Informationskampen och Ukraina — memo 2

Rysslands inte så suveräna internet och kriget i Ukraina

Carolina Vendil Pallin

Kriget i Ukraina är på många sätt ett chockerande gammaldags krig. En brutal invasion av ett slag som många trodde inte kunde ske i dagens Europa. Men samtidigt är det ett krig som åtminstone delvis utspelar sig i en slående modern miljö: den digitaliserade informationsmiljön. I en serie memon kommer FOI berätta om, beskriva och analysera hur det här utspelar sig – den kamp som pågår kring och med information, på såväl som bortom det fysiska slagfältet. Krig och kommunikation har alltid hängt nära samman, men med kriget i Ukraina är den kopplingen starkare än någonsin.

"Enligt Roskomnadzor har alla hittills genomförda övningar varit framgångsrika. Övningarna är ämnade att utesluta [avbrott inom det ryska segmentet av internet] och övningarna demonstrerar att vi är redo, att allt fungerar robust och säkert vid all form av påverkan utifrån."

Chefen för den ryska myndigheten för övervakning av kommunikation, Roskomnadzor, Andrej Lipov, utvärderar sommarens cyberövning i oktober 2021.[1]

Ryssland tycks bara några månader innan den 24 februari 2022 ha varit övertygat om att landets internet, ”ett ryskt segment av det globala internet”, var säkert och kunde stå emot cyberattacker liksom försök att påverka dess funktionalitet. Lagändringar, installation av utrustning samt övningar i Ryssland under de senaste åren har haft som mål att skapa ett ryskt ”suveränt internet”. Hur väl fungerade då de åtgärder som Ryssland har vidtagit? Och hur kommer kriget att påverka utvecklingen av internet i Ryssland och dess uppkoppling mot omvärlden?

I början av 2019 antog Ryssland en rad lagändringar, ett lagpaket som i rysk press gick under rubriken ”lagen om ett suveränt internet”. I både bild och ord var det lätt att få intrycket att Ryssland skulle kapa alla kablar som kopplade upp landets internet mot väst. I själva verket ville landets politiska ledning åstadkomma något mer komplicerat: dels ville Ryssland säkerställa att internet fungerar för ryska användare i möjligaste mån oberoende av omvärlden; dels ville man öka möjligheterna att övervaka och begränsa vilken information landets medborgare kunde ta del av. Lagen (nr. 90-FZ) trädde i kraft den 1 november 2019 och innebar i korthet att:[2]

- Vid ”hot” ska Roskomnadzor kunna styra trafiken inom det man definierar som ”ett ryskt segment av internet”, vilka vägar trafiken går och vilka noder den ska passera. Ett uttalat mål var att begränsa andelen trafik som ”studsar” på servrar utanför ryskt territorium, men också att öka kontrollen (se nedan).

- Lagen definierar vad som är ”gränsövergångar” för ett ryskt internet och vad som är ”internetknutpunkter” (trafikutväxlingspunkter). Ägarna till dessa gränsövergångar och knutpunkter liksom även internetoperatörer är ålagda att säkerställa att Roskomnadzor kan ta över och styra trafiken centralt om ett hot uppstår.

- Operatörer ska installera teknisk utrustning som går under akronymen TSPU,[3] som kan identifiera avsändaren av specifik trafik på internet och blockera

1 Roskomnadzor, förkortning för den ryska myndigheten: Federala tjänsten för övervakning och tillsyn inom kommunikation, informationsteknologi och massmedier. Lipovs uttalande återgavs i *Kommersant,* 19 oktober 2021: https://www.kommersant.ru/doc/5040099 [2022-08-16].

2 Federal lag nr. 90-FZ, 1 maj 2020: https://rg.ru/2019/05/07/fz90-dok.html [2022-08-24]. Lagen bestod av en rad ändringar till två existerande lagar, dels ”Om kommunikation” (nr. 126-FZ), dels ”Om information, informationsteknologier och om skyddet av information” (nr. 149-FZ). Se även Vendil Pallin, Carolina (2019), ”Ryssland nationaliserar internet – lagförslaget om ett ’suveränt internet’”, FOI Memo 6016, 27 februari.

