Cybersäkerhet och cyberoperationer

Rysk doktrin och praktik[1]

av Carolina Vendil Pallin

Säkerhet i morgondagens Europa
– SVENSKA PERSPEKTIV

Résumé

Russian official documents rarely, if ever, mention the word "cyber". The key word is "information", where information security and warfare encompasses everything from protection of infrastructure to propaganda and control over social media. It is in fact impossible to understand many of the policy choices and activities that Russia undertakes in the cyber realm without understanding its need to control information content as well as the routes the information travels. The Russian Security Council and the Federal Security Service (FSB) have come to dominate decision making on cyber. In the most important document, the Information Security Doctrine from 2016, four areas stand out: the protection of critical information infrastructure; reducing Russia's dependence on foreign technology; controlling both internet traffic and content; and, finally, reaching an international agreement on information security that mirror Russian concerns. Within the Armed Forces, cyber security and warfare is a subcategory to within electronic warfare and secure communications. Many of the cyber operations attributed to Russia were most likely conducted by the intelligence and security services, most notably the FSB and the Military Intelligence Directorate (GRU). In sum, Russia is probably among the top five countries when it comes to conducting cyber operations, but it is also increasingly worried about its own cyber security. Its prime concern, however, tends to be control over information content and surveillance of the domestic population.

EN GOOGLING PÅ orden "Ryssland" och "cyber" ger inte bara en stor mängd resultat, den resulterar också i braskande rubriker om "cyberhot från Ryssland" och "ryska cyberattacker". En motsvarande sökning på ryska med orden "Россия" (Ryssland) och "кибер" (cyber) resulterar främst i information om ett ryskt företag med namnet "Cyberryssland" (*Kiber Rossija*). Sökorden "США" (USA) och "кибер" resulterar inte heller i träffar om amerikanska cyberattacker mot Ryssland. Istället genereras material om USA:s cyberstrategi och om nätshoppingresultatet under "cybermåndagen" i USA. Vad förklarar denna diskrepans mellan hur intresserade vi tycks vara av cyberhot från Ryssland och Rysslands till synes mer matta intresse? Är Ryssland ledande på cyberoperationer? Är Ryssland obekymrat om cyberattacker mot egna landet? Beror det i så fall på att Ryssland inte anser sig vara sårbart på området?

Diskrepansen ovan bottnar i den ryska synen på cyber som en del av en större helhet där ledordet är "information" snarare än "cyber". Ryssland har t ex en uppdaterad informationssäkerhetsdoktrin från 2016 och dess

väpnade styrkor har ett dokument med titeln ”Konceptuell syn på Ryska Federationens Väpnade styrkors verksamhet i informationssfären” från 2011.[2] Ordet ”cyber” nämns som regel inte i ryska officiella dokument. Istället delas informationssäkerhet upp i teknisk informationssäkerhet och psykologisk informationssäkerhet, där det första begreppet närmast motsvarar det som väst vanligen refererar till som cybersäkerhet. Samtidigt är det inte så enkelt att man bara kan dela upp det ryska begreppet och översätta det till cyber. Ryssland ser på informationssäkerhet och informationskrigföring som en helhet och för in alltifrån cyberattacker och skydd av infrastruktur till det som skrivs på sociala medier, sägs på tevekanaler och i uttalanden av Hillary Clinton i samband med protesterna i Kiev 2013–2014 under samma informationsparaply. Det här är väsentligt att förstå även för den som studerar främst Rysslands doktrin och handlande på det tekniska informationssäkerhetsområdet.

Ryssland är allt annat än obekymrat på cyberområdet och en hel del av dess oro för psykologisk informationskrigföring spiller dessutom över i åtgärder på den tekniska informationssäkerheten. Sålunda offras inte sällan driftsäkerhet och inhemsk innovationspolitik för att man ska uppnå mer kontroll över vilken information som färdas i RuNet, det segment av internet har definierats av att ryska var huvudspråket och domänadresserna slutade på .ru eller .su (eller ibland med .pф).

En av förklaringarna till hur rysk syn på cyberstrategi har utvecklats är vilka aktörer som varit huvudsakligen ansvariga för utformningen av den i det ryska politiska systemet. Denna artikel analyserar därför inