Kina kao „velika cyber sila”:
Dva glasa Pekinga u telekomunikaciji

Rush Doshi, Emily de La Bruyère, Nathan Picarsic i John Ferguson

Ožujak 2021.

Sažetak

Vanjska kineska vlada i komercijalne poruke o informatičkoj tehnologiji (IT) govore jednim glasom. Na domaćem tržištu čuje se drugi, drugačiji glas. Prvi glas naglašava slobodna tržišta, otvorenost, suradnju i međuovisnost, teme koje upućuju na to da bi Huawei i druge kineske tvrtke trebalo tretirati kao druge dionike globalnog privatnog sektora te da ih treba prihvatiti u strane mreže. Za to vrijeme, domaća kineska vlada te komercijalni i akademski diskurs naglašavaju *ograničenja* slobodnih tržišta i opasnosti oslanjanja na strane tehnologije i, u skladu s tim, potrebu za industrijskom politikom i kontrolom vlade u svrhu zaštite tehnologija, tvrtki i mreža. Domaći kineski diskurs također ukazuje na to da se komercijalne komunikacijske mreže, uključujući telekomunikacijske sustave, mogu upotrebljavati za ofenzivnu demonstraciju snage i utjecaja, da međunarodne tehničke norme nude sredstva kojima se takva snaga i utjecaj mogu učvrstiti i, prije svega, da su IT arhitekture domena natjecanja nulte sume.

Nije nikakva novost da vanjska kineska vlada i korporativne poruke mogu biti neiskrene. Međutim, osnovne razlike između tih poruka i unutarnje rasprave Kine o IT-u i dalje su uglavnom nedokumentirane, unatoč sve većem razvoju i utjecaju Kine na područjima međunarodne IT infrastrukture, tehnologije i normi. Ovim se izvješćem nastoji ispuniti taj jaz, dokumentirati napetost između vanjskih i unutarnjih rasprava Kine o telekomunikacijama, ali i o širem području IT-a. U izvješću se također analizira unutarnji diskursa za uvid u namjeru, ambicije i strategiju Pekinga. Ovo izvješće postavlja pitanja o kineskoj vladi i komercijalnim porukama, kao i o tome što te poruke mogu prikrivati.

Ovo izvješće motivirano je rastućim utjecajem Kine na telekomunikacije i rastućom kontroverzom koja prati taj utjecaj. Međutim, kineski telekomunikacijski resursi, ambicije i strateški okviri šire su isprepleteni s područjem IT-a. Iz tog razloga, u ovom se izvješću razmatra kineska vlada, komercijalna i akademska rasprava o IT-u, općenito, ali i specifično o telekomunikacijama. Ovo izvješće također kontekstualizira svoju analizu unutar programa Pekinga kojim želi postati „velika cyber sila”, odnosno „velika mrežna sila”, što je plan ambicija Kine da preskoči postojeće vođe industrije i definira arhitekturu digitalne revolucije.

Novi tehnološki krajolik oblikuje se. Kina radi na definiranju tog krajolika. Više nego ikada prije, važno je da se kineske ambicije dokumentiraju.

Uvod

Kineska telekomunikacijska tvrtka Huawei 2020. je kontaktirala poznati zapadni list sa sljedećim zahtjevom: Bi li objavili niz od 10 članaka kao podršku tvrtki Huawei dok se tvrtka hrvala sa zapadnim pritiskom?[1] Tvrtka Huawei predložila je niz tema za te članke, uključujući navodno poštovanje intelektualnog vlasništva tvrtke, koristi koje su državne subvencije tvrtke pružile svijetu, ulogu tvrtke kao odgovornog aktera koji vjeruje u tržišno natjecanje te status tvrtke kao tvrtke u vlasništvu zaposlenika, neovisne o utjecaju kineske vlade. Tvrtka Huawei ponudila je svoje znanstvenike i osoblje za intervjue. Također je predložila konzultacije s odabranim glasovima koji ne pripadaju tvrtki Huawei. Huawei je zatražio konačnu reviziju materijala prije objave.

Ulaganje truda u oblikovanje javnih izvješća nije rijetkost među velikim poduzećima, kako u Kini, tako i domaća. Ipak, Huawei je poseban. Ističe se svojom suradnjom s naporima šire kineske vlade da utječe na globalni diskurs o telekomunikacijskim i informacijskim mrežama. Te poruke tvrtke i vlade uvelike se razlikuju od diskursa domaće kineske vlade te domaćeg kineskog akademskog i komercijalnog diskursa.

Vanjska kineska vlada i komercijalne poruke o informatičkoj tehnologiji (IT) govore jednim glasom. Ali domaća vlada otkriva radikalno drugačiji, drugi glas. Kao i predloženi članci tvrtke Huawei, vanjska kineska vlada naglašava slobodna tržišta, otvorenost, suradnju i međuovisnost, teme koje upućuju na to da bi Huawei i druge kineske tvrtke trebalo tretirati kao druge dionike globalnog privatnog sektora te da ih treba uključiti u strane mreže. U međuvremenu, domaći kineski diskurs naglašava *ograničenja* slobodnih tržišta i, u skladu s tim, potrebu za industrijskom politikom i kontrolom vlade u svrhu zaštite tehnologija, tvrtki i mreža, opasnost od oslanjanja na stranu tehnologiju, konkurentnu vrijednost postavljanja međunarodnih standarda i, u pozadini svega, neizbježnost natjecanja nulte sume u IT-u.

Nije nikakva novost da vanjska kineska vlada i korporativne poruke mogu biti neiskrene. Međutim, osnovne razlike između tih poruka i unutarnje rasprave Kine o IT-u i dalje su uglavnom nedokumentirane, unatoč sve većem razvoju i utjecaju Kine na područjima međunarodne IT infrastrukture, tehnologije i normi. Ovim se izvješćem nastoji ispuniti taj jaz, dokumentirati napetost između vanjskih i unutarnjih rasprava Kine o telekomunikacijama, ali i o širem području IT-a. U izvješću se također analizira unutarnji diskursa za uvid u namjeru, ambicije i strategiju Pekinga. Ovo izvješće postavlja pitanja o kineskoj vladi i komercijalnim porukama, kao i o tome što te poruke mogu prikrivati.

Ovo izvješće posebno je motivirano rastućim utjecajem Kine na telekomunikacije i rastućom kontroverzom koja prati taj utjecaj. Međutim, kineski telekomunikacijski resursi, ambicije i strateški okviri šire su isprepleteni s područjem IT-a. Iz tog razloga, u ovom se izvješću razmatra kineska vlada, komercijalna i akademska rasprava o IT-u, općenito, ali i specifično o telekomunikacijama. Ovo izvješće također kontekstualizira svoju analizu unutar programa Pekinga kojim želi postati „velika cyber sila",[2] što je plan ambicija Kine da preskoči postojeće vođe industrije i definira arhitekturu digitalne revolucije. Izvješće iznosi nekoliko primarnih nalaza:

1. **Dok Kina često iznutra raspravlja o svojim ambicijama „velike cyber sile“, rijetko priznaju te ambicije u porukama koje šalju van.** Izraz „velika cyber sila” ključni je koncept koji usmjerava kinesku strategiju u telekomunikacijama, ali i u širem području IT-a. Pojavljuje se u naslovu gotovo svakog važnog govora predsjednika Xija Jinpinga o kineskoj telekomunikacijskoj i mrežnoj strategiji, usmjerenog na domaću publiku od 2014. Ali taj izraz rijetko se može pronaći u porukama usmjerenima vanjskoj stranoj javnosti i glasnogovornici Ministarstva vanjskih poslova spominju je samo jednom u šest godina. To ukazuje da Peking namjerno razvodnjuje rasprave o svojim ambicijama kako ne bi uznemirio stranu javnost.

2. **Dok kineska vlada potiče stranu javnost na kupnju proizvoda Huawei, njezini vođe upozoravaju domaću javnost na opasnosti koje proizlaze iz oslanjanja na stranu tehnologiju.** Godinama prije trgovinskog rata i ograničenja Trumpove administracije za Huawei, Xi je tvrdio da je „kontrola drugih nad temeljnom tehnologijom naša najveća skrivena opasnost“ i da je omogućavanje strancima da kontroliraju temeljnu tehnologiju „poput izgradnje kuće na tuđim temeljima”.[3] Izjavio je da „Kina mora imati vlastitu tehnologiju i mora imati jaku tehnologiju”.[4]

3. **Kineska vlada potiče stranu javnost koja je skeptična o tvrtki Huawei da se drže tržišnih načela. Istovremeno, vlada upozorava domaću javnost da razvoj IT mreže zahtijeva industrijsku politiku te se ne može povjeriti tržišnim silama.** Xi je izričito izjavio da: „tržišna razmjena ne može donijeti temeljne tehnologije, a novac ne može kupiti temeljne tehnologije”.[5]

4. **Peking naziva vanjsku zabrinutosti za sigurnost zbog tvrtke Huawei „jadnim izgovorom” i čistom „politikom”.[6] U isto vrijeme Kina izražava slične zabrinutosti na domaćem tržištu zbog uključivanja strane tehnologije u svoje mreže.** Sigurnost je od ključne važnosti za Xija koji je u više navrata u više navrata proglasio da „bez kibernetičke sigurnosti neće biti nacionalne sigurnosti”.[7] U skladu s tim, zalaže se samo za usvajanje vanjske tehnologije kojom se može „upravljati”, dok čelnici u Ministarstvu industrije i informacijske tehnologije (MIIT) naglašavaju da se stranim tehnološkim mrežama u pravilu ne može „upravljati”.[8] Kina stoga mora izraditi vlastite mreže koje su „neovisne te se njima može upravljati”.[9]

5. **Komercijalni i akademski kineski izvori sugeriraju da zabrinutost međunarodne zajednice za sigurnost zbog kineskih telekomunikacija možda nije neutemeljena te da Peking možda vidi telekomunikacijske i ostale komercijalne mreže kao sredstva za projiciranje ofenzivne moći na globalnoj razini.** XI predstavlja IT kao ključni dio kineske strategije vojno-civilne fuzije: godine 2018. rekao je da je „vojno-civilna fuzija u kibernetičkoj sigurnosti i informatizaciji ključno i granično područje za vojno-civilnu fuziju.”[10] Nadalje, Qin an, direktor kineskog instituta za strategiju na kibernetičkom prostoru, tvrdio je 2016. da je „zbog visoke monopolističke prirode sustava informacijske tehnologije, malo vjerojatno da će biti dva različita sustava za vojnu i civilnu uporabu … iznimno je potrebno [za Kinu] integrirati vojne i civilne resurse putem sustava vojno-civilne fuzije.”[11]

6. **Kada raspravlja o postavljanju standarda sa stranom javnošću, kineska vlada naglašava suradnju koja je isplativa za sve uključene strane. Ali u domaćim raspravama naglašava konkurentnu vrijednost standarda za uspostavu tehnološke dominacije i, u skladu s tim, potrebu za izgradnjom „moći diskursa“ u globalnom IT razvoju.** Xi tvrdi da u kibernetičkoj sigurnosti i telekomunikacijama „igra velike moći nije samo igra tehnologije, već i igra ideja i moći diskursa”, što se odnosi na upravljanje internetom i standarde.[12] Drugi izvori nadovezuju se na Xijeve riječi, ukazujući kako Kina radi na postavljanju standarda u tehnologiji 5G, i na širem području IT-a, kako bi pretekla Zapad i time si omogućila gospodarske i vojne prednosti. Ukratko, oni „koji postavljaju standarde, stječu svijet.”[13]

Ovo izvješće započinje pregledom strateškog okvira u koji se uklapaju telekomunikacijske ambicije Pekinga, koncepta „velike cyber sile”, koji je prvo predstavio Xi 2014., koji obuhvaća velike ambicije za preuzimanje četvrte industrijske revolucije. Unutar tog okvira sljedeći odjeljci istražuju specifične elemente pekinškog diskursa o telekomunikacijama i IT-u, kao i kontrast između vanjskih i unutarnjih poruka. Prvi se fokusira na relativno obrambeni element: opasnost ovisnosti o stranim „temeljnim tehnologijama” i potreba za industrijskom politikom, umjesto oslanjanja na tržišne snage, kako bi se ta opasnost nadoknadila. Sljedeći odjeljak govori o kineskoj raspravi o mrežnoj i kibernetičkoj sigurnosti: s jedne strane, neuvažavanje vanjske zabrinutosti za sigurnost zbog kineskih sustava i tehnologija od strane Pekinga, a s druge strane preokupacija Pekinga s kibernetičkom i mrežnom sigurnošću te ulozi koju tu igraju domaći proizvodni faktori; nadalje, sugestije da Peking međunarodne, komercijalne informacijske mreže zapravo vidi kao sredstva za projiciranje ofenzivne moći. Zadnji odjeljak istražuje ambicije Kine za postavljanje standarda i odgovarajući napor u svrhu stjecanja strukturne snage.

Napomena o metodologiji

U procjeni vanjskog diskursa, ovo izvješće u prvom redu oslanja se na službene diplomatske izjave i primjedbe glasnogovornika Ministarstva vanjskih poslova Kine. One su namijenjene stranoj javnosti.

Za domaći diskurs, izvješće se okreće širem rasponu izvora, uključujući govore i članke Xija i drugih osoba na visokim funkcijama u kineskoj vladi usmjerene na domaću javnost, kao i desecima mjerodavnih listova povezanih s elementima stranačke države, od MIIT-a do Narodne oslobodilačke vojske (PLA).