3 TSPU – *technitjeskije sredstva protivodejstvija ugrozami,* tekniska medel för att motverka hot. Det finns föga uppgifter om exakt vad denna tekniska utrustning kan göra, men den innehåller bland annat möjligheten att genomföra så kallad *deep packet inspection* (DPI), vilket innebär ökade möjligheter för staten att filtrera informationen på internet, att packa upp trafikpaketen och blockera dessa om de innehåller information som är olaglig i Ryssland. Se t.ex. Anastasija Gavriljuk, (2022), ”Blok kreptjajet” [Stärkt blockering], *Kommersant,* 29 mars: https://www.kommersant.ru/doc/5281701 [2022-08-15].

FOI Memo: 7925
Projektnummer: I1498503
Godkänd av: Jessica Appelgren

September 2022

information som är förbjuden i Ryssland. Samma utrustning ska också göra det möjligt för Roskomnadzor att centralt styra trafiken på det ryska segmentet av internet.

- Det ryska segmentet av internet ska fungera även om ryska telekomoperatörer inte kan koppla upp sig mot den globala infrastrukturen. Därför skulle senast till sommaren 2022 ett ”nationellt domännamnsystem”, en reservstruktur för domännamnen .ru, .рф och .su. finnas på plats.[4]

- Ryssland ska minst en gång per år genomföra övningar som myndigheter, nätoperatörer och nätägare är ålagda att delta i.

I och med dessa lagändringar lade Ryssland grunden för att kunna använda sig av en så kallad *kill switch,* en möjlighet att skärma av det ryska segmentet av internet från omvärlden – en begränsad tid eller i en viss region – utan att ryska internetanvändare skulle märka en avsevärd skillnad. Flera andra länder har infört denna möjlighet, t.ex. Storbritannien och Turkiet. Det rör sig dock inte om att kapa alla anslutningar till det globala internet för all framtid, utan snarare om att vid behov kunna skärma av det egna segmentet. Däremot skiljer sig det som skulle vara anledningen för en sådan åtgärd mellan länder; för auktoritära länder är inte sällan demonstrationer och protester skäl för att stänga av internet.

Var Rysslands internet suveränt?

Frågan om Ryssland verkligen hade ett suveränt internet den 24 februari är mer komplicerad än den kan tyckas vid en första anblick. Till att börja med är ett suveränt internet något av en oxymoron. Internets stora värde består i att det är ett nätverk av nätverk. Att frivilligt begränsa antal nätverk innebär därmed en kostnad i termer av att användare får tillgång till färre nätverk, men också att egna data inte når ut på det globala internet – åtminstone inte lika lätt. Det innebär också att trafik kan komma att färdas långsammare när det finns färre alternativa vägar för trafiken att ta. Det internet som vi alla använder nästan dagligen består dels av mjukvara för styrning och routing som lägger grunden för hur vi kan dela information, få tillgång till den och för hur den färdas i kablar; dels består det av hårdvara i termer av alltifrån persondatorer och intranät till servrar och transatlantiska kablar. Slutligen är internet beroende av en ekonomisk infrastruktur, möjligheten att tjäna pengar på trafiken. Denna väldigt ofullständiga beskrivning av hur internet fungerar ger en inblick i hur besvärlig uppgiften att kontrollera ett nationellt segment av internet är.

Till skillnad från Kinas internet växte Rysslands internet fram underifrån utan alltför stor statlig inblandning. Det finns till exempel över 3 500 ryska internetoperatörer, ofta med egna uppkopplingar mot omvärlden, att jämföra med länder som Kazakstan och Belarus som har ett par tiotal.[5] Att kontrollera ett ”ryskt internet” blev därmed en utmaning för ryska myndigheter när de på 10-talet väl tog sig an uppgiften på allvar. Ryssland valde att definiera ett ryskt segment av internet utifrån fysisk infrastruktur som finns inom de ryska territoriella gränserna (kablar, gränsövergångar och noder) och toppdomänstrukturen (.ru, .su och .рф) för att därefter öka kontrollen över dessa. Inte minst skulle alla operatörer tvingas delta i arbetet med att kontrollera trafikinnehållet på internet. Medan ryska företrädare ofta hänvisade till hotet att Ryssland skulle stängas av från internets globala infrastruktur som motivering till åtgärderna, stod uppgiften att öka den statliga kontrollen över en rysk informationssfär på internet av allt att döma också i fokus. Ryssland visade sig däremot långt ifrån så immunt mot cyberattacker som Roskomnadzors chef trodde i oktober 2021.

