl koji se sastoji od blokova podataka koji su međusobno povezani. Svaki blok sadrži link (vezu) sa prethodnim blokom i na taj način se formira lanac.

sposoban da održi podatke nepromenljivim i omogućava *peer-to-peer* transakcije, odnosno komunikaciju putem interneta gde nije potreban server niti je definisana hijerarhija između računara. Zaštitom integriteta podataka, *blockchain* gradi poverenje u digitalni prenos i omogućava da se transakcije izvršavaju efikasnije i sigurnije, direktno, bez potrebe za posrednicima. Smanjuje ogromnu količinu resursa potrebnih za potvrđivanje identiteta (Chou 2018, 117). Mogući, dodatni, mehanizam zaštite jeste i primena tzv. sistema za otkrivanje upada (*Intrusion Detection System* – IDS). Zadatak sistema za otkrivanje upada je otkrivanje aktivnosti koje potencijalno ukazuju na to da je sistem ugrožen (Khan and Herrmann 2019, 3). U cilju rešavanja bezbednosnih rizika nekoliko poznatih kompanija razvija različite, bezbednije, platforme kao što su *IBM Watson IoT Cloud platform* i *Microsoft Azure platform* (Cangea 2019, 9).

Brojne pretnje „internet stvarima" ukazuju na sveobuhvatnost i složenost problema koji prete tom tehnološkom području koje beleži rekordno veliki porast i značaj za društvo u celini. „Internet stvari" ne pokazuje nikakve znakove usporavanja u razvoju i primeni na globalnom planu. Taj trend će sigurno pratiti i nastanak novih, sve opasnijih i ozbiljnijih pretnji (Filipović i dr. 2019, 817).

Zaključak

Savremeni svet karakterišu različita gledišta, pre svih velikih svetskih sila, na problem upravljanja internetom i usvajanja regulative koja se tiče interneta (sajber prostora). Grupa država predvođena Sjedinjenim Američkim Državama zalaže se za nefragmentirani, globalni internet, odnosno otvoren pristup upravljanju internetom kojim bi se obezbedila zaštita ljudskih prava, sloboda govora i slobodan protok informacija. Druga grupa država, predvođena Rusijom i Kinom, zalaže se za nacionalno segmentirani internet tj. veću ulogu država u upravljanju internetom, čime bi se poboljšala informaciona bezbednost, upravljanje sadržajem, i na taj način obezbedio teritorijalni integritet i suverenitet država. Pojedine države, kao što je npr. Francuska, zalažu se za tzv. balansirani pristup koji podrazumeva slobodno funcionisanje brojnih usluga i servisa ali sa nekim ograničenjima. Određeni sadržaji i *online* komunikacija treba da se kontrolišu radi zaštite nacionalnih interesa u sklopu npr. sprovođenja antiterorističkih mera i drugih opravdanih razloga. U međunarodnoj zajednici je poslednjih godina sve prisutnije neslaganje po pitanju upravljanja internetom.

Pitanje primenljivosti i dovoljnosti međunarodnog prava u kontekstu upotrebe upravljanja internetom nije rešeno i ostaje u osnovi međunarodnog dijaloga o

bezbednosti informacija. Sve veći broj država bezbednost informaciono-komunikacionih tehnologija smatra pitanjem od velikog značaja za nacionalnu i međunarodnu bezbednost. Ugroženost informacionog društva značajno je uvećana sve masovnijom upotrebom „internet stvari".