Izvori koji se ne mogu osobno pripisati Xiju, moraju se smatrati manje mjerodavnim i stoga im se mora pridati manja vrijednost nego onima s njegovim imprimaturom. Čak i unutar kineskog centraliziranog sustava vlasti, visoki dužnosnici vjerojatno imju različita mišljenja; čak i unutar relativno kontrolirane visoke akademske zajednice u Kini (npr. Kineska akademija znanosti), stručnjaci se vjerojatno u elementima svojih analiza razlikuju od vladina vodstva. Unatoč tim ograničenjima, autori ovog izvješća smatraju da su neslužbeni ili manje službeni izvori ključni za razumijevanje kineskih konkurentnih okvira i ambicija. Xi vjerojatno neće vrlo detaljno govoriti o određenoj tehnologiji ili tehnološkoj primjeni. Ali službenici u MIIT-u ili Ministarstvu znanosti i tehnologije vjerojatno hoće. Visoki dužnosnici vlade, čije izjave podliježu redovitom nadzoru, također vjerojatno neće raspravljati o osjetljivim temama (npr. vojnoj primjeni tehnologije 5G), ali izoliraniji akademski i komercijalni izvori hoće. Vladine izjave obično odražavaju politiku kakva ona trenutno je, ali akademske i komercijalne rasprave mogu pružiti uvid u razvoj i nove trendove.

Ovo izvješću nastoji provjeriti mjerodavnost svih izvora koji se upotrebljavaju, usput pružajući kontekst. Mjerodavnost izvora ocijenjena je na temelju autora, izdavača i stupnja u kojem su argumenti nalik ostalim naporima kineskog strateškog diskursa. Ova metodologija ne pretpostavlja da bilo koji pojedinačni izvor pruža savršeno objašnjenje. Umjesto toga, cilj je predstaviti relativno sveobuhvatnu i izravnu zbirku izvora koji zajedno odražavaju interni govor Kine o telekomunikacijama i IT-u na strateškoj razini.

Ambicija: Kina kao „velika cyber sila”

„Izgradnja Kine u „veliku cyber silu” dugoročan je i složen sustavan strateški projekt koji uključuje sve aspekte gospodarstva i društva.”

– Chen Zhaoxiong, zamjenik ministra industrije i informacijske tehnologije, 2017.[14]

Xi je predstavio koncept „velike cyber sile” (网络强国), koji je također preveden kao „velika mrežna sila”[15], u veljači 2014. pri pokretanju tijela najviše razine za internetska pitanja Kineske komunističke stranke: Središnje vodeće male grupe za kibernetičku sigurnost i informatizaciju.[16] Zatim, Xi je postavio postajanje „velikom cyber silom” temeljem kineske internetske politike, što je kritičan korak prema ostvarivanju stogodišnjih ciljeva partije, odnosno ključnih koraka koje partija želi postići do stogodišnjice njezina utemeljenja (2021.) i njezine pobjede u kineskom građanskom ratu (2049.).[17] Koncept velike cyber sile postao je rasprostranjen u službenom kineskom diskursu. Pojavio se kao ključni okvir za kinesku strategiju u telekomunikacijama i na širem području IT-a, a izraz „velika cyber sila” pojavio se u naslovu gotovo svakog važnog Xijeva govora o kineskoj telekomunikacijskoj i mrežnoj strategiji usmjerenoj domaćoj javnosti od 2014.

Međutim, izraz se rijetkoupotrebljava u porukama usmjerenima na vanjsku stranu javnost. Pojavljuje se samo jednom u šest godina u izjavama glasnogovornika Ministarstva vanjskih poslova.[18] Rijetke reference na „veliku cyber silu” u vanjskim porukama sugeriraju da Peking namjerno smanjuje opseg svojih ambicija pri komunikaciji sa stranom javnosti. Takav oprez nije neopravdan: na temelju Xijovih govora i izjava povezanih dužnosnika, u ovom odjeljku utvrđeno je da koncept velike cyber sile predlaže upravo takvu vrstu velikih, konkurentnih ambicija koje će vjerojatno povećati strane alarme.[19]

Xi izričito tvrdi da je njegov program globalan: velika cyber sila ima globalan utjecaj. Na Svjetskoj internetskoj konferenciji 2015. godine izjavio je sljedeće: „Kina će snažno provoditi strategiju koja će Kinu učiniti velikom cyber silom”, među ostalim izgradnjom „zajednice zajedničke sudbine u kibernetičkom prostoru“, globalne internetske infrastrukture i odgovarajućih normi za upravljanje internetom.[20] Slično tome, članak iz 2017. godine u glavnom listu partije Qiushi, koji su napisali dužnosnici Kibernetičke administracije Kine (CAC),[21] opisuje produbljivanje utjecaja Kine na globalno upravljanje internetom kao ključan cilj u razvoju statusa velike cyber sile.[22]

Ova vizija globalne velike cyber sile počiva na konkurentnoj orijentaciji. Xi predstavlja informatičku revoluciju kao priliku da se nadoknadi relativno nepovoljan položaj Kine u prethodnim industrijskim revolucijama. Predlaže koncept velike cyber sile kao putokaz. U govoru iz 2016. godine u kojem se dotaknuo brojnih tema, Xi je objasnio važnost postajanja velikom cyber silom u kontekstu poniženja koje je Kina pretrpila u Opijumskim ratovima i neuspjeha zemlje da se industrijalizira u 20. stoljeću.[23] Primijetio je kako je Kina propustila industrijsku revoluciju, ali će preuzeti informatičku revoluciju. U ovoj borbi za kibernetički prostor, prema Xiju „pobjednici će se radovati, a gubitnici će propasti."[24]

Kineski dužnosnici ponavljali su tu ideju. Na primjer, zamjenik ministra MIIT-a Chen Zhaoxiong tvrdio je u članku iz 2019. objavljenom u listu Journal of Military-Civil Fusion in Cyberspace (List o vojno-civilnoj fuziji u kibernetičkom prostoru) da je sadašnjost trenutak povijesnog značaja koji će oblikovati ravnotežu moći u globalnoj politici i ekonomiji, i u skladu s tim trenutak u kojem Kina ima priliku preuzeti novu moć. „Trenutno i buduće razdoblje velika je strateških prilika za Kinu da se iz značajne zemlje proizvođača i značajne cyber zemlje pretvori u veliku zemlju proizvođača i veliku cyber silu",[25] napisao je. Nudi širi strateški kontekst: „Tijekom povijesti svjetske civilizacije, svaka tehnološka revolucija i industrijska promjena donijela je nesagledive učinke i utjecaje na ljudsko društvo, što je potaklo temeljitu prilagodbu svjetske ekonomske i političke strukture." U tim vremenima promjene, tko god može „shvatiti povijesni trend" i „napraviti prvi potez" može postići „nagli razvoj" i iskoristiti konkurentske prednosti.[26]

U članku iz 2017. u listu People's Daily, Chen je također naglasio kako je natjecanje u kibernetičkom prostoru natjecanje velikih sila i da projekt velike cyber sile ovisi o kineskoj pobjedi u tom natjecanju. Objasnio je da je „kibernetički prostor postao nova arena za velike zemlje" i mnoge „veće zemlje na svijetu smatraju internet strateškim smjerom budućeg natjecanja." Kao rezultat toga, oni „promiču i primjenjuju nove generacije mrežne informacijske tehnologije" i „natječu se za vodstvo u kibernetičkom prostoru."[27] Kina nije iznimka: u svjetlu „sve žešćeg međunarodnog natjecanja, [Kina] mora hitno iskoristiti nove prilike ovog novog doba" i „ubrzati izgradnju novih prednosti u međunarodnom natjecanju", kao i suradnju u digitalnom dobu. Kina mora „preuzeti vodstvo tehnološke konkurencije povezane s dugoročnim i ukupnim stanjem."[28]

Ova logika da infomatička revolucija pruža konkurentnu priliku za Kinu da se naglo uzdigne na vrh globalnog reda posebno se spominje u raspravama o telekomunikacijama. „Tehnologija 5G sve više pridaje strateško vodstvo za osvajanje dugoročne konkurentne prednosti zemlje", napisao je Duan Weilun,[29] zamjenik ravnatelja Ureda vodeće skupine za reformu opsežnog produbljivanja u grupi Datang Telecom Group, u članku iz 2020. godine.[30]

Članak iz 2020. u listu Party & Government Forum (Forum stranke i vlada), listu kojeg vodi Stranačka škola Kineske komunističke stranke (CCP, Chinese Communist Party), izravniji je: „Prije doba interneta, europske i američke zemlje imale su vodeću ulogu u ustroju novog svjetskog gospodarskog reda, političkog reda i pravnog poretka", ali „u doba interneta, posebice u novom razdoblju informatizacije koje predvodi tehnologija 5G, u potpunosti je moguće da Kina stekne prednost i postigne veće doprinose." Taj članak ne ostavlja sumnju u ono što će kineski doprinosi uključivati: „U doba interneta, tko god ima moć diskursa [话语权] i moć donošenja pravila, [规则制定权] ima moć voditi poredak budućnosti [主导权]." Iz te perspektive, tehnologija 5G pruža „povijesnu priliku" za vodstvo na više područja osim same tehnologije i priliku za „poboljšanjem međunarodne konkurentnosti Kine", unatoč tome što je propustila prošle, slične revolucionarne promjene.[31]

Indigenizacija: Ovisnost kao „skrivena opasnost" Kine

„Kontrola drugih nad temeljnom tehnologijom naša je najveća skrivena opasnost."
—Xi Jinping, 2016.[32]

Ako je ambicija za postajanjem velike cyber sile prigušena u vanjskim porukama o kineskim digitalnim planovima, sastavni dijelovi tih planova obično su potpuno krivo predstavljeni. Naglasak koji Peking stavlja na domaće temeljne tehnologije i na neadekvatnost tržišnih mehanizama da ih zaštiti, pružaju očit i jasan slučaj.

U porukama za vanjsku javnost, kineska vlada i komercijalni izvori često tvrde kako bi slobodna tržišta, a ne politika, trebala odrediti telekomunikacijski krajolik. Na primjer, glasnogovornici Ministarstva vanjskih poslova vanjskoj javnosti često naglašavaju važnost tržišnih načela pri donošenju odluka o tehnologiji. Nekoliko glasnogovornika tvrdilo je da je „pošteno, pravedno, otvoreno i nediskriminirajuće poslovno okruženje" nekompatibilno s ograničenjima i zabrinutostima koje se iskazuju prema tvrtki Huawei.[33] Glasnogovornica Ministarstva vanjskih poslova Hua Chuniying istaknula je u srpnju 2020. da su takva ograničenja „očiglena kršenja načela tržišnog gospodarstva i pravila slobodne trgovine", a odluka Ujedinjenog Kraljevstva da ih provodi pokazuje da su Britanci „protiv međunarodne zajednice".[34] Na drugoj tiskovnoj konferenciji tvrdila je da „ono što je SAD učinio jasno pokazuje da je borba za tržišno gospodarstvo i načelo pravednog tržišnog natjecanja od strane SAD-a samo varka" i da ponašanje SAD-a „krši pravila međunarodne trgovine".[35]

Međutim, Xijove izjave usmjerene domaćoj javnosti, kao i one ostalih osoba u kineskoj vladi i komercijalnom okruženju, imaju drugačiji ton. Naglašavaju važnost, ako ne i prioritet, smanjenja ovisnosti o stranim izvorima temeljne tehnologije (核心技术) i odgovarajućim ograničenjima slobodnih tržišta. U skladu s tim, podupiru potrebu za provedbom industrijske politike. Takva industrijska politika usmjerena je na lance proizvodnje i opskrbe kao i na istraživanje i razvoj. Također služi ustroju bliske suradnje između vlade i privatnog sektora u svojim domaćim i međunarodnim operacijama.

Xi je u više navrata naglasio unutarnju snagu i relativnu neovisnost u temeljnoj tehnologiji kao ključne čimbenike u izgradnji velike cyber sile. Naglašava to dok Kina izvozi tehnologiju koja stvara međunarodno oslanjanje na nju. U svojem prvom važnom obraćanju kojim je naglašen koncept postajanja „velikom cyber silom" 2014. godine, Xi je istaknuo potrebu smanjenja oslanjanja na stranu tehnologiju i „jačanja autohtonih inovacija (自主创新) temeljnih tehnologija i izgradnje infrastrukture".[36] Tvrdio je kako „da bi se Kina izgradila u veliku cyber silu, Kina mora imati vlastitu tehnologiju, i mora imati snažnu tehnologiju."[37] Važno je da je taj govor, a s njim i rasprava Kine o raspletu uzajamne tehnološke ovisnosti prethodila izboru Donalda Trumpa, trgovinskom ratu i američkoj retorici koja se može sažeti kao usredotočenje na „razdvajanje".

Xi je objasnio svoju usmjerenost na temeljnu tehnologiju u velikom govoru o internetskoj politici 2016. godine, također prije izbora u SAD-u. U tom je govoru Xi ponudio opširnu definiciju „temeljne tehnologije": „Po mom mišljenju, može se shvatiti iz tri aspekta. Jedan je aspekt osnovna tehnologija i općenita tehnologija; drugi je asimetrična tehnologija ili tehnologija „ubojičinog buzdovana"; a treći je najnovija tehnologija i disruptivna tehnologija."[38] U zamjetnom dodatku, Xi je naveo da je ključ u sljedećem: „u tim poljima na istoj smo početnoj liniji kao i strane zemlje. Ako se možemo unaprijed pripremiti i fokusirati na istraživanje, vrlo je moguće ostvariti transformaciju od trčanja za drugima do trčanja ispred drugih i vođenja."[39] Drugim riječima, elementi temeljne tehnologije ne identificiraju se samo zbog njihove temeljne prirode, već i zbog trenutnog konkurentnog statusa Kine u temeljnim tehnologijama i potencijala za konačno vodstvo koji daju Kini.