It-säkerhet

Efter Rysslands förnyade invasion av Ukraina den 24 februari uppmanade Ukrainas digitaliseringsminister, Mychailo Fedorov, till cyberattacker mot ryska ministerier och myndigheter, men startade också en kampanj för att företag som Google och Apple skulle delta i en digital blockad mot Ryssland.[6] Gruppen *Anonymous* anammade uppmaningen att attackera ryska mål. Ukraina skapade dessutom *IT Army of Ukraine,* som bl.a. via

4 Roskomnadzor, "Lista över domännamnsgrupper inom nationella DNS", order nr. 216, 29 juli 2019: https://cdnstatic.rg.ru/uploads/attachments/173/62/92/55686.pdf [2022-08-24]; Roskomnadzor, Förordning för nationellt DNS, order nr. 229. 31 juli 2019: https://cdnstatic.rg.ru/uploads/attachments/177/71/68/56453.pdf [2022-08-24].

5 *Interfax,* “Ostavit nelzia otkljutjit” [Omöjligt att överge avstängning], 4 april 2022: https://www.interfax.ru/digital/833055 [2022-08-15].

6 Zakrzewski, Cat (2022), ”4,000 letters and four hours of sleep: Ukrainian leader wages digital war”, *The Washington Post*, 30 mars: https://www.washingtonpost.com/technology/2022/03/30/mykhailo-fedorov-ukraine-digital-front/ [2022-08-24].

meddelandetjänsten Telegram koordinerade attacker mot Ryssland.[7] Attackerna ledde till att t.ex. kremlin.ru och flera regeringshemsidor var omöjliga att nå redan under eftermiddagen den 24 februari. Även stora bankers hemsidor drabbades, som Sberbank och Alfa-bank. Attackerna var i huvudsak överbelastningsattacker[8] och kunde spåras till datorer i en rad länder (inklusive Ryssland). Attackerna var inledningsvis så kallad *hacktivism,* en social protest snarare än en avancerad attack från en statlig aktör,[9] men så småningom följde även mer avancerade och välorganiserade attacker.[10]

Ryssland var avsevärt mer sårbart och beroende av omvärlden än vad den officiella retoriken hade gett vid handen och tvingades införa så kallad geoblockering för att skydda centrala internetresurser. Det innebar att endast användare i länder inom Oberoende staters samvälde (OSS) kunde nå t.ex. den ryska regeringens hemsidor. Så småningom kunde hemsidorna börja fungera mer normalt, men Ryssland har blivit föremål för omfattande cyberattacker allt sedan 24 februari. Vid ett möte med det ryska Säkerhetsrådets permanenta medlemmar i maj talade president Vladimir Putin om att ”en verklig aggression, ett krig i informationssfären” hade utlysts gentemot Ryssland. Han efterlyste fler åtgärder för att skydda kritisk informationsinfrastruktur.[11]

En instruktion som ryska Ministeriet för digital utveckling skickade till bredbandsoperatörer gav upphov till ett rykte om att Ryssland skulle aktivera sin *kill switch* på fredagen den 11 mars. I själva verket rörde det sig om en instruktion om att flytta webbsidor och webbtjänster till ”ryska servrar”. Det var i sin tur troligen ett led i att förbereda möjligheten att stänga av ryska resurser från omvärlden om behovet skulle uppstå, men också en åtgärd för att skydda landets internetsegment från pågående cyberattacker. En uppmaning om att iaktta försiktighet och se över lösenord åtföljde åtgärden.[12] Att stänga av åtkomsten till det globala internet torde, trots lagen om ett suveränt internet, vara en av de sista tillflykterna för Ryssland liksom för andra länder; konsekvenserna är oförutsägbara för alltifrån enskilda användare och små livsmedelsbutiker till stora sjukhus och bankkoncerner. Åtgärden riskerar därmed att rimma illa med den officiella propagandan om att det som Ryssland ägnar sig åt i Ukraina är en begränsad militär specialoperation och alls inget krig.[13]

Importberoende

Minst suveränt är dock Ryssland i frågan om importberoende. Målet att minska landets beroende av import av såväl mjuk- som hårdvara har varit prioriterat allt sedan Ryssland antog sin första informationssäkerhetsdoktrin 2000. Trots detta har landet snarare halkat längre efter teknologiutvecklingen vad gäller t.ex. mikroelektronik. Det har visat sig svårt att övertala ens statliga bolag att gå över till rysk programvara och ryska operativsystem och landets it-företagare har ofta protesterat mot alltför hårda krav på vad som ska anses vara ”rysktillverkat”.