Rusko stanovište vezano za upravljanje internetom proizilazi iz zabrinutosti zbog američke dominacije upravljanja internetom kroz „Internet korporaciju za dodeljene nazive i brojeve". Mehanizmi funkcionisanja pomenute organizacije nisu do kraja transparentni kao što je npr. izbor članova odbora. Rusija promoviše stav da je Međunarodna unija za telekomunikacije, specijalizovana agencija Ujedinjenih nacija, najprihvatljivije rešenje za upravljanje internetom. Kina je proširila svoju poziciju u globalnim regulatornim telima i preuzima sve aktivniju ulogu po pitanju upravljanja internetom – sve češće inicira i zahteva da se usvoje globalne norme, propisi i standardi. Imajući u vidu veličinu Kine i njenog tržišta i njenu sve značajniju ulogu u međunarodnim odnosima, to može imati veliki uticaj na razvoj i primenu novih tehnologija, od električnih vozila do veštačke inteligencije, telekomunikacione infrastrukture i „internet stvari". Kina u okviru Generalne skupštine Ujedinjenih nacija i kroz Šangajsku organizaciju za saradnju, u saradnji sa ostalim članicama, promoviše Kodeks ponašanja za informacionu bezbednost. Kina takođe organizuje godišnju Svetsku internet konferenciju u Vuženu fokusiranu, između ostalog, na stvaranje globalnih normi upravljanja internetom.

Ruski i kineski lideri sve više posmatraju zavisnost od američke i evropske tehnologije kao ozbiljnu ranjivost. Usled narastajućih problema i procena negativnog uticaja na bezbednost, nacionalnim zakonodavstvom u Rusiji i Kini regulisana su brojna pitanja vezana za internet. Skladištenje prikupljanih podataka od građana obavezno je na serverima koji se fizički nalaze na teritoriji Rusije, odnosno Kine. To znači da kompanije kao što su *Google*, *Twitter*, *Facebook* i druge moraju da hostuju servere na prostoru Rusije i Kine ako žele da budu prisutne na njihovim tržištu. Ako to ne učine i nastave da koriste servere koji se nalaze van matičnih država – uglavnom u SAD – vlasti dveju država će onemogućiti pristup njihovim stranicama i servisima. Takođe, uspostavljen je mehanizam boljeg praćenja toka informacija koje ulaze ili izlaze iz njihovih zemalja.

U Rusiji je normativno uspostavljen mehanizam za upravljanje ruskim segmentom interneta, i to u pogledu saobraćaja, dostupnosti resursa i usluga. Zahvaljujući sopstvenoj opremi, serverima i domenima, kritična nacionalna infrastruktura je znatno bezbednija. Ruska vlada nastoji da celokupan internet saobraćaj bude pod nacionalnom kontrolom i to tako što on prolazi kroz tzv. tačke rutiranja na kojima se upravlja podacima koji ulaze ili izlaze iz zemlje. Kineska mrežna barijera (*firewall*), takođe kontroliše svoje tačke rutiranja, koristeći filtere sadržaja, blokiranje ključnih reči i određenih sajtova kao i drugim tehničkim rešenjima. I

američka vlada nastoji da uspostavi mehanizme kontrole internet sadržaja na svojoj teritoriji. Novi pristup i incijative pokazuju nameru da se spreči skladištenje i procesuiranje korisničnih podataka, vredne intelektualne svojine kompanija i drugih bitnih podataka i informacija na tzv. klaud-sistemima (*cloud computing*).

Na osnovu analize aktivnosti i dokumenata različitih subjekata upravljanja internetom, evidentno je da suprotstavljeni nacionalni interesi vodećih svetskih sila ne dozvoljavaju postizanje konsenzusa oko osnovnih principa upravljanja internetom. Rusija i Kina, uz podršku drugih zemalja, istrajaće u nameri da se promeni način funkcionisanja upravljanja internetom. Do tada, internet okruženje biće sve nestabilnije i nebezbednije, između ostalog usled masovnije upotrebe „internet stvari". Internet je već, na neki način, fragmentiran tako da je u određenim zemljama moguće regulisati sadržaj, blokirati pristup određenim uslugama i sadržajima, nadzirati korisnike. Pored Rusije i Kine verovatno će u perspektivi i neke druge zemlje pokušati da uspostave kontrolu nad nacionalnim internet saobraćajem. Dakle, budući internet će verovatno omogućiti i nacionalnim vladama daleko veći mehanizam kontrole unutar državnih granica. Povećana fragmentacija dovešće do uspostavljanja tzv. digitalnih granica u sajber prostoru.

Internet treba da bude multilateralan, transparentan i demokratski, uz puno učešće međunarodnih i regionalnih organizacija vlada, privatnog sektora, civilnog društva po različitim pitanjima vezanim za upravljanje internetom. Određeni sadržaji i servisi mogu, eventualno, da budu kontrolisani u skladu sa nacionalnim i međunarodnim regulativama i zakonodavstvom. Model upravljanja više subjekata se nameće kao realan model upravljanja internetom. Međutim, suprotstavljeni nacionalni interesi vodećih svetskih sila verovatno će dovesti do toga da dijalog o upravljanju internetom ostane polarizovan i u doglednoj budućnosti.

Bibliografija

AIOTI [Alliance for Internet of Things Innovation]. n.d. Accessed 10 February 2021. https://ec.europa.eu/digital-single-market/en/alliance-internet-things-innovation-aioti.

Alvarez, Yigliana, Leguizamón-Páez Miguel Angel and Londoño, Tania J. 2021. "Risks and security solutions existing in the Internet of things (IoT) in relation to Big Data". *Ingeniería y Competitividad* 23 (1): 1–13.

Anand, Pooja, Singh Yashwant, Selwal Arvind, Kumar Singh P., Andreea Felseghi R. and Raboaca Maria S. 2020. "IoVT: Internet of Vulnerable Things? Threat

Architecture, Attack Surfaces, and Vulnerabilities in Internet of Things and Its Applications towards Smart Grids". *Energies* 13 (18): 1–23.

ASEAN [International organisation of Southeast Asian countries]. 2018. "United States leaders' statement on cybersecurity cooperation". Accessed 12 January 2021. https://asean.org/asean-united-states-leaders-statement-cybersecurity-cooperation/.

Botta, Alessio, De Donato Walter, Persico Valerio and Pescapé Antonio. 2016. "Integration of cloud computing and internet of things: A survey". *Future Generation Computer System* 56: 684–700.

Cangea, Otilia. 2019. "A Comparative Analysis of Internet of Things Security Strategies". *BULETINUL University of Ploiesti* LXXI (1): 1–10.

Chou, Shuo Y. 2018. "The Fourth Industrial Revolution: Digital Fusion With Internet of Things". *Journal of International Affairs* 72 (1): 107–120.

Council of Europe Internet Governance Strategy 2016–2019, 30 March 2016, https://rm.coe.int/internet-governance-strategy-2016-2019-updated-version-06-mar-2018/1680790ebe.

Dhanjani, Nitesh. 2015. *Abusing the Internet of Things: Blackouts, Freakouts, and Stakeouts*, Boston: O'Reilly Media.

Directive (EU) 2016/1148 of the European Parliament and of the Council on security of network and information systems (NIS Directive), *Official Journal of the European Union*, L 194/1, 6 July 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN.

Doctrine RF No. 646/2016 - Doctrine of the Information Security Doctrine of the Russian Federation. 2016. Presidential Decree No. 646, The Ministry of Foreign Affairs of the Russian Federation, 5 December 2016, https://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163.

Eneken, Tikk. 2019. "Cyber arms control and resilience", in SIPRI Yearbook Online – Armaments, *Disarmament and International Security*, Stocholm International Peace Research Institute, Oxford: Oxford University Press.

European Commision. 2013. Cybersecurity Strategy of the European Union, February 7. https://ec.europa.eu/home-affairs/sites/default/files/e-library/documents/policies/organized-crime-and-human-trafficking/cybercrime/docs/join_2013_1_en.pdf.

European Pariliament Res. 2015/2526[RSP] on the Renewal of the mandate of the Internet Governance Forum, 11 February 2015, https://www.wgig.org/docs/WGIGREPORT.pdf.

Filipović, Matija A., Bralić Vladimir i Malešević Nikola. 2019. "Internet stvari i moguće ugroze", prezentovano na 12. Međunarodna znanstveno-stručna konferencija "Dani kriznog upravljanja 2019", Veleučilište Velika Gorica, Velika Gorica, 27-29.5.2019.

Internet Governance Forum. 2018. "IGF 2018 Chair Summary – The Internet of Trust", Accessed 4 January 2021. https://www.intgovforum.org/multilingual/index.php?q=filedepot_download/6212/1417.

Internet Governance Forum. 2019. "Final report from the 14th Forum". Accessed 2 February 2021. https://dig.watch/igf2019_Final_Report.

Internet Governance Forum. 2020. "Internet Governance Forum calls for bridging digital divides, harnessing the Internet to support human resilience and build solidarity amid COVID-19". Accessed 2 February 2021. https://www.un.org/sustainabledevelopment/blog/2020/11/internet-governance-forum-calls-for-bridging-digital-divides-harnessing-the-internet-to-support-human-resilience-and-build-solidarity-amid-covid-19/.

IoT Security Foundation. n.d. "Understanding the Contemporary Use of Vulnerability Disclosure in Consumer Internet of Things Product Companies". Accessed 22 February 2021. https://www.iotsecurityfoundation.org/wp-content/uploads/2018/11/Vulnerability-Disclosure-Design-v4.p.

Jeutner, Valentin. 2019. "The Digital Geneva Convention". *Journal of International Humanitarian Legal Studies* 10 (1): 158–170.

Kaspersky Laboratory. n.d. "New Trends in the world of IoT threats". Accessed 12 March 2021. https://securelist.com/new-trends-inthe-world-of-iot-threats/87991/.

Kerttunen, Mika and Tikk Eneken. 2019. "National cyber security strategies: Commitment to development", *Cyber Policy Institute* (1): 1–14.

Khan, Ali Z. and Herrmann Peter. 2019. "Recent Advancements in Intrusion Detection Systems for the Internet of Things, Security and Communication Networks". *Hindawi.* DOI: https://doi.org/10.1155/2019/4301409.

Kurbalija, Jovan. 2011. *Uvod u upravljanje Internetom.* Beograd: Albatros plus.

Mahlyanov, Dobrin. 2018. "Internet of Things – A new attack vector for hybrid threats". *Information & Security: An International Journal* 39 (2): 175–182.

NATO Declaration No. 095/2018, Joint declaration on EU–NATO cooperation", *NATO Press Release No. 095*, 10 July 2018. https://www.nato.int/cps/en/natohq/official_texts_156626.htm.

NATO Cyber Defence. 2020. Accessed 12 January 2021. https://www.nato.int/cps/en/natohq/topics_78170.htm.

Nocetti, Julien. 2015. "Contest and Conquest: Russia and global internet governance". *International Affairs* 91 (1): 111–130.

OSCE Decision No. 1106/2013, Initial set of OSCE confidence-building measures to reduce the risks of conflict stemming from the use of information and communication technologies, Permanent Council of the Organization for Security and Co-operation in Europe - OSCE, 3 December 2013, https://www.osce.org/files/f/documents/d/1/109168.pdf.

OSCE Decision No. 1202/2016, OSCE confidence-building measures to reduce the risks of conflict stemming from the use of information and communication technologies, Organization for Security and Co-operation in Europe (OSCE) – Permanent Council, 10 March 2016, https://www.osce.org/files/f/documents/d/a/227281.pdf.

Paris Call for Trust and Security in Cyberspace. 2018. Accessed 10 February 2021, https://pariscall.international/en/.

Petrolo, Riccardo, Loscri Valeria and Mitton Nathalie, 2015. "Towards a smart city based on cloud of things, a survey on the smart city vision and paradigms". *Transactions on Emerging Telecommunications Technologies* 28 (1): 1–11.

Picone, Marco, Cirani Simone and Veltri Luca. 2021. "Blockchain Security and Privacy for the Internet of Things". *Sensors* 21 (3): 1–4.

Pokorni, Slavko, 2019. "Reliability And Availability of the Internet of Things". *Vojnotehnicki glasnik* 67 (3): 588–600.

Regulation (EU) 2019/881 of the European Parliament and of the Council (Cybersecurity Act), *Official Journal of the European Union*, I. 151/15, 17 April 2019, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN.

Rytel, Marcin, Felkner Anna and Janiszewski Marek. 2020. "Towards a Safer Internet of Things - A Survey of IoT Vulnerability Data Sources". *Sensors* 20 (21): 1–26.