Unatoč toj povoljnoj sveukupnoj prognozi, Xi je na drugom mjestu govorio o postojećim tehnološkim nedostacima Kine. „U usporedbi s naprednom razinom svijeta i u usporedbi s našim strateškim ciljem da se izgradimo u veliku cyber silu, još uvijek postoji jaz u mnogim aspektima", kazao je dodajući: „Najveći jaz leži u temeljnoj tehnologiji."[40] Naglasio je opasnosti koje dolaze uz to. „Temeljna tehnologija interneta naša je najveća „glavna arterija"", Xi je izjavio s izrazom (命门) koji se odnosi na vitalno područje tijela odgovornog za disanje, razgradnju i reprodukciju.[41] „Kontrola drugih nad temeljnom tehnologijom naša je najveća skrivena opasnost."[42]

Stoga je ključno za Kinu da ojača svoju temeljnu tehnologiju. „Ako želimo obuhvatiti inicijativu kineskog razvoja interneta i osigurati sigurnost interneta i nacionalnu sigurnost, moramo riješiti problem temeljne tehnologije i nastojati postići „pretjecanje na krivulji"[43] u određenim područjima."[44] Xi je ovu tvrdnju opravdao jezikom koji se odnosi na vanjsku ovisnost o Kini kao i na ovisnost Kine o drugima:

> Bez obzira na veličinu internetske tvrtke, bez obzira na njezinu tržišnu vrijednost, ako uvelike ovisi o stranim zemljama u svojim temeljnim komponentama i ako je „glavna arterija" opskrbnog lanca u rukama drugih, to je kao da gradite kuću na tuđim temeljima. Koliko god da je velika i prekrasna, neće se moći suprotstaviti vjetru i kiši i bit će toliko ranjiva da će se možda urušiti pri prvom udarcu.[45]

Xi stoga poziva na snažnu industrijsku politiku. Kina bi morala „uložiti više ljudskih, materijalnih i financijskih sredstava u temeljna tehnološka istraživanja i razvoj", kao i „prikupiti naše najbolje snage i izraditi strateške sporazume" za daljnji napredak. Kina bi trebala „sastaviti nacrt razvojne strategije za temeljnu tehnologiju i opremu u informacijskom polju" i „sastaviti plan, raspored, popis zadataka, kao i kratkoročne, srednjoročne i dugoročne ciljeve." I Kina bi se morala "usredotočiti na penjanje na položaj strateškog vodstva."[46]

Xi je predložio da Kina tako učini u skladu s nekom vrstom kompromisa između potpunog protekcionizma[47] i integracije slobodnog tržišta.[48] „Temeljna tehnologija važno je oružje zemlje, a najkritičnija i temeljna tehnologija mora se temeljiti na autohtonim inovacijama i samooslanjanju", istaknuo je. Slobodno tržište ne bi bilo dovoljno. Tržišna razmjena ne može donijeti temeljne tehnologije, a novac ne može kupiti temeljne tehnologije. Moramo se osloniti na vlastito istraživanje i razvoj." U isto vrijeme, u globaliziranom okruženju ne može se očekivati da će se takvo istraživanje i razvoj dogoditi „iza zatvorenih vrata". Xi je objasnio da „samo kad se borimo protiv gospodara, možemo spoznati jaz" u sposobnosti.[49] Kina „ne bi odbila novu tehnologiju". Umjesto toga, strateški bi odlučila „koje se mogu uvesti [iz inozemstva], probaviti, apsorbirati, a zatim ponovo inovirati", a „koje moraju biti autohtone i samostalne inovacije."[50]

Xi je dodatno pojasnio da će industrijska politika Kine voditi i podupirati opskrbne lance i proizvodnu bazu, kao i istraživanje i razvoj. Objasnio je da bi bez čvrste proizvodne baze za temeljne tehnologije kapacitet bio „gubitak posla" i da „u globalnom informacijskom polju sposobnost integracije lanaca inovacija, proizvodnih lanaca i vrijednosnih lanaca sve više postaje ključ uspjeha ili neuspjeha", a da bi se to učinilo „konačni rezultat tehnološkog istraživanja i razvoja u temeljnoj tehnologiji ne bi trebali biti samo tehnička izvješća, znanstveni istraživački dokumenti i laboratorijski uzorci, već bi [također] trebali biti tržišni proizvodi, tehnička snaga, i industrijska snaga".[51] Drugim riječima, znanstvena istraživanja mogu dati dovoljan povrat samo ako ih podržavaju opskrbni lanci i snaga proizvodnje.

Kako u domaćoj, tako i u međunarodnoj primjeni, ova industrijska politika zahtijevala bi blisku suradnju između kineske vlade i korporativnih igrača. Xi je u svojem govoru iz 2016. objasnio kako je privatnim poduzećima također potrebna država, iako je „sudbina [tehnoloških] poduzeća usko povezana s razvojem zemlje". „Bez državne potpore, bez potpore [kineskog naroda], bez služenja zemlji i narodu, poduzećima je teško ojačati i narasti."[52] Državna potpora proširile bi se na strane operacije poduzeća: kao što je Xi tvrdio 2016., „moramo poticati i podržavati kineske internetske tvrtke da postanu globalne … i aktivno sudjelovati u izgradnji „pojasa i puta" kako bi se postiglo načelo „gdje god su naši nacionalni interesi, [naša] informatizacija [tehnologija] također će obuhvaćati ta područja."[53] Xi se još nije osvrnuo na pitanje stvaraju li te globalne ambicije za ostatak svijeta opasnu ovisnost o stranim (u ovom slučaju kineskim) tehnologijama, pitanje koje je Peking odlučan razriješiti na vlastitom tržištu.

Članak Chena Zhaoksionga iz 2019. godine posebno je usmjeren na nedostatke tržišnih snaga kada je riječ o razvoju temeljne tehnologije i stoga na potrebu za industrijskom politikom. „Novac i tržište", piše Chen, nijedno nije „donijelo temeljnu tehnologiju operativnog sustava" niti je dopustilo da ta tehnologija bude „probavljena, apsorbirana i ponovo inovirana." Kina stoga nije imala izbora nego podržati „autohtone inovacije" kako bi mogla „izgraditi siguran sustav informacijske tehnologije kojim se može upravljati."[54]

Drugi kineski izvori primjenjuju taj okvir izravno na tehnologiju 5G. Na primjer, članak iz 2017. godine u listu Communications World (Svijet komunikacija) koji je povezan s MIIT-om, potiče vladu da „koordinira operatere i povezane odjele radi učinkovitog uvođenja nacionalnog eksperimentalnog plana za pripremu tehnologije 5G za komercijalnu uporabu", plan koji je Kina u konačnici započela provoditi 2020. godine.[55] Slično tome, autori sa sveučilišta Shanxi tvrdili su u članku iz 2020. godine u listu International Economics and Trade (Međunarodna ekonomija i trgovina) da izgradnja industrije tehnologije 5G zahtijeva „vrhunski dizajn" od strane državnih nacionalnih upravnih odjela te da vlada mora „također pružiti financijsku potporu". To pripisuju „dugoročnom razvoju i istraživanju koje zahtijeva veliku količinu novaca" koje je potrebno za visokotehnološku industriju kao što je tehnologija 5G. Drugim riječima „država provodi vrhunski dizajn na strateškoj razini i racionalno upotrebljava fondove za potporu industriji."[56]

Kibernetička i mrežna sigurnost: „Napadački i obrambeno”

„Bez kibernetičke sigurnosti nema nacionalne sigurnosti.”

—Xi Jinping, 2014.[57]

Kineske vanjske poruke o kibernetičkoj i mrežnoj sigurnosti također omalovažavaju rizike koje strane tehnologije, kao što su Huawei, mogu predstavljati u informacijskim sustavima. Međutim, domaći diskurs kineske vlade daje prednost sigurnosti i predstavlja „neovisne [IT sustave] kojima se može upravljati“[58] kao sredstvo za postizanje tog cilja. Nadalje, kineski akademski i komercijalni razgovori o uvredljivim primjenama informativnih mreža ukazuju na to da su sigurnosni problemi u pogledu kineskih sustava opravdani. Peking možda vidi komercijalne telekomunikacije i druge IT mreže kao sredstva za projiciranje vojne snage i oblikovanje globalnog sustava i prikaza prema svojim interesima.

Glasnogovornica Ministarstva vanjskih poslova Hua Chuniying opisala je zabrinutost u pogledu kibernetičke i mrežne sigurnosti kao primjere zemalja koje „politiziraju komercijalna i tehnološka pitanja pod svaku cijenu”. Tvrdila je 2020. godine da ograničenja za tvrtku Huawei „nisu stvar nacionalne sigurnosti, već političke manipulacije.”[59] Još izravnije, Hua je također izjavila kako je „promicanje nacionalne sigurnosti” tako jadan izgovor američke strane” te da se strane zabrinutosti temelje na politiziranim, „nepostojećim rizicima”[60] koji se temelje na „prekomjerno rastegnutom konceptu nacionalne sigurnosti”.[61]

Neovisne tehnologije za kibernetičku i mrežnu sigurnost

Ako su Sjedinjene Američke Države preuveličale koncept nacionalne sigurnosti, Pekingov domaći diskurs pokazuje da Peking dijeli istu krivnju. Takav diskurs naglašava ključnu važnost sigurnosti u informacijskim mrežama, pozivajući na usvajanje neovisnih tehnologija kojima se može upravljati. U istom govoru iz 2014. godine u kojem je Xi uveo koncept „velike cyber sile” i pokrenuo malu vodeću grupu čiji je zadatak provedba tog cilja, izjavio je, „bez kibernetičke sigurnosti [ili mreže][62] nema nacionalne sigurnosti”.[63] Također je uveo izraz koji je postao glavno uporište kineskog diskursa o telekomunikacijama. „Kibernetička sigurnost i informatizacija dva su krila jednog tijela i dva kotača jednog motora”, rekao je. „Moraju se planirati, rasporediti, razvijati i provoditi na jedinstven način.”[64] Drugim riječima, sigurnost je u središtu kineskih digitalnih ambicija. Ova ključna uloga sigurnosti u izgradnji „velike cyber sile” gotovo se stalno pojavljuje u Xijovim velikim govorima o toj temi.[65]

Rasprava koja se prenosi iz Xijovih primjedbi naglasak na sigurnost posebno primjenjuje na telekomunikacije. Istraživači istraživačkog tehnološkog centra Političkog i pravnog odbora Središnje vojne komisije (军委政法委侦查技术中心) naglasak stavljaju na sigurnost tehnologije 5G:

> Kao napredna komunikacijska tehnologija današnjice, široka primjena tehnologije 5G donijet će nove promjene u proizvodnji i životu cijelog društva. Sigurnosna pitanja povezanih tehnologija i aplikacija povezana su sa javnom socijalnom sigurnošću i vojnim interesima i trebala bi biti uključena kao glavni čimbenici iz perspektive sveukupne nacionalne sigurnosti.[66]

Domaći kineski diskurs ukazuje na tehnologije i sustave „kojima se može upravljati" (可控) kao sredstva za postizanje sigurnosti. Xi je 2016. godine objasnio da bi Kina trebala razmotriti jesu li tehnologije „sigurne i može li se njima upravljati" prije nego ih uvede.[67] Također je 2016. godine rekao kako Kina mora „izgraditi siguran sustav informacijske tehnologije kojim se može upravljati."[68]

Drugi izvori oštrije naglašavaju imperativ domaćih tehnologija. U članku iz 2019. godine u listu Journal of Military-Civil Fusion in Cyberspace (Časopis o vojno-civilnoj fuziji u kibernetičkom prostoru), Chen Zhaoksiong tvrdio je da Kina mora „izgraditi siguran sustav informacijske tehnologije kojim se može upravljati" i to učiniti putem „autohtonih inovacija".[69] U članku iz 2015. godine, istraživač sa Šangajske akademije društvenih znanosti objasnio je sigurnosne rizike oslanjanja na vanjske IT tehnologije: „Kasno smo započeli s informacijskom tehnologijom, oslanjajući se na zapadne tehnologije za temeljne tehnologije kao što su čipovi i operativni sustavi." To je stvorilo ranjivost: „Zapadne zemlje, koje predvode Sjedinjene Američke Države, iskorištavaju tehnološku industriju za razvoj i prilagodu različitih oružja za cyber napad za postizanje kibernetičkog nadzora, kibernetičkih napada i kibernetičkog odvraćanja." Zaključuje: „Ako temeljne tehnologije nisu neovisne i ako se njima ne može upravljati, mreža koju gradimo bit će „nezaštićena mreža".[70]

Militarizirane tehnološke informacijske mreže

Na sljedećoj razini, analiza akademskih i komercijalnih izvora ukazuje na to da vanjska zabrinutost za sigurnosti zbog kineskih tehnologija i sustava nije neutemeljena i da Peking komercijalne i civilne IT mreže možda vidi kao alate za projiciranje ofenzivne moći.[71] Ta projekcija moći može imati mnogo oblika. Na najtradicionalnijoj razini kineski je diskurs prepun rasprava o informativnim mrežama, uključujući telekomunikacije, sustave vojno-civilne fuzije i vojne primjene tehnologije 5G.

Vojno-civilna fuzija odnosi se na integraciju vojnih i civilnih resursa, aktera te na pozicioniranje u svrhu ujedinjenog cilja.[72] Xi je 2015. godine podigao civilno-vojnu fuziju na razinu nacionalne strategiju.[73] Često je naglašavao ključno mjesto IT-a u toj strategiji: Na nacionalnoj stručnoj konferenciji o kibernetičkoj sigurnosti i informatizacijskom radu 2018. godine Xi je rekao: „Vojno-civilna fuzija u kibernetičkoj sigurnosti i informatizaciji ključno je i granično područje za vojno-civilnu fuziju, a ujedno je i najdinamičnije područje i područje s najvećim potencijalom za napredovanje u vojno-civilnoj fuziji."[74]

Daljnje kineske rasprave još su izravnije o odnosu između informativnih mreža i vojno-civilne fuzije što ukazuje na to da komercijalne mreže mogu služiti u vojne svrhe. Na primjer, Qin An 2016. je godine tvrdio da je „zbog visoke monopolističke prirode sustava informacijske tehnologije, malo vjerojatno da će biti dva različita sustava za vojnu i civilnu uporabu", a dva sustava u stvarnosti će biti jedan sustav. Nadalje, s obzirom na „trenutačne tehnološke temelje Kine … težak je zadatak za Kinu" izgraditi sustav koji može konkurirati naprednim standardima svijeta. Stoga je „posebice potrebno [za Kinu] integrirati vojne i civilne resurse putem sustava vojno-civilne fuzije".[75]

Isto tako, Duan Weilun je 2020. godine pozvao Kinu na „jačanje osnovnih općih tehnologija mrežnog sustava tehnologije 5G za vojnu i civilnu uporabu, podržavanje detaljnog razvoja vojno-civilne fuzije tehnologije 5G i njezine tehnološke evolucije i promicanje opsežne primjene autonomnih tehnologija 5G i tehnologija 5G kojima se može upravljati u vojnoj opremi".[76]

Članak u listu National Defense (Nacionalna obrana) istraživača Akademije vojne znanosti razvio je ideju o fuziji korak dalje. Autori predlažu da „vojna primjena tehnologije 5G treba slijediti evolucijske zakone informatizacije" koji uključuju „globalno prodiranje" tehnologije 5G i „sveobuhvatno povezivanje" između vojnih i civilnih sposobnosti. U skladu s tim tvrde da bi kineska izgradnja tehnologije 5G trebala izgraditi „blisku vezu između vremena mira i vremena rata".[77]

Taj okvir sugerira da bi pristupi Kine tehnologiji 5G i drugim informacijskim mrežama, kao i tehnologijama i aplikacijama koje su na njima izgrađene, mogli sadržavati vojnu korisnost sa stajališta dizajna. Dodatni izvori nude uvid u specifične vojne implikacije.

Sposobnosti informiranja u središtu su kineskog programa vojne modernizacije.[78] Kao što je Zheng Anqi iz Kineske akademije informatičke i komunikacijske tehnologije rekao 2020. godine: „Ako moderne vojne sile imaju jaku informativnu moć, imaju jaku vojnu moć."[79] Prema Zhengu vojska mora „shvatiti temu doba u vojnom području informacija jer zemlja provodi strategiju mrežne snage, apsorbirati i učiti od potpuno novih informacijskih tehnologija i koncepata te iskoristiti razvoj tehnologije 5G za upotrebu interneta stvari, velikih podataka, i računalstva u oblaku."[80] Zheng zaključuje: „Temelj informacijske snage je mreža. Bez podrške sveprisutnih, širokopojasnih i mobilnih mreža, moćna informacijska vojska je samo prazna priča."[81] Slično tome, istraživači na Akademiji vojnih znanosti objasnili su, također 2020. godine, da će Kina „u potpunosti razviti mogućnosti budućih komunikacijskih tehnologija, uključujući velike veze, nisku latenciju, veliku širinu pojasa i široku pokrivenost kako bi pružila snažniju znanstvenu i tehnološku podršku našem vojnom inteligentnom borbenom sustavu."[82]

Članak iz 2019. godine u listu China's National Defense (Kineska nacionalna obrana) koji su napisali vojni časnici i stalno osoblje Akademije vojnih znanosti nudi snažan sažetak vojnih primjena tehnologije 5G. Pišu da „tehnologija 5G ima jaku vrijednost vojne primjene. Od velikog je strateškog značaja iskoristiti priliku za vojnu primjenu tehnologije 5G."[83] U općenitom pogledu kineske vojne strategije i informatizacije vojske tvrde da je „tehnologija mobilne komunikacije pete generacije (tehnologija 5G) novi motor za nadogradnju mrežno-informativne industrije vojno-civilne fuzije i nova potpora snažnoj vojsci s pomoću informacija."[84] A autori ukazuju na to da se vojna vrijednost tehnologije 5G treba upotebljavati za ofenzivu, primjećujući da Kina mora „pažljivo proučavati i sveobuhvatno demonstrirati i formulirati strategiju naše vojske za razvoj tehnologije 5G za pobjedu nad neprijateljem."[85]

Ovi autori detaljno prikazuju niz slučajeva uporabe za tehnologiju 5G. Prvo, međusobno povezivanje, zapovjedništvo i kontrola na bojištu: primjećuju da kineska vojska traži „sveobuhvatnu integraciju umreženih sustava." U praksi taj je cilj „integrirati zajedničke operacije [diljem] trodimenzionalne informacijske mreže kopna, mora, zraka i prostora" gdje je „svaka borbena jedinica i čak oružana platforma, senzor i druga oprema za borbu … sigurno, brzo i besprijekorno povezana." Ti su ciljevi dugoročni, ali autori ističu da tehnologija 5G pruža potrebne mogućnosti za operativnost ove vizije umreženog bojišta: „Tehnologija 5G pruža tehničke uvjete za međusobno povezivanje različitih sustava naoružanja, informacijskih sustava te zapovjednih sustava i sustava kontrole." [86]

Drugo, napredni vojni alati: autori lista National Defense (Nacionalna obrana) ocrtavaju mnoštvo mogućnosti, od „projiciranih virtualnih holografskih slika", vojnog interneta stvari i vojnih robota, koje tehnologija 5G čini mogućima.[87]

Treće i šire, komunikacija na bojištu: „Različiti mobilni terminali mogu izravno upotrebljavati komunikacijske mreže tehnologije 5G za šifriranu komunikaciju podataka, čime se vojsci pruža integrirana komunikacija sa „širokom pokrivenosti, velikom brzinom i snažnom kompatibilnosti" na bojištu. Ti se mobilni terminali mogu integrirati s tradicionalnijim vojnim mrežama i opremom, uključujući „satelite za vojnu komunikaciju, zrakoplove za rano upozoravanje i druge resurse", tako da „komunikacija postiže gotovo neometane učinke, što može značajno smanjiti troškove vojnih operacija".[88]

Članak iz 2019. godine u listu Business Observation koji je napisao direktor odjela za računalstva u oblaku tvrtke China Telecom također tvrdi da „iz vojne perspektive … kvalitativni skok tehnologije 5G u brzini prijenosa i stabilnosti omogućuje toj tehnologiji da lako zadovolji potrebe budućih komunikacijskih zadataka na bojištu".[89] 5G mreže čak bi se mogle upotrebljavati za podršku globalno raspoređene Narodne oslobodilačke vojske (PLA):

> Kada se komunikacijski sustav tehnologije 5G razmjesti globalno, imat će iste ili čak veće mogućnosti pružanja usluga kao i vojni komunikacijski sustavi. Osim pristupa vojnim taktičkim komunikacijskim mrežama, različiti vojni mobilni terminali mogu i izravno koristiti 5G komunikacijske mreže za šifriranu podatkovnu komunikaciju, što pruža vojsci integrirane mogućnosti pričuvne komunikacije zrak-zemlja, što može znatno poboljšati mogućnosti informacijske podrške na bojištu.[90]

Stručnjaci Akademije vojnih znanosti dodali su logistiku kao još jednu vojnu primjenu u članku iz 2020. godine: „Tehnologija 5G donosi promjene modela, poboljšanja učinkovitosti i gospodarske koristi u području civilne logistike. Može se predvidjeti da će imati ključnu ulogu u izgradnji napredne vojne logistike"[91]

Sun Bolin iz Stručne savjetodavne radne skupine kineskog društva za automatizaciju sažima vrijednost tih vojnih zahtjeva u članku iz 2020. i opisuje scenarij za rat omogućen tehnologijom 5G koji naglašava prijetnju militarizirane telekomunikacijske mreže:

> Kada rat tek počne, tehnologija 5G mogla bi potpuno paralizirati protivničko zapovjedništvo, kontrolni sustav i sustav logističke podrške. Prije nego što bitka počne, ishod će već biti poznat. Tehnologija komunikacije 5G omogućit će vojsci integriranu informacijsku komunikacijsku mrežu zrak-zemlja sa širokim područjem pokrivenosti, prijenosom velike brzine i jakom kompatibilnosti, što će uvelike poboljšati mogućnosti informacijske podrške na bojištu.[92]

Informacijske mreže i nova vrsta sigurnosne prijetnje

Priroda projekcije snage s pomoću tehnologije 5G pruža mnogo više od tradicionalne sigurnosne domene. Kineska rasprava o kibernetičkoj i mrežnoj sigurnosti proizlazi iz širokog okvira onoga što sigurnost zahtijeva i ranjivosti koje IT stvara. Gospodarske, socijalne i informativne domene igraju ulogu uz vojno područje u ovom konceptu mrežne i kibernetičke sigurnosti. U tim područjima informacijske mreže mogu se upotrebljavati za djelovanje, prisilu ili destruktivnu svrhu, kao i za provođenje izravnog napada, kao što je, primjerice, širenje propagande ili oblikovanje tržišta kapitala.

Chen Baoguo iz Međunarodnog instituta za tehnologiju Državnoga vijeća pojasnio je u članku iz 2010. godine da je povećana izloženost vanjskim igračima koju je doveo napredak u IT-u riskirala zaobilaženje suvereniteta države:

> Nova generacija informacijske tehnologije … povećala je uzajamno prodiranje i međuovisnost među zemljama … Za zemlje je postalo teško uživati u suverenitetu unutarnjih poslova, diplomacije i vojske na tradicionalan i apsolutan način. Stoga, u doba informatizacije i gospodarske integracije, odluka bilo koje zemlje teško može biti vlastita odluka. U doba nove generacije informacijske tehnologije, tradicionalni apsolutni suverenitet i neovisnost zemlje sve su više oslabljeni, iznutra i izvana, novom generacijom informacijske tehnologije.[93]

U podršku ovog argumenta Chen ističe ovisnost nacionalnih i socijalnih sustava o informacijskim mrežama i, u skladu s tim, ranjivost koju te mreže stvaraju:

> Kao rezultat nove generacije revolucije informacijske tehnologije nacionalna sigurnosna pitanja više nisu ograničena na tradicionalnu vojnu i gospodarsku sigurnost. Cijelo društvo sve više ovisi o internetu. Razvoj nove generacije informacijske tehnologije postao je temelj društva 21. stoljeća, a internet je postao živčano središte zemlje. Financijski, komercijalni, prometni, komunikacijski, obrazovni, i zdravstveni sustavi koji djeluju putem interneta postali su temelj za nacionalni gospodarski i socijalni razvoj.[94]

Ukratko, informacijske mreže proširuju domenu nadmetanja i povezanosti, čime se povećava ranjivost. Mrežni napad može zaprijetiti „financijskim, komercijalnim, transportnim, komunikacijskim, obrazovnim, i zdravstvenim sustavima koji operiraju putem njega”.[95]

Drugi izvori nadilaze okvir područja ranjivosti koje su stvorile mreže kako bi istražili *vrste* prijetnji unutar njih. Posebice ukazuju ne samo na izravno sukobe, već i na utjecaj, odnosno rizik da bi se informacijski sustavi mogli upotrebljavati za oblikovanje državnih afera na način koji utječe na nacionalnu sigurnost i autonomiju. Liu Honglin iz šangajske Municipalne stranke Kineske komunističke stranke upozorio je 2011. godine na „kulturno prodiranje, ideološku infiltraciju i političku infiltraciju“ koje bi IT mogao dopustiti:

> U informacijskom dobu postoji više kultura i mnogo ideja. Zapadne zemlje koriste prednosti informacijske tehnologije za provedbu kulturnog prodiranja, ideološke infiltracije i političke infiltracije kako bi postigli političke ciljeve. To će nesumnjivo utjecati na ideologiju i ideološki temelj Stranke. Nadalje, informacijska mreža prekinula je jednosmjerni prijenos tradicionalnih medija „odozgo prema dolje”. Ako se otvori još većem interaktivnom informacijskom okruženju, kako će se naša stranka pridržavati marksizma i razvijati ga, oduprijeti se utjecaju misli i jačati privlačnost ideologije Stranke?[96]

Slično tome, Projekt Nacionalnog fonda za socijalnu znanost objavljen 2020. godine opisuje opasnost ideološke subverzije i „kulturološke erozije” koja se pojavljuje zbog tehnologije 5G i drugih, prekograničnih tehnoloških sustava: „U novom razdoblju, s inovacijama i primjenom novih tehnologija koje predstavljaju AI i 5G … nacionalna kulturna sigurnost suočava se s brojnim izazovima kao što su nedostatak inovacija u kulturnoj teoriji, slabost širenja glavne ideologije i slaba sposobnost rješavanja erozivnog učinka zapadne kulture.” Kao odgovor, u izvješću se navodi sljedeće: „naša zemlja treba, od visine makrostrateškog plana naconalne sigurnosti … izgraditi nacionalni sustav kulturnog osiguranja „unutarnjeg i vanjskog povezivanja” (内外联动), „napadački i obrambeno” (攻守兼备).”[97] Ta ideja o spajanju napada i obrane može značiti da se Peking ne namjerava samo zaštititi od vanjskog utjecaja koji se primjenjuje na informacijske mreže, već i da ih upotrebljava za vlastiti projekt.

Godine 2020. glasnogovornik Ministarstva vanjskih poslova Zhao Lijian sugerirao je da bi upotreba opreme tvrtke Huawei u drugim zemljama spriječila špijunažu Sjedinjenih Država: „Razlog zašto Sjedinjene Države potiskuju tvrtku Huawei može biti zato što se brinu da ako druge države upotrebljavaju tvrtku Huawei, Sjedinjene Države više neće moći proći kroz „stražnja vrata” i prisluškivati.”[98] Ta rečenica priznaje sigurnosnu prednost koja se može postići putem stranih informacijskih mreža. Također postavlja pitanje o tome kako se sigurnosna slika razvija kada takvu prednost zahtijeva igrač koji vidi komercijalne mreže kao bojišta vojnog i ideološkog sukoba.

U članak iz 2017. godine Long Zaiye, istraživač na Forumu za strategiju vojno-civilne fuzije na kibernetičkom prostor, nudi dojmljiv portret kineske fuzije napada i obrane u mrežnoj i kibernetičkoj sigurnosti:

> Na svom putovanju od veće cyber sile do velike cyber sile, Kina dugo vremena sudjeluje u teškim borbama s različitim protivničkim snagama. Moramo … koordinirati pitanja sigurnosti mreže i prepoznati da je internet približio neprijatelje i bojište. S trenutačnom pozadinom vremena, pobijedili smo u ukupnoj bitci protiv kontradikcija i sukoba, eliminirali prepreke … i učinkovito odgovorili na pitanja javne sigurnosti informacijskog društva s modelom za inspekciju mreže. Konkretna provedba usmjerena je na tri aspekta: Prvo, globalno istraživanje mete. Izviđanje u stilu mreže i grupne analize provode se na umreženim ciljevima na globalnoj razini, a označena su privremena sigurnosna područja i ključna područja pregleda. Drugi je aspekt detaljna istraga neprijateljskih meta. Za nacionalne ciljeve koji su uvrstili [Kinu] za glavnog strateškog protivnika ili su iskusili neprijateljstva, provodit ćemo ključne inspekcije i nasumične kontrole kako bismo ih identificirali. Treća je provjera borbenih ciljeva. Redoviti pregledavi država, tvrtki ili osobnih ciljeva koji mogu predstavljati opasnost [za Kinu] i zadržati mogućnost borbe protiv uništenja u bilo kojem trenutku.[99]

Postavljanje standarda: Potraga Kine za „moći diskursa”

„Trenutačno se igra kibernetičke sigurnosti velikih moći ne odnosi samo na igru tehnologije, već i na igru ideja i diskursa.”

—Xi Jinping, 2016.[100]

Informacijske tehnologije nude i suptilniji, sustavniji oblik projekcije moći: postavljanje standarda. Interni kineski diskurs predlaže konkurentske ambicije za postavljanje međunarodnih tehničkih standarda u svrhu povećanja globalne snage.

Taj okvir u potpunosti je odsutan u raspravama namijenjenima stranoj javnosti. U porukama Pekinga za vanjsku javnost postavljanje standarda predstavlja se kao uzajamno korisna domena te se poziva na suradnju i razvoj zajedničkih pravila unutar nje. Na primjer, u razgovoru o Inicijativi za globalnu sigurnost podataka 2020. godine, glasnogovornik Ministarstva vanjskih poslova Zhao Lijian tvrdio je da Kina nastoji „pružiti plan za formuliranje globalnih standarda”, oslanjajući se na uključive koncepte „uzajamnog poštovanja i zajedničkog upravljanja”, napore za „izgradnju uzajamnog povjerenja i produbljivanje suradnje”, potpore za „multilateralizam“ i nove načine „suradnje s drugima”. Zhao je izjavio da je „opsežno savjetovanje i zajednički doprinos zajedničkim povlasticama pravi put naprijed“ ako Kina želi izgraditi „zajednicu sa zajedničkom budućnošću u kibernetičkom prostoru.“[101] Slično tome, članak iz 2016. godine u listu People’s Daily navodi da „Kina i Sjedinjene Države trebaju mrežnu suradnju, a ne sukobe … obostrano korisnu suradnju i zajedničko istraživanje mrežnih pravila ponašanja”.[102]

Kineski interni diskurs donosi drukčiju priču. Postavljanje standarda nastaje kao sredstvo vođenja ili čak dominiranja budućom tehnologijom i, u tom smislu, vođenja ili dominiranja svjetskim poretkom koji je u razvoju. Standardi se dosljedno smatraju nultom sumom, konkurentnima i instrumentima nacionalne snage. Značajno drukčije od javne izjave Ministarstva vanjskih poslova, članak iz 2015. u listu Zhejiang Daily koji je napisao tadašnji zamjenik ravnatelja Ureda za istraživanje politike stranačkog odbora provincije Zhejiang pruža jezgrovit primjer konkurentne i strateška važnosti koju Kina pridaje standardima:

> U uvjetima gospodarske globalizacije i modernog tržišnog gospodarstva … Standardi predstavljaju vodstvo, snagu diskursa i moć kontrole. Stoga „tko stekne postavljanje standarda, stječe svijet" (“得标准者得天下”), a „prvorazredna poduzeća prodaju standarde. Drugorazredne tvrtke prodaju-marke, a trećerazredne tvrtke prodaju proizvode " (“一流企业卖标准、二流企业卖品牌、三流企业卖产品”).[103]

Najviše razine stranke, uključujući Xija, odrazile su taj naglasak na standarde. Također su naveli vladinu ulogu u vođenju napora u pogledu postavljanja tehničkih standarda. Xi je 2016. godine izjavio da će Kina „aktivno provesti strategiju standardizacije",[104] kako bi ojačala i izvozila kineske tehničke standarde.[105] „Moramo ubrzati unaprjeđenje međunarodne moći diskursa Kine i moći donošenja pravila u kibernetičkom prostoru i uložiti ustrajne napore u cilju izgradnje velike cyber sile", tada je rekao.[106] Peking je u ožujku 2018. pokrenuo Projekt kineskih standarda 2035 na čelu s kineskom Akademijom inženjerstva.[107] Nakon dvogodišnje istraživačke faze taj se projekt razvio u Istraživanje razvoja nacionalne strategije za standardizaciju u siječnju 2020.[108] „Glavne točke rada na standardizaciji iz 2020. godine" koje je u ožujku 2020. izdao kineski Nacionalni odbor za standardizaciju naveo je namjere „jačanja interakcije između strategije standardizacije i glavnih nacionalnih strategija."[109]

Ni domaći kineski diskurs ne sugerira da je proces postavljanja standarda proces suradnje. Direktor kineske Akademije znanosti primjetio je 2016. godine da će različiti „principi" koje je Xi postavio za upravljanje kibernetičkim prostorom „također biti prepoznati od strane svih zemalja na svijetu i postati osnovne norme za upravljanje internetom u svim zemljama."[110]

Ambicije Kine za standardizaciju proširene su diljem različitih područja. Primjenjuju se na brzu željeznicu kao i na telekomunikacije. Međutim, čini se da Peking posebno naglašava područja u kojima se još uvijek postavljaju globalni standardi, odnosno područja na kojima Kina ima priliku skočiti u vodstvo.[111] Na primjer, glavne točke rada nacionalne standardiziracije u 2020. godini ocrtavaju napore u novim industrijama (npr. inteligentna proizvodnja, novi energetski i energetski učinkoviti transportni sustavi, napredni materijali); emergentni prioriteti (npr. tehnologija za sprečavanje i kontrolu virusa COVID-19); biotehnologija (npr. materijali na biološkoj bazi i napredna medicinska oprema); uslužna infrastruktura (npr. e-trgovina, financije, društveni kredit i logistika); informacijska tehnologija (npr. internet stvari, računalstvo u oblaku, veliki podaci, tehnologija 5G, pametni gradovi, geografske informacije).[112]

Kao što taksonomija sugerira, tehnologija 5G i šira informacijska tehnologija igraju središnju ulogu u kineskom programu za postavljanje standarda. Kineska vlada podupire i organizira promicanje telekomunikacijskih standarda. Xi je 2016. godine izjavio kako će Kina „promicati reformu globalnog sustava upravljanja internetom" putem postojećih institucija kao što su Ujedinjeni narodi te putem novih kineskih mehanizama kao što su Belt and Road Initiative (Inicijativa pojasa i puta) i podređeni pokreti kao Digital Silk Road (Digitalni svileni put).[113] Zhao Dachun, predstavnik Nacionalnog narodnog kongresa i zamjenik glavnog direktora tvrtke China Mobile, objasnio je 2018. godine središnju ulogu države u organizaciji i promicanju telekomunikacijskih standarda. „U smislu utvrđivanja normi za tehnologiju 5G, dodjele spektra, izdavanja dozvola, tehničke provjere i industrijske promidžbe", istaknuo je, „vlada i relevantni odjeli izradit će dizajn na najvišoj razini i pružiti odgovarajuću potporu politike za ubrzavanje razvoja industrije tehnologije 5G."[114]

U drugom razmatranju uloge države u postavljanju standarda i naglasku na tehnologiju 5G, Tong Guohua, predsjednik i tajnik stranačkog odbora grupe China Information and Communication Technology Group, obećao je 2018. godine da „za budući razvoj industrije slijedimo upute glavnog tajnika Xija i strateško raspoređivanja državne uprave za nadzor imovine i administrativnu komisiju Državnog vijeća za oblikovanje šest industrijskih uređenja, prvenstveno fokusiranih na standarde tehnolgije 5G", među ostalim.[115]

U članku iz 2020. godine, Duan Weilun opisao je uspjeh tog pristupa:

> Nakon godina napora u kojima smo slijedili [ostale] u tehnologiji 2G, sustizanja u tehnologiji 3G, usklađivanja [s drugima] u tehnologiji 4G, Kina je ušla u prvi kamp razvoja tehnologije 5G na svijetu i preuzela vodstvo u tehnološkim inovacijama. Kineska poduzeća u potpunosti su sudjelovala u oblikovanju međunarodnih standarda tehnologije 5G, jačanju međunarodne suradnje u tehnologiji 5G te su surađivala s međunarodnim poduzećima u promicanju uspostave globalnog unificiranog standarda tehnologije 5G.[116]

Duan podržava ovu tvrdnju dokazima: „Od travnja 2019. broj primjena standardnih osnovnih patenta (SEP, Standards-Essential Patents) za komunikacijske sustave tehnologije 5G kineskih poduzeća rangiran je prvi na svijetu, što čini 34 %."[117] Ključni akteri koji su podnijeli te zahtjeve bili su Huawei, ZTE i Institut za telekomunikacijske znanosti i tehnologiju.[118] Duan zatim nastavlja predstavljati liniju napora kroz koje bi Kina mogla nastaviti svoj standardni uspjeh, pozivajući kineske tvrtke da se uključe u rad s Međunarodnom organizacijom za standardizaciju, Međunarodnom elektrotehničkom komisijom i Međunarodnom telekomunikacijskom unijom kako bi „aktivno sudjelovali u oblikovanju tehnologije 5G i drugih međunarodnih standarda za sigurnost informacijskih tehnologija nove generacije … i dodatno povećali međunarodni glas Kine i utjecaj u formulaciji međunarodnih standarda za sigurnost u mrežnom prostoru."[119]

Kineski diskurs jasno opisuje globalne, konkurentne ambicije u skladu s državnim naporima u oblikovanju telekomunikacijskih standarda. Članak iz 2019 autora na Akademiji vojnih znanosti[120] u listu China's National Defense nudi jasan sažetak uloga:

> Temeljna tehnologija 5G gotovo je potpuno nova. Tko god prvi ovlada modelom, arhitekturom i standardima tehnologije 5G, ima pravo govoriti u budućoj mobilnoj mreži i ima prednosti djelovati prvi u industrijskom lancu. Može zauzeti strateško vodeće mjesto u budućoj ekonomskoj trgovini i vojnom natjecanju.[121]

Ovi citati upućuju na to da će samo jedan igrač moći preuzeti tu „stratešku vodeću poziciju". Ista tvrdnja izravnije je izražena na drugim mjestima. Shenzhen Commercial Daily za tehnologiju 5G kaže da „pobjednik uzima sve" (赢家通吃) 2019. godine.[122] Miao Wei, šef Ministarstva industrije i informacijske tehnologije, sam je odobrio taj argument. U govoru 2020. godine, Miao Wei je rekao kako su „postojala tri globalna standarda u razdoblju tehnologije 3G, dva globalna standarda u razdoblju tehnologije 4G i jedan jedinstveni globalni standard u razdoblju tehnologije 5G".[123]

Zašto su standardi tehnologije 5G u kojima pobjednik uzima sve tako strateški važni? Djelomično zbog toga što, tvrdi Tong Guohua, ako Kina može odrediti te standarde, može lakše kontrolirati svoju tehnologiju i mreže, čime podržava nacionalnu autonomiju. „Samostalno svladavanje standarda i samostalna izgradnja mreža", napisao je 2018. godine, „uvelike jamči informacije, pa čak i nacionalnu sigurnost."[124]

Međutim, standardi tehnologije 5G i šire informacijske tehnologije nude i strateške, potencijalno napadačke i temeljne nagrade. Kineski diskurs ukazuje na to da će standardi informacijske tehnologije definirati arhitekturu novog svijeta informacijske tehnologije. Postavljanje tih standarda stoga nudi mogućnost pisanja pravila budućeg svijeta i samim time za pretjecanje ili zamjenjivanje zapadnjačkog reda. Članak iz 2020. u listu Chinese Cadres Tribune jasno ovo iznosi:

> U doba interneta, tko god ima moć diskursa i moć donošenja pravila, ima moć voditi poredak budućnosti … Prije doba interneta, europske i američke zemlje imale su vodeću ulogu u ustroju novog svjetskog gospodarskog reda, političkog reda i pravnog poretka" … Međutim „u doba interneta, posebice u novom razdoblju informatizacije koje predvodi tehnologija 5G, u potpunosti je moguće da Kina stekne prednost i postigne veće doprinose. Povijesna prilika koju donosi internet zasigurno će postati važan poticaj za povećanje međunarodne konkurentnosti Kine.[125]

Taj je opis „razdoblja informatizacije koje je stvorila tehnologija 5G" od ključne važnosti. Pomaže u objašnjenju iznimne važnosti koju Kina dodjeljuje tehnologiji 5G u njezinom velikom naporu da definira arhitekturu razdoblja informatizacije. Tehnologija 5G opisuje se kao vrsta standarda – sustav koji će osnažiti kaskadni skup tehnologija, sposobnosti i standarda te će stoga definirati veći ekosustav informacijske tehnologije. Zhao Dachun objasnio je to u kliničkom smislu u intervjuu 2018. godine:

> Istraživanje i razvoj tehnologije 5G važna je mjera za provedbu mrežne snage i razvoj digitalnog gospodarstva. Može potaknuti razvoj interneta stvari, industrijskog interneta stvari itd. i time omogućiti digitalnu transformaciju cijele industrije i pružiti snažnu potporu izgradnji pametnog društva.[126]

Iste godine Tong Guohua[127] ponudio je neznatno drugačiju izjavu:

> Velika važnost tehnologije 5G za razvoj zemlje [Kina] je u tome da će potkopati primjenu različitih industrija, a zatim pokrenuti rođenje novih standarda i ekosustava u raznim industrijama. Može se reći da je natjecanje za vodeću poziciju u tehnologiji 5G glavni prioritet za gospodarski rast i konkurentnost zemlje.[128]

Chen Baoguo dodao je još jednu razinu slici u dalekovidnom članku iz 2010. godine u kojemu ukazuje kako će se ekosustav standarda i mreža koji će tehnologija 5G osnažiti, protegnuti ne samo u virtualni informacijski svijet, već i u fizički:

> Tehnologija interneta stvari omogućuje kontrolu stvarnog svijeta putem mreže … U prošlosti je ideja bila razdvojiti fizičku infrastrukturu od infrastrukture informacijske tehnologije: zračne luke, autoceste i zgrade s jedne strane, a s druge strane podatkovni centri, osobna računala, širokopojasni internet itd. U doba interneta stvari, armirani beton, kablovi, čipovi i širokopojasni internet bit će integrirani u jedinstvenu infrastrukturu. U tom smislu, mreža i stvarnost postaju integralna cijelina.[129]

Samim time, svijet koji se može definirati postavljanjem standarda 5G tehnologije pokriva stvarni i virtualni svijet i ima vlast ne samo nad kretanjem informacija, već i nad fizičkim prostorom.