Efter den 24 februari har denna fråga ställts på sin spets. Bristen på till exempel halvledare är global. För Ryssland tillkommer sanktionerna och en mer allmän ovilja från västliga företag att handla med Ryssland, vilket även gäller företag i Asien som är beroende av handel med USA.[14] Lägg till detta att ryska it-utvecklare verkar ha varit bland de första att lämna landet efter den 24 februari; troligen rör det sig om tiotusentals personer som arbetar inom it-sektorn.[15] Mycket talar för att Ryssland nu har

7 *IT Army of Ukraine,* engelsk kanal på telegram, https://t.me/itarmyofukraine2022 [2022-08-24]. Se även Soesanto, Stefan (2022), ”The IT Army of Ukraine: Structure, Tasking, and Ecosystem”, CSS Cyberdefense Report, juni, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2022-06-IT-Army-of-Ukraine.pdf [2022-08-24].

8 Även benämnda som DDoS-attacker, *distributed denial of service,* och består i att utsätta en hemsida för så många förfrågningar om tillträde att den slutar att fungera som den ska.

9 Stepanova, Julija (2022), ”Bojtsy nevidimogo froda” [Krigare från en osynlig front], *Kommersant, 28 februari:* https://www.kommersant.ru/doc/5238079 [2022-08-24].

10 Stepanova, Julija (2022), ”Frod bez flangov” [Bedrägeri utan flanker], *Kommersant,* 25 februari: https://www.kommersant.ru/doc/5236688. [2022-03-01].

11 Vladimir Putin, (2022), ”O povysjenii ustojtjivosti i bezopasnosti funktionirovanija informatsionnoj infrastryktura gosudarstva” [Om att öka robustheten och säkerheten i statens informationsinfrastrukturs funktionalitet], 20 maj: www.scrf.gov.ru/council/session/3241/ [2022-08-15].

12 *Meduza (2022), “*V Rossii pravda sobirajutsia otkljutjit ’vnesjnij’ internet?” [Förbereder man sig verkligen för att stänga av ’utrikes’ internet i Ryssland?], 6 mars: https://meduza.io/feature/2022/03/06/v-rossii-pravda-sobirayutsya-otklyuchit-vneshniy-internet-chto-eto-znachit-zayti-na-zarubezhnye-sayty-budet-nevozmozhno [2022-08-24].

13 Se t.ex. intervjun med experten Karen Kazarjan, ”Eto dovolno bezumnyj sjag – otkljutat set iznutri” [Att stänga av inifrån, det är ett ganska oövertänkt steg], *Rosbalt,* 21 mars*:* https://www.rosbalt.ru/russia/2022/03/21/1949558 [2022-08-16].

14 Epifanova, Alena (2022), ”Russia’s technological isolation”, *DGAP Online Commentary*, 6 april: https://dgap.org/en/research/publications/russias-technological-isolation [2022-08-24].

15 Se t.ex. Wilde, Gavin och Sherman, Justin, (2022), ”Putin’s Internet Plan: Dependency with a Veneer of Sovereignty”, *Brookings – Tech Stream*, 11 maj: https://www.brookings.edu/techstream/putins-internet-plan-dependency-with-a-veneer-of-sovereignty/ [2022-05-16].

avhänt sig möjligheten att åtminstone balansera sitt beroende av Kina med import även från Väst.

I sitt tal till Säkerhetsrådet i maj påminde Putin om att utländska tjänster för it-skydd var helt förbjudna från 2025 och efterlyste skapandet av en ”rysk elektronisk komponentbas”. Ryssland skulle inte bara stimulera importsubstitutionsåtgärderna utan även komma förbi de konkurrenter som dominerade marknaden idag med egna unika produkter.[16] När Rysslands president uttalat ett mål så marscherar rysk byråkrati i takt – åtminstone retoriskt. Därmed finns nu målsättningar om ”teknologisk suveränitet”,[17] men mer troligt är att Rysslands strategiska mål att ta ett teknologiskt kliv för att bygga landets ekonomiska tillväxt ytterligare försvårats efter den 24 februari. Snarare finns risker för att underhåll och modernisering blir lidande. Det finns t.o.m. farhågor om att landet inte har komponenter för att fullt bygga ut övervakningsutrustningen för ett suveränt internet (TSPU). I april 2022 hade bara 80 företag installerat TSPU – även om de största operatörerna, som VimpelCom och MTS, vilka tillsammans kontrollerar cirka 65 procent av marknaden, hade installerat TSPU så tycks landets suveräna internet vara långtifrån i mål.[18]

Kontroll över information

Framför allt har dock Ryssland vidtagit åtgärder för att skydda sin informationssfär på internet, för att begränsa tillgången till oberoende information för ryska invånare. Efter den 24 februari har repressionen och behovet av att begränsa oberoende informationskällor ökat ytterligare för den ryska politiska ledningen. Det har skett bland annat genom att Roskomnadzor numera blockerar Facebook, Twitter och Instagram (ryska myndigheter har också angivit att Meta har status som extremistisk organisation). Vidare förbjöd Ryssland redan under våren cirka 30 inhemska oberoende media från att verka i landet – som den populära radiostationen *Echo Moskvy* och tevekanalen Dozjd. Ingen av dessa åtgärder har varit hundraprocentigt effektiva. Det går fortfarande att nå Facebook, Twitter och Instagram i Ryssland. Dels är blockeringen inte total och anledningen till detta kan vara att TSPU inte är fullt utbyggt. Dels har många, framför allt unga, internetanvändare skaffat sig VPN-uppkoppling,[19] som tillåter dem att kringgå blockeringen.[20]

Allt talar för att ryska myndigheter kommer att fortsätta att stärka kontrollen över det man definierar som ett ryskt segment av internet. Journalister från *Echo Moskvy* har övergått till att sända över YouTube, som i augusti 2022 fortfarande inte var blockerat i Ryssland. Det finns ryska alternativ, främst tjänsten RuTube, men relativt få har hittills migrerat dit trots åtgärder från ryska myndigheter för att främja en sådan utveckling. Dels uppfattas troligen videotjänsten RuTube som mindre fri och den kommer aldrig att ha lika stort utbud som YouTube. Och storleken har betydelse. Ryska influencers må tvingas lämna Instagram när det stängts ned, men det innebär också för de flesta mindre möjligheter att tjäna pengar på innehåll, vad än rysk propaganda må påstå. Vad gäller RuTube fick också förtroendet en rejäl törn när en hackerattack stängde ned tjänsten under flera dagar. Attacken var avancerad och allt talar för att den genomfördes av en grupp med tillgång till källkoden. Troligen kan det faktum att ryska företag, liksom företag världen runt, outsourcar programutveckling bidragit till att attacken mot RuTube var så pass omfattande och framgångsrik.[21] Att en betydande andel av outsourcade programutvecklare var ukrainare framstod inte som något stort problem före den 24 februari. Nu är det en betydande säkerhetsrisk för Ryssland.

16 Vladimir Putin, (2022), ”O povysjenii ustojtjivosti i bezopasnosti funktionirovanija informatsionnoj infrastryktura gosudarstva” [Om att öka robustheten och säkerheten i statens informationsinfrastrukturs funktionalitet], 20 maj: www.scrf.gov.ru/council/session/3241/ [2022-08-15].

17 Dmitrij Peskov, (2022), ”Ostrov Rossija” [Ön Ryssland], *RBK, 9 juni:* https://www.rbc.ru/opinions/economics/09/06/2022/62a0e95b9a79472d8b713207. [2022-08-15].

18 Anastasija Gavriljuk, (2022), ”Blok kreptjajet” [Stärkt blockering], *Kommersant, 29 mars:* https://www.kommersant.ru/doc/5281701 [2022-08-15]; Interfax, “Ostavit nelzia otkljutjit” [Omöjligt att överge avstängning], 4 april 2022: https://www.interfax.ru/digital/833055 [2022-08-15]. Se även de inspektioner som Roskomnadzor inledde av installationen av TSPU i maj, Tatiana Isakova, (2022), ”Prokurory prodkljutjajutsia k setiam” [Åklagare kopplar upp sig], *Kommersant, 26 maj:* https://www.kommersant.ru/doc/5368526 [2022-08-15].

19 VPN – *virtual private network,* en tjänst som tillåter användare att vara anonyma genom en krypterad ”tunnel” på internet. När en rysk användare med en VPN-uppkoppling t.ex. använder Instagram kan den ryska staten således bara se att det förekommer trafik mellan användaren och en VPN-server, inte vilken hemsida användaren besöker eller vilket trafikinnehåll som förekommer.