Sicari, Sabrina, Rizzardi Alessandra, Cappiello Cinzia, Miorandi Daniele and Coen-Porisini A. "Toward Data Governance in the Internet of Things". chapter in Yager, Ronald R. and Espada Pascual J. 2018. *New Advances in the Internet of Things*. Berlin: Springer.

Tipton, Harold F. and Krause, Micki. 2004. *Information Security Management Handbook (fifth edition)*, New York: CRC Press.

Trautman, Lawrence J. and Ormerod Peter C. 2017. "Industrial Cyber Vulnerabilities: Lessons from Stuxnet and the Internet of Things". *University of Miami Law Review* 72: 761–826. DOI: 10.2139/ssrn.2982629.

[UNGAa] United Nations General Assembly Resolution A/RES/74/197, Information and communications technologies for sustainable development, December 19 2019. https://unctad.org/system/files/official-document/ares74d197_en.pdf.

[UNGAb] United Nations General Assembly Report of the Secretary-General A/66/152, Developments in the field of information and telecommunications in the context of international security, July 15 2011. https://undocs.org/pdf?symbol=en/A/66/152.

[UNGAc] United Nations General Assembly Resolution A/73/27, Developments in the field of information and telecommunications in the context of international security, December 11 2018. https://undocs.org/en/A/RES/73/27.

[UNGAd] United Nations General Assembly Resolution 73/266, Advancing responsible state behaviour in cyberspace in the context of international security, December 22 2018. https://undocs.org/A/RES/73/266.

[UNGAe] United Nations General Assembly Secretary-General's Strategy on New Technologies, September 2018. https://www.un.org/en/newtechnologies/images/pdf/SGs-Strategy-on-New-Technologies.pdf.

[UNWGIG] United Nations Working Group on Internet Governance (UN WGIG) Report No. 05.41622", June 2005. https://www.wgig.org/docs/WGIGREPORT.pdf.

[UN-ITU WSIS+10] United Nations International Telecommunication Union World Summit on the Information Society WSIS+10 Outcome Documents, June 2014. https://www.itu.int/net/wsis/implementation/2014/forum/inc/doc/outcome/362828V2E.pdf.

U.S. - Office of the Coordinator for Cyber Issues (S/CCI), Recommendations to the President on deterring adversaries and better protecting the American people from cyber threats, 31 May 2018, https://www.state.gov/wp-content/ uploads/2019/04/Recommendations-to-the-President-on-Deterring-Adversaries-and-Better-Protecting-the-American-People-From-Cyber-Threats.pdf.

Villamil, Sebastian, Hernández Cesar and Tarazona Giovanny 2020. "An overview of internet of things". *TELKOMNIKA – Telecommunication, Computing, Electronics and Control* 18 (5): 2320–2327.

Zeadally, Sherali and Tsikerdekis, Michail. 2019. "Securing Internet of Things (IoT) with machine learning". *International Journal of Communication Systems* 33 (1): 1–16.

Dejan VULETIĆ, Branislav ĐORĐEVIĆ

PROBLEMS AND CHALLENGES OF INTERNET GOVERNANCE AT THE INTERNATIONAL LEVEL

Abstract: The activities of the United Nations, as the most important international organization, as well as the efforts of certain regional and national organizations, are discussed in this article on the subject of Internet governance. The article pays special attention to the "internet of things," the increasing use of which causes the emergence of new, dangerous, and serious threats, further complicating the problem of Internet governance. The stated subject of the research is directly related to the aim of the paper, which is to present and analyse the activities of various entities, international, regional and national institutions and organizations, as well as leading states, primarily the United States and Russia, and documents that attempt to regulate activities in cyberspace. The basic hypothesis is that opposing national interests prevent international bodies, particularly the United Nations, from reaching a consensus on the fundamental principles of Internet governance, resulting in insecurity in the face of increasingly frequent, diverse, and serious threats to the Internet and cyberspace in general. Based on the arguments presented in the paper, there have been numerous attempts to regulate Internet governance that have not materialized in concrete decisions implemented in national legislation and practice. Due to the growing dependence on information and communication technologies, the problem of the non-existence of regulations in this area makes the information society even more vulnerable.

Keywords: internet, cyberspace, internet of things, vulnerabilities, management, security.