Sve te točke, uloga države u postavljanju normi za tehnologiju 5G, njihov stav „pobjednik uzima sve"; njihova uloga u pokretanju većih ekosustava koji će definirati razdoblje informacija te kontrola koju ti ekosustavi nude nad virtualnim i fizičkim svjetovima, zajedno tvore kineski diskurs koji tvori standard tehnologije 5G kao kompetitivne i strateški determinirane domene. „Kina i dalje dominira globalnim standardom mobilnih komunikacija", govori Tong Guohua u intervjuu iz 2017. godine, u kojem također kaže: „Pretjecanje u razdoblju tehnologije 5G pruža rijetku povijesnu priliku."[130]

Kina također ima priliku slomiti vlast SAD-a i Zapada nad međunarodnim standardima te tako potkopati utjecaj SAD-a i Zapada. Kontrola nad globalnim standardima, a naročito nad standardima informacijske tehnologije, dosljedno se opisuje kao osnova globalne snage SAD-a i Zapada. Jang Zhen, tadašnji predsjednik Vijeća Jiangsu instituta za komunikacije, rekao je 2010. godine:

> Sjedinjene Američke Države postavljaju standarde i temeljne tehnologije interneta. Internet je samo virtualni svijet, a internet stvari ogroman je sustav koji povezuje sve stvari na svijetu … Ako su ključne tehnologije i glavni standardi interneta stvari u rukama razvijenih zemalja Zapada, a [Kina] nema neovisna prava intelektualnog vlasništva, onda Kina neće imati priliku postići svoj miran rast i pomlađivanje na nacionalnoj razini.[131]

Zaključak

Nova digitalna arhitektura stvara se. Ova arhitektura oblikovat će protok komunikacija i resursa, sigurnost i prosperitet, globalne norme i informacije. Informirat će međunarodnu ravnotežu snaga i načine na koje se snaga može upotrebljavati unutar te ravnoteže.

Peking se postavlja u položaj u kojemu može igrati ključnu ulogu, a čak i voditi razvoj ove arhitekture. Kineska vlada to čini dok istovremeno u porukama za vanjsku javnost govori o pretpostavkama i ciljevima koji su u suprotnosti s onima koje interno komuniciraju. Da Kina govori s dva glasa nije nikakav novi zaključak. Međutim, osnovne razlike između ta dva glasa u IT-u i dalje su uglavnom nedokumentirane, unatoč sve većem utjecaju Kine na područjima međunarodne IT infrastrukture, tehnologije i normi.

O autorima

Rush Doshi bio je direktor Brookingsove inicijative za kinesku strategiju i član vanjske politike instituta Brookings. Bio je kolega u kineskom centru Paul Tsai na Yaleu i dio inauguracijskog razreda Wilson China Fellows. Njegova istraživanja usredotočena su na veliku kinesku strategiju, kao i na pitanja sigurnosti Indo-Pacifika. Doshi je autor knjige *The Long Game: China's Grand Strategy to Displace American Order* (Duga igra: velika strategija Kine za svrgavanje američkog uređenja), izdavača Oxford University Press. Trenutno služi u Bidenovoj administraciji.

Emily de La Bruyère suosnivačica je tvrtke Horizon Advisory, geopolitičkog konzultantskog savjetovanja, kao i viši član Zaklade za obranu demokracija (Foundation for Defense of Democracies, FDD). Njezin se rad usredotočuje na standardizacijske ambicije Kine, strategiju vojno-civilne fuzije i geopolitičke platforme, kao i na njihove implikacije na globalnu sigurnost i ekonomski red. Ima prvostupnu diploma *summa cum laude* sa sveučilišta Princeton i magisterij *summa cum laude* sa sveučilišta Sciences Po u Parizu, gdje je bila kolegica Michela David-Weilla.

Nathan Picarsic suosnivač je tvrtke Horizon Advisory, geopolitičkog konzultantskog savjetovanja, i viši član Zaklade za obranu demokracija (Foundation for Defense of Democracies, FDD). Njegovo istraživanje usredotočuje se na razvoj konkurentnih strategija koje reagiraju na asimetričnu usmjerenost Kineske komunističke stranke na globalna gospodarska i sigurnosna natjecanja. Ima prvostupnu diplomu sa sveučilišta Harvard i završio je programe poslovne izobrazbu na sveučilištu Harvard Business School i sveučilištu Defense Acquisition University (Sveučilište za obrambenu akviziciju).

John Ferguson bivši je stažist u tvrtki Brookings s centrom za studiju politike Istočne Azije i inicijativom za kinesku strategiju. Diplomirat će na Harvardu u svibnju 2022. godine i time steći prvostupnu diplomu u vladi i drugostupnu diplomu u regionalnoj studiji Istočne Azije, istovremeno u četiri godine. Prethodno je bio istraživački stažist za direktora Centra Carnegie-Tsinghua za globalnu politiku i predvodio je inicijativu za preddiplomsku vanjsku politiku na Harvardu.

Priznanja

Autori se žele zahvaliti bivšim stažistima Isabelli Lu, Gaoqi Zhang i Zijin Zhou za njihovu istraživačku pomoć na ovom projektu, Anni Newby i Tedu Reintu za uređivanje ovog rada i Chrisu Krupinskom za uređenje. Brookings je zahvalan Ministarstvu vanjskih poslova SAD-a i Institutu za izvješćivanje o ratu i miru za financiranje ovog istraživanja.

Ovo je izvješće dovršeno prije državne službe Rusha Doshija, uključuje samo otvorene izvore i ne predstavlja nužno službenu politiku ili položaj bilo koje agencije vlade SAD-a.

Brookings Institution neprofitna je organizacija posvećena neovisnim istraživanjima i političkim rješenjima. Njezina je misija provođenje kvalitetnih, neovisnih istraživanja i, na temelju tih istraživanja, pružanje inovativnih, praktičnih preporuka za kreatore politika i javnost. Zaključci i preporuke bilo koje objave institucije Brookings isključivo su zaključci i preporuke autora i ne odražavaju stajališta institucije, njezinog rukovodstva ili njezinih drugih akademika.

Reference

[1] Istraživački tim ovoga rada primio je kopije poruka e-pošte između savjetodavne službe publikacije i pisaca za koje su se nadali da će pisati sadržaj u ime tvrtke Huawei.
[2] Pojam „cyber" (网络) u „velika cyber sila" može se prevesti kao „mreža". Ovo izvješće temelji se na prijevodu„ velika cyber sila", ali prepoznaje da ima mjesta za neslaganje. U stvari, barem jedan od autora preferira prijevod „velika mrežna sila" zbog stupova razvoja koji su najčešće povezani s težnjom za ambicijom koncepta. (Pogledajte: Emily de La Bruyère, „The Network Great Power Strategy: A Blueprint for China's Digital Ambitions" („Strategija velike mrežne moći: plan digitalnih ambicija Kine"), Nacionalni ured za azijska istraživanja, izlazi 2021.)
[3] 习近平 [Xi Jinping], „习近平在网信工作座谈会上的讲话全文发表" [Puni tekst govora Xi Jinping na Forumu o kibernetičkoj sigurnosti i informatizacijskom radu], (govor, Peking, 25. travnja 2016.), http://www.xinhuanet.com//politics/2016-04/25/c_1118731175.htm.
[4] 习近平 [Xi Jinping], "习近平：把我国从网络大国建设成为网络强国-高层动态-新华网" [Xi Jinping: Izgradimo Kinu iz veće cyber države u veliku cyber silu], Xinhua, 27. veljače 2014., http://www.xinhuanet.com//politics/2014-02/27/c_119538788.htm.
[5] 习近平 [Xi Jinping], „习近平在网信工作座谈会上的讲话全文发表" [Puni tekst govora Xija Jinpinga na Forumu o kibernetičkoj sigurnosti i informatizacijskom radu].
[6] Hua Chunying, „Glasnogovornica Ministarstva vanjskih poslova Hua Chunying na redovnoj tiskovnoj konferenciji 15. srpnja 2020." (govor, Peking, 15. srpnja 2020.), https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/t1797967.shtml; Hua Chunying, „Glasnogovornica Ministarstva vanjskih poslova Hua Chunying na redovnoj tiskovnoj konferenciji 11. prosinca 2020." (govor, Peking, 11. prosinca 2020.), https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/2511_665403/t1839583.shtml.
[7] "中央网络安全和信息化领导小组第一次会议召开" [Održan je prvi sastanak vodeće skupine za sigurnost i informatizaciju središnje mreže], 中央政府门户网站 [Central Government Portal], 27. veljače 2014., http://www.gov.cn/ldhd/2014-02/27/content_2625036.htm.
[8] „习近平称努力让关键核心技术自主可控 促产业迈向全球价值链中高端" [Xi Jinping izjavio je kako se prave napori da se ključne temeljne tehnologije učine neovisnima i takvima da se njima može upravljati, za promicanje industrije u visoki globalni lanac vrijednosti], Reuters, 28. svibnja 2018.https://cn.reuters.com/article/china-xi-jinping-tech-value-chain-0528-idCNKCS1IT0XT.; 陈肇雄 [Chen Zhaoksiong], „推进工业和信息化高质量发展" [Promicanje razvoja industrije i informatizacije visoke kvalitete], 网信军民融合 [Vojno-civilna fuzija na kibernetičkom području], 9. srpnja 2019., CNKI: F424;F49.
[9] „习近平称努力让关键核心技术自主可控 促产业迈向全球价值链中高端" [Xi Jinping izjavio je kako se prave napori da se ključne temeljne tehnologije učine neovisnima i takvima da se njima može upravljati, za promicanje industrije u visoki globalni lanac vrijednosti], Reuters.
[10] 习近平 [Xi Jinping], "习近平：自主创新推进网络强国建设" [Xi Jinping: Neovisna inovacija promovira izgradnju mrežne sile], *新华* [Xinhua], 21. travnja 2018., http://www.xinhuanet.com/politics/2018-04/21/c_1122719810.htm.
[11] 秦安 [Qin An], "网络强国的意识认识共识" [Svijest, razumijevanje i konsenzus mrežne moći], *中国信息技术安全评估中心 [Kineska informacijska sigurnost],* 9 (2016.), CNKI: TP393.08.
[12] 习近平 [Xi Jinping], „习近平在网信工作座谈会上的讲话全文发表" [Puni tekst govora Xija Jinpinga na Forumu o kibernetičkoj sigurnosti i informatizacijskom radu].
[13] 郭占恒 [Guo Zhanheng], "习近平标准化思想与浙江实践" [Misao Xija Jinpinga o standardizaciji i praksa Zhejiang], *浙江日报 [Zhejiang Daily]*, 25. rujna 2015., CNKI: F203;F092.7. Oba citirana izraza uobičajena su u kineskim korporacijskim i političkim raspravama o standardima.