20 Levadacentrum, (2022), ”Internet, sotsialnyje seti i VPN” [Internet, sociala medier och VPN], 8 april: https://www.levada.ru/2022/04/08/internet-sotsialnye-seti-i-vpn/ [2022-08-16]. Se även atlasVPN, (2022), ”VPN Usage in Russia Skyrockets by 10,000% Following Instagram Ban”, 15 mars: https://atlasvpn.com/blog/vpn-usage-in-russia-skyrockets-by-10-000-following-instagram-ban [2022-08-16].

21 Aleksandr Plusjtjev, (2022), ”Totjka”, *Youtube,* 15 maj: https://www.youtube.com/watch?v=cSZueZiqvcE&list=PLZVQqcKxEn_6YaOniJmxATjODSVUbbMkd&index=12&t=3s [2022-08-16].

Konsekvenser för Ryssland och för det globala internet

Sanktionerna i kombination med att företag drar sig ur Ryssland på obestämd tid kan också komma att bidra till en uppdelning av internet.[22] Ryssland kommer att tvingas vända sig mer mot Kina och förlita sig på import av kinesisk teknologi liksom av komponenter och t.ex. servrar. Att internationella företag upphör att tillhandahålla sin produktion – alltifrån programvara, uppdateringar av denna till service på redan levererad utrustning och maskinvara liksom inköp av ny sådan – kommer också att få konsekvenser för vilka möjligheter ryska internetanvändare har att få tillgång till oberoende information. Det tillsammans med ryska åtgärder för att begränsa tillgången till oberoende information samt sanktioner som förhindrar ryska internetanvändare att använda sina kontokort för att betala för tjänster, som t.ex. VPN, riskerar att bidra till en uppdelning i olika informationssfärer globalt. Den ryska befolkningen kan komma att befinna sig i en informationsbubbla som ser helt annorlunda ut än det utbud av information som västliga internetanvändare har tillgång till. Troligen finns här också en psykologisk effekt – ryska internetanvändare kan tänkas välja informationsom framhåller Rysslands goda sidor och välja bort den som är kritisk, inte minst i tider då landet framstår som under hot i officiell propaganda. Lägg till detta de möjligheter till övervakning av internettrafiken, som den ryska regeringen har byggt upp samt införandet av stränga straff för att ens benämna den ryska militära operationen som ett ”krig”. En majoritet av den ryska befolkningen riskerar därmed att leva med en bild av vad som händer i världen, inklusive i Ryssland och Ukraina, som stämmer väl överens med den ryska officiella propagandan.

Ingen uppdelning av internet kommer dock att vara total och Ryssland kommer inte att lyckas att helt skära av ryska internetanvändares uppkoppling mot omvärlden. Inte heller tycks Rysslands officiella bild av ett ryskt internet som suveränt ha så mycket med verkligheten att göra. Ryssland har i allt väsentligt förblivit importberoende och de internetanvändare som vill hittar vägar runt blockeringar och övervakning. Vidare tycks de åtgärder som skulle ha vidtagits senast sommaren 2022 inte ha vidtagits fullt ut. Snarare tyder erfarenheten på att såväl ryska myndigheter som landets bredbandsoperatörer och andra aktörer har dragit benen efter sig vad gäller att genomföra åtgärderna – såsom ofta är fallet inom andra sektorer av rysk byråkrati och näringsliv. Samtidigt finns all anledning att fundera över hur typiskt ”ryska” de problem är som Ryssland stångas med på cyberområdet efter den 24 februari 2022. För samtliga länder gäller att det som kan tyckas vara tillräcklig säkerhet på cyberområdet i fred kommer att vara något helt annat i krig. Ryssland är långt ifrån ensamt om att outsourca programutveckling och importera komponenter. Vid en väpnad konflikt kommer dessa svagheter och beroenden att ställas på sin spets. ■

Carolina Vendil Pallin, fil.dr., är forskningsledare vid FOI:s enhet för Säkerhetspolitik.

22 Mueller, Milton (2017), *Will the Internet Fragment? Sovereignty, Globalization, and Cyberspace*, Cambridge: Polity Press. Se även hur geopolitik och Kinas agerande påverkar denna process, Hoffmann, S., D. Lazanski och E. Taylor. (2020), ”Standardising the Splinternet: How China’s Technical Standards Could Fragment the Internet”, *Journal of Cyber Policy* 5(2): 239–264.