[14] 陈肇雄 [Chen Zhaoxong], „加快推进新时代网络强国建设" [Ubrzavanje izgradnje mrežne snage u novom dobu], *People's Daily*, 17. studenog 2017., http://opinion.people.com.cn/n1/2017/1117/c1003-29651140.html.
[15] Pogledajte 2. završnu bilješku.
[16] Središnja vodeća mala grupa za kibernetičku sigurnost i informatizaciju naziva se 中央网络安全和信息化领导小组, a zatim se u ožujku 2018. pretvara u komisiju: 中央网络安全和信息化委员会.
[17] "中央网络安全和信息化领导小组第一次会议召开" [Održan je prvi sastanak vodeće skupine za sigurnost i informatizaciju središnje mreže], 中央政府门户网站 [Central Government Portal]."
[18] Usluga Oriprobe upotrebljena je za pretraživanje izraza 网络强国. Xi Jinping i član stalnog odbora Politburo Wang Huning upotrijebiti su taj izraz najmanje dva puta na Svjetskoj internetskoj konferenciji, ali s mnogo manje pojedinosti nego u govorima u kojima se obraćaju domaćoj javnosti, i to ne nedavno.
[19] Popis relevantnih Xijevih govora i citata potražite ovdje: 习近平 [Xi Jinping], „习近平谈加快建设网络强国-中共中央网络安全和信息化委员会办公室" [Xi Jinping govori o ubrzanju izgradnje cyber sile – Ured središnjeg odbora za kibernatičku sigurnost i informacijske tehnologije CPC], 9. rujna 2019., http://www.cac.gov.cn/2019-09/11/c_1569738113999057.htm; pogledajte i
Paul Triolo, Lorand Laskai, Graham Webster i Katarin Tai, „Xi Jinping stavlja „autohtone inovacije" i „temeljne tehnologije" u središte razvojnih prioriteta", New America, 1. svibnja 2018., http://newamerica.org/cybersecurity-initiative/digichina/blog/xi-jinping-puts-indigenous-innovation-and-core-technologies-center-development-priorities/.
[20] 习近平 [Xi Jinping], „习近平在第二届世界互联网大会开幕式上的讲话" [Govor Xija Jinpinga na svečanom otvorenju Druge svjetske internetske konferencije], (govor, Wuzhen, 16. prosinca 2015.), http://www.xinhuanet.com//politics/2015-12/16/c_1117481089.htm.
[21] CAC je regulator interneta za Kinu. Ovaj članak temelji se na analizi izjava Xija Jinpinga.
[22] „深入贯彻习近平总书记网络强国战略思想 扎实推进网络安全和信息化工作" [Dubinska provedba strateškog razmišljanja glavnog tajnika Xija Jinpinga o jačanju zemlje putem interneta i solidan napredak u sigurnosti i informacijama mreže], *求是 [Qiushi],* 15. rujna 2017. http://www.qstheory.cn/dukan/qs/2017-09/15/c_1121647633.htm.
[23] 习近平 [Xi Jinping], „习近平在网信工作座谈会上的讲话全文发表" [Puni tekst govora Xija Jinpinga na Forumu o kibernetičkoj sigurnosti i informatizacijskom radu].
[24] Ibid; iste godine, zamjenik direktora kineske uprave za kiberprostor Zhuang Rongwen ponovio je tu rečenicu: „Propustili smo svoje prilike tijekom industrijske revolucije … ne smijemo zaostajati u novom krugu natjecanja." Pogledajte: Mandy Zuo, „Kina želi postati internetska supersila do 2050. Godine", *South China Morning Post*, 28. srpnja 2016., https://www.scmp.com/news/china/policies-politics/article/1995936/china-aims-become-internet-cyberpower-2020.
[25] 陈肇雄 [Chen Zhaoxong], „推进工业和信息化高质量发展" [Promicanje visokokvalitetnog razvoja industrije i informatizacije].
[26] Ibid.
[27] Ibid.
[28] 陈肇雄 [Chen Zhaoxiong], "加快推进新时代网络强国建设" [Accelerate the Construction of a Network Power in the New Era (Ubrzavanje izgradnje mrežne snage u novom dobu)], *人民网－人民日报 [People's Daily]*, 17. studenog 2017., http://theory.people.com.cn/n1/2017/1117/c40531-29651453.html.
[29] Duan je pisao sa suautorom Hanom Xiaoluom, koji je također povezan s grupom Datang Group.
[30] 段伟伦 [Duan Weilun] i 韩晓露 [Han Xiaolu], „全球数字经济战略博弈下的 5G 供应链安全研究" [Istraživanje o sigurnosti lanca opskrbe tehnologije 5G u kontekstu strateške igre globalne digitalne ekonomije], *信息安全研究 [Istraživanje o informacijskoj sigurnosti]* 6, br. 1 (2020.): 46 – 51, http://www.sicris.cn/CN/abstract/abstract715.shtml.
[31] 许正中 [Xu Zhengzhong], "网络空间治理的任务与挑战" [The Tasks and Challenges of Network Space Governance (Zadaci i izazovi upravljanja mrežnim prostorom], *中国党政干部论坛 [Party & Government Forum]*, br. 1 (2020.): 36 – 37, CNKI: D669. Autor je član stalnog odbora stranačkog odbora provincije Hubei i direktor provincijskog partijskog odbora odjela za propagandu.
[32] 习近平 [Xi Jinping], „习近平在网信工作座谈会上的讲话全文发表" [Puni tekst govora Xija Jinpinga na Forumu o kibernetičkoj sigurnosti i informatizacijskom radu].

[33] Zhao Lijian, „Glasnogovornik Ministarstva vanjskih poslova Zhao Lijian na redovnoj tiskovnoj konferenciji 19. studenog 2020.," (govor, Peking, 19. studenog 2020.), https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/t1833798.shtml.
[34] Hua Chunying, "Glasnogovornica Ministarstva vanjskih poslova Hua Chunying na redovnoj tiskovnoj konferenciji 15. srpnja 2020."
[35] Zhao Lijian, „glasnogovornik Ministarstva vanjskih poslova Zhao Lijian na redovnoj tiskovnoj konferenciji 18. kolovoza 2020." (govor, Peking, 18. kolovoza 2020.), https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/t1807193.shtml.
[36] 习近平 [Xi Jinping], "习近平：把我国从网络大国建设成为网络强国-高层动态-新华网" [Xi Jinping: Build China from a Major Cyber Country to a Cyber Great Power (Izgradimo Kinu iz veće cyber države u veliku cyber silu)].
[37] Ibid.
[38] 习近平 [Xi Jinping], "习近平在网信工作座谈会上的讲话全文发表" [Puni tekst govora Xija Jinpinga na Forumu o kibernetičkoj sigurnosti i informatizacijskom radu].
[39] Ibid.
[40] Ibid.
[41] Ovaj pojam doslovno se prevodi kao „vrata života" ili „vrata vitalnosti", ali budući da se ovdje upotrebljava metaforički na kineskom, odlučili smo se za englesku metaforu koja je razumljivija čitateljima koji govore engleski.
[42] 习近平 [Xi Jinping], „习近平在网信工作座谈会上的讲话全文发表" [Puni tekst govora Xija Jinpinga na Forumu o kibernetičkoj sigurnosti i informatizacijskom radu].
[43] Izraz koji se odnosi na pretjecanje konkurenta s vanjske strane pri zavoju.
[44] 习近平 [Xi Jinping], „习近平在网信工作座谈会上的讲话全文发表" [Puni tekst govora Xija Jinpinga na Forumu o kibernetičkoj sigurnosti i informatizacijskom radu].
[45] Ibid.
[46] 习近平 [Xi Jinping], "习近平在第二届世界互联网大会开幕式上的讲话" [Govor Xija Jinpinga na svečanom otvorenju Druge svjetske internetske konferencije].
[47] Xi je rekao: „Jedan pogled je da moramo zatvoriti vrata, započeti iznova, potpuno se riješiti ovisnosti o vanjskoj tehnologiji i osloniti se na autohtone inovacije kako bi postigli razvoj jer ćemo inače uvijek pratiti druge i nikada ih nećemo sustići."
[48] Xi je rekao da je potrebno „otvoriti se i inovirati i razvijati vlastitu tehnologiju na ramenima [stranih] divova."
[49] 习近平 [Xi Jinping], „习近平在网信工作座谈会上的讲话全文发表" [Puni tekst govora Xija Jinpinga na Forumu o kibernetičkoj sigurnosti i informatizacijskom radu].
[50] Ibid.
[51] Ibid.
[52] Ibid.
[53] Ibid.
[54] 陈肇雄 [Chen Zhaoxong], „推进工业和信息化高质量发展" [Promicanje visokokvalitetnog razvoja industrije i informatizacije].
[55] 墨翡 [Mo Fei], "英国高调发布 5G 战略 意欲成为全球领导者" [UK pokreće strategiju visokog profila za tehnologije 5G, namjerava postati globalni predvodnik], *通信世界 [Communications World]*, br. 21 (2017.), CNKI: F627.
[56] 乔龙 [Qiao Long] 任天舒 [Ren Tianshu] i 刘优 [Liu you], „中国高新技术产业应对贸易摩擦的影响研究 – 以 5G 产业为例" [Istraživanje o utjecaju kineskih visokotehnoloških industrija kao odgovor na trgovinske tenzije – uzimanje industrije tehnologije 5G kao primjer], *国际经贸 [International Economics and Trade]*, 5 (2020.) CNKI: F276.44;F752.02.
[57] „中央网络安全和信息化领导小组第一次会议召开" [Održan je prvi sastanak vodeće skupine za sigurnost i informatizaciju središnje mreže], 中央政府门户网站 [Central Government Portal]."
[58] „习近平称努力让关键核心技术自主可控促产业迈向全球价值链中高端" [Xi Jinping izjavio je kako se prave napori da se ključne temeljne tehnologije učine neovisnima i takvima da se njima može upravljati, za promicanje industrije u visoki globalni lanac vrijednosti].
[59] Hua Chunying, "Glasnogovornica Ministarstva vanjskih poslova Hua Chunying na redovnoj tiskovnoj konferenciji 15. srpnja 2020."
[60] Hua Chunying, "Glasnogovornica Ministarstva vanjskih poslova Hua Chunying na redovnoj tiskovnoj konferenciji 11. prosinca 2020."

[61] Hua Chunying, „Glasnogovornica Ministarstva vanjskih poslova Hua Chunying na redovnoj tiskovnoj konferenciji 9. listopada 2020." (govor, Peking, 9. listopada 2020.), https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/t1822871.shtml.

[62] Kineski pojam „cyber" (网络) u „kibernetičkoj (cyber) sigurnosti" može se prevesti kao „mreža". Za potrebe ovog izvješća, navedena upotreba pojma bit će prevedena kao „kibernetička sigurnost", a ne „mrežna sigurnost". U općoj će se raspravi upotrebljavati izraz „kibernetička i mrežna sigurnost".

[63] "中央网络安全和信息化领导小组第一次会议召开" [Održan je prvi sastanak vodeće skupine za sigurnost i informatizaciju središnje mreže], 中央政府门户网站 [Central Government Portal]." Također je imenovao glavnu grupu pokrenutu na tom događanju kao „Središnju vodeću mala grupa za kibernetičku sigurnost i informatizaciju" i definirao je u smislu sigurnosti.

[64] Ibid.

[65] Na primjer, Xijova reiteracija iz 2018. godine da "bez mrežne sigurnosti nema nacionalne sigurnosti." Pogledajte: 习近平 [Xi Jinping], "习近平：自主创新推进网络强国建设" [Xi Jinping: Neovisna inovacija promovira izgradnju mrežne sile]."

[66] 刘楝 [Liu li], 孟宪民 [Meng Xianmin] i 李阳 [li Yang], „5G 安全及网络监管问题探析" [Analiza pitanja sigurnosti tehnologije 5G i nadzora mreže], *国防科技 [National Defense Technology]* 41, br. 3 (2020.): 76 – 79, CNKI: TN929.5;TN915.08.

[67] 习近平 [Xi Jinping], „习近平在网信工作座谈会上的讲话全文发表" [Puni tekst govora Xija Jinpinga na Forumu o kibernetičkoj sigurnosti i informatizacijskom radu].

[68] 习近平 [Xi Jinping], „习近平：加快推进网络信息技术自主创新 朝着建设网络强国目标不懈努力" [Xi Jinping: Ubrzati neovisnu inovaciju mrežne informacijske tehnologije i uložiti ustrajne napore u cilj izgradnje mrežne sile], (govor, Peking, 10. listopada 2016.), http://cpc.people.com.cn/n1/2016/1010/c64094-28763907.html.

[69] 陈肇雄 [Chen Zhaoxong], „推进工业和信息化高质量发展" [Promicanje visokokvalitetnog razvoja industrije i informatizacije].

[70] 轩传树 [Xuan Chuanshu], "正确认识网络强国建设所面对的成就_问题和影响" [Ispravno razumijevanje postignuća izgradnje mrežne sile: Problemi i učinak], *中国信息安全 [Kineska informacijska sigurnost]*, 2 (veljača 2015.), CNKI: TP393.08;E86.

[71] Takav agresivan i ofenzivan jezik neće se vjerojatno pojaviti u javnoj retorici Xija Jinpinga, niti u javnoj retorici drugih vladinih subjekata koji usmjeravaju svoje izjave vanjskoj javnosti te su podložni međunarodnom nadzoru. Stoga se ovaj odjeljak prvenstveno oslanja na manje službene izvore. Naravno, ovo dolazi s upozorenjem u vezi autoritativnosti: ovi se ne bi trebali smatrati službenim mandatima ili strategijama koje je izdala kineska vlada, nego razmatranjima prevladavajućih mišljenja u kineskim analitičkim krugovima.

[72] Za dubinsku raspravu o kineskoj strategiji vojno-civilne fuzije pogledajte: Emily de La Bruyère i Nathan Picarsic, „Military-Civil Fusion: China's Approach to R&D, Implications for Peacetime Competition, and Crafting a US Strategy" (Vojno-civilna fuzija: kineski pristup istraživanju i razvoju, implikacije za mirnodopsku konkurenciju i izrada američke strategije), Simpozij za istraživanje akvizicije USN/NPS, svibanj 2019., https://nps.edu/web/gsdm/acquisition-research-program.

[73] „《2015 年中国军民融合发展报告》呈现五大亮点 " [Pet istaknutih dijelova Izvješća o razvoju vojno-civilne fuzije iz 2015. godine], 中国日报 [China Daily],, 24. rujna 2015., https://cn.chinadaily.com.cn/2015-09/24/content_21968926.htm.

[74] 习近平 [Xi Jinping], "习近平：自主创新推进网络强国建设" [Xi Jinping: Neovisna inovacija promovira izgradnju mrežne sile].

[75] 秦安 [Qin An], "网络强国的意识认识共识" [Svijest, razumijevanje i konsenzus mrežne moći].

[76] 段伟伦 [Duan Weilun] i 韩晓露 [Han Xiaolu], „全球数字经济战略博弈下的 5G 供应链安全研究" [Istraživanje o sigurnosti lanca opskrbe tehnologije 5G u kontekstu strateške igre globalne digitalne ekonomije], CNKI: F623;TN929.5.

[77] 郭超 [Guo Chao], 于川信 [Yu Chuanxin] i 王景芳 [Wang Jingfang], „对第五代移动通信技术军事应用的几点认识" [Neka poimanja o vojnoj primjeni tehnologije mobilne komunikacije pete generacije], *国防 [National Defense]*, br. 1 (2019.): 27 – 29, CNKI: E962;TN929.5.

[78] Pogledajte, na primjer, govor Xija na 22. studijskoj sjednici Kineske komunističke stranke Politburo u srpnju 2020., u kojem poziva na ubrzanje „informatizacije i inteligencije" za jačanje kineske vojske: „习近平在中央政治局第二十二次集体学习时强调 统一思想坚定信心鼓足干劲抓紧工作 奋力推进国防和军队现代化建设" [Tijekom 22. kolektivnog studijskog zasjedanja političkog ureda središnjeg odbora, Xi Jinping naglasio je ujedinjenje razmišljanja, čvrstog povjerenja i entuzijazma te napornog rada na promicanju modernizacije nacionalne obrane i vojske], *新华* [Xinhua], 31. srpnja 2020., http://www.xinhuanet.com/politics/leaders/2020-07/31/c_1126310486.htm.

[79] 郑安琪 [Zheng Anqi], „立足现实基础推动我国网络强国建设" [Promicanje izgradnje mreže u mojoj zemlji na temelju stvarnosti], *通信管理与技术 [Communication Management and Technology (Upravljanje komunikacijom i tehnologijom]* 3 (2020.), CNKI: F49.

[80] Ibid.

[81] Ibid.

[82] 李峰 [Li Feng], 马方方 [Ma Fangfang], 刘海 [Li Hai] i 李凯 [Li Kai], "浅析 5G 技术在现代军事物流中的应用" [Analiza primjene tehnologije 5G u modernoj vojnoj logistici], *物流技术 [Logistics Technology (Logistička tehnologija]* 39, br. 4 (2020.): 133 – 37, CNKI: TN929.5;E075.

[83] 郭超 [Guo Chao], 于川信 [Yu Chuanxin], and 王景芳 [Wang Jingfang], "对第五代移动通信技术军事应用的几点认识" [Neka poimanja o vojnoj primjeni tehnologije mobilne komunikacije pete generacije].

[84] Ibid.

[85] Ibid.

[86] Ibid.

[87] Ibid.

[88] Ibid.

[89] 王峰 [Wang Feng], "军民融合热度渐升 A 股酝酿主题行情" [Entuzijazam za vojno-civilnu fuziju raste, A-dionice stvaraju tematsko tržište], *商业观察 [Business Observation]* 8 (2019.): 42-47, CNKI:F426.48;E25;F832.51.

[90] Ibid.

[91] 李峰 [Li Feng], 马方方 [Ma Fangfang], 刘海 [Li Hai] i 李凯 [Li Kai], "浅析 5G 技术在现代军事物流中的应用" [Analiza primjene tehnologije 5G u modernoj vojnoj logistici].

[92] 孙柏林 [Sun Bolin], "5G 赋能现代军事" [Tehnologija 5G osnažuje modernu vojsku], *计算机仿真 [Computer Simulation]* 37, br. 1 (2020.): 1 – 6, CNKI: TN929.5;E11.

[93] 陈宝国 [Chen Baoguo], "新一轮信息技术革命浪潮对我国的影响" [Utjecaj nove revolucije informacijske tehnologije na našu zemlju], *科学决策 [Scientific Decision Making]* 11 (2010.): 1 – 25, CNKI: F49.

[94] Ibid.

[95] Ibid.

[96] 刘红凛 [Liu Honglin], "信息化发展对党的建设的多重影响" [Višestruki utjecaji razvoja informacija na izgradnju stranke], *中共中央党校学报 [Journal of the Party School of the Central Committee of the C.P.C.]* (prosinac 2011.), CNKI: TP399-C2.

[97] 易华勇 [Yi Huayong] and 邓伯军 [Deng Bojun], "新时代中国国家文化安全策论" [Kineska politika nacionalne kulturne sigurnosti u novom razdoblju], *江海学刊 [Jianghai Academic Journal]* (2020.), CNKI: TP18;TN929.5;G120.

[98] Zhao Lijian, „glasnogovornik Ministarstva vanjskih poslova Zhao Lijian na redovnoj tiskovnoj konferenciji 19. listopada 2020." (govor, Peking, 19. listopada 2020.), https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/t1807193.shtml.

[99] 龙在野 [Long Zaiye], "网络强国和信息治国的网信军民融合路径探悉" [Istraživanje Puta kibernatičko-informacijske vojno-civilne fuzije za mrežnu snagu i upravljanje informacijama], *网信军民融合 [Military-Civil Fusion in Cyberspace]* (listopad 2017.), CNKI: E25.

[100] 习近平 [Xi Jinping], „习近平在网信工作座谈会上的讲话全文发表" [Puni tekst govora Xija Jinpinga na Forumu o kibernetičkoj sigurnosti i informatizacijskom radu].

[101] Zhao Lijian, „Glasnogovornik Ministarstva vanjskih poslova Zhao Lijian na redovnoj tiskovnoj konferenciji 8. rujna 2020." (govor, Peking, 8. rujna 2020.), https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/t1813183.shtml.

[102] "'网络空间战略论坛'三载路：网络强国理论高地行" [Trogodišnji plan „Foruma za strategiju na kibernetičkom prostoru": Cyber Great Power Theory Highland Tour].

[103] 郭占恒 [Guo Zhanheng], "习近平标准化思想与浙江实践" [Misao Xija Jinpinga o standardizaciji i praksa Zhejiang], *浙江日报 [Zhejiang Daily]*, 25. rujna 2015., CNKI: F203;F092.7. Oba citirana izraza uobičajena su u kineskim korporacijskim i političkim raspravama o standardima.
[104] "'标准化'作用何在？习近平为你一一讲来" [Koja je uloga „standardizacije"? Xi Jinping vam govori], *中国日报 [China Daily]*, 13 rujna 2016., https://china.chinadaily.com.cn/2016-09/13/content_26783549.htm. To nije bio novi fokus za Xija: još od 2006. godine, kada je bio tajnik stranačkog odbora provincije Zhejiang, Xi je predložio „aktivno provođenje strategije prava intelektualnog vlasništva i standardizacije" te je nazvao „standardizaciju" „vodećim strateškim položajem" za gospodarski i socijalni razvoj. Pogledajte: 郭占恒 [Guo Zhanheng], "习近平标准化思想与浙江实践" [Misao Xija Jinpinga o standardizaciji i praksa Zhejiang].
[105] Za dodatnu raspravu o kineskim ambicijama standardizacije, pogledajte Emily de La Bruyère i Nathan Picarsic, „China Standards 2035: Beijing's Platform Geopolitics and Standardization Work in 2020," Horizon Advisory, travanj 2020., https://www.horizonadvisory.org/china-standards-2035-introduction; Emily de La Bruyère, „Platform Geopolitics: The New Metrics for Building Geopolitical Power in a New World," *The National Interest*, 12. travnja 2020., https://nationalinterest.org/feature/new-metrics-building-geopolitical-power-new-world-143147.
[106] 习近平 [Xi Jinping], „中共中央政治局就实施网络强国战略进行第三十六次集体学习" [Politički ured središnjeg odbora CPC-a provodi 36. skupnu studiju o provedbi strategije mrežne snage], 新华 [Xinhua], 9. listopada 2016., http://www.gov.cn/xinwen/2016-10/09/content_5116444.htm.
[107] 金英果 [Jin Yingguo], "'中国标准 2035'项目" [China Standards 2035 Project], *中国标准话 [China Standardization]* 1 (2019.): 38 – 43, CNKI: F203.
[108] "'中国标准 2035'项目结题会暨'国家标准化发展战略研究'项目启动会在京召开" [Sastanak zatvaranja projekta „China Standard 2035" i sastanak početka projekta „National Standardization Development Strategy Research" održani u Pekingu], *铁道技术监督 [Railway Technical Supervision]* 2 (2020.): 16, CNKI: F203.
[109] „2020 年全国标准化工作要点" [Glavne točke rada nacionalne standardizacije u 2020. godini], 国家标准化管理委员会 [Administracija nacionalne standardizacije].
[110] 孙强 [Sun Qiang], "乌镇讲话彰显习近平网络强国战略的思想内核" [Govor u Wuzhenu ističe ideološki temelj strategije mrežne snage Xija Jinpinga], *人民日报 [People's Daily]*, siječanj 2016., CNKI: TP393.4.
[111] Ovaj račun ne razlikuje se od tvrdnje Xija Jinpinga, navedene ranije u ovom izvješću, da su temeljne tehnologije područje gdje je Kina „na istoj početnoj liniji kao i strane zemlje. Ako se možemo unaprijed pripremiti i fokusirati na istraživanje, vrlo je moguće ostvariti transformaciju od trčanja za drugima do trčanja ispred drugih i vođenja." Pogledajte: 习近平 [Xi Jinping], "习近平在网信工作座谈会上的讲话全文发表" [Puni tekst govora Xija Jinpinga na Forumu o kibernetičkoj sigurnosti i informatizacijskom radu].
[112] „2020 年全国标准化工作要点" [Glavne točke rada nacionalne standardizacije u 2020. godini], 国家标准化管理委员会 [Administracija nacionalne standardizacije].
[113] 习近平 [Xi Jinping], „习近平：加快推进网络信息技术自主创新 朝着建设网络强国目标不懈努力" [Xi Jinping: Ubrzati neovisnu inovaciju mrežne informacijske tehnologije i uložiti ustrajne napore u cilj izgradnje mrežne sile [People's Daily].
[114] 高超 [Gao Chao], "加快 5G 进程助力网络强国建设" [Ubrzanje procesa tehnologije 5G za pomoć u izgradnji mrežne snage], *通信产业报 [Communication Industry News]*, 12. ožujka 2018., http://www.qikan.com/article/txcy20180928.html.
[115] 童国华 [Tong Guohua], "立足自主 重点布局 探索网络空间内生安全" [Na temelju autonomije, fokusa na uređenje, istraživanje endogene sigurnosti u kibernetičkom prostoru], *保密科学技术 [Confidential Science and Technology]* 11 (2018.): 33, CNKI: TP393.08.
[116] 段伟伦 [Duan Weilun] i 韩晓露 [Han Xiaolu], „全球数字经济战略博弈下的 5G 供应链安全研究" [Istraživanje o sigurnosti lanca opskrbe tehnologije 5G u kontekstu strateške igre globalne digitalne ekonomije]. Duan piše sa suautorom Hanom Xiaoluom, koji je također povezan s grupom Datang Group.
[117] Ibid.
[118] Ibid.
[119] Ibid.
[120] Članak su napisali potporučnik na postdiplomskom studiju Akademije vojnih znanosti, profesor na Akademiji vojnih znanosti i pukovnik iz 93605. jedince. Pogledajte: 郭超 [Guo Chao], 于川信 [Yu Chuanxin], and 王景芳 [Wang Jingfang], "对第五代移动通信技术军事应用的几点认识" [Neka poimanja o vojnoj primjeni tehnologije mobilne komunikacije pete generacije].
[121] Ibid.

[122] 胡蓉 [Hu Rong], “发展 5G，深圳使命在肩” [Razvoj tehnologije 5G, misija Shenzhen na ramenima je te tehnologije], *深圳商报 [Shenzhen Commercial Daily]*, 29. travnja 2019., http://www.sznews.com/news/content/mb/2019-04/29/content_21705204.htm.
[123] 苏德悦 [Su Deyue], “苗圩在国务院新闻发布会上表示稳步推进 5G 网络建设 深化 5G 应用发展” [Miao Wei pozvao je na državnoj konferenciji Vijeća za medije na stalno promicanje izgradnje 5G mreža i produbljivanje razvoja tehnologija umjetne inteligencije za 5G aplikacije], 人民邮电报 [People’s Post and Telegraph], 21. siječnja 2020., http://www.cnii.com.cn/sy/tt/202001/t20200121_150863.html.
[124] 童国华 [Tong Guohua], “立足自主 重点布局 探索网络空间内生安全” [Na temelju autonomije, fokusa na uređenje, istraživanje endogene sigurnosti u kibernetičkom prostoru].
[125] 许正中 [Xu Zhengzhong], “网络空间治理的任务与挑战” [Zadaci i izazovi upravljanja mrežnim prostorom].
[126] 高超 [Gao Chao], “加快 5G 进程助力网络强国建设” [Ubrzanje procesa tehnologije 5G za pomoć u izgradnji mrežne snage].
[127] Tong, koji je također prethodno citiran, predsjednik je i tajnik stranačkog odbora kineske Grupe za informacijsku i komunikacijsku tehnologiju.
[128] 童国华 [Tong Guohua], “立足自主 重点布局 探索网络空间内生安全” [Na temelju autonomije, fokusa na uređenje, istraživanje endogene sigurnosti u kibernetičkom prostoru].
[129] 陈宝国 [Chen Baoguo], “新一轮信息技术革命浪潮对我国的影响” [Utjecaj nove revolucije informacijske tehnologije na našu zemlju.].
[130] 童国华 [Tong Guo], “大唐电信集团董事长兼总裁童国华：不忘初心 牢记使命，做引领 5G 发展的国家队” [Tong Guohua, predsjednik i direktor grupe Datang Telecom Group: Ne zaboravite svoju prvobitnu aspiraciju, imajte svoju misiju na umu i budite nacionalni tim koji vodi razvoj tehnologije 5G], *中国电子报 [China Electronic News]*, 21. studeni 2017., http://www.cena.com.cn/infocom/20171121/90412.html.
[131] 杨震 [Yang Zhen], „物联网：引领新一轮信息技术革命” [Internet stvari: Vođenje nove runde revolucije informacijske tehnologije], *江苏通信 [Jiangsu Communications]* 3 (2010.): 12113, CNKI: F49;F426.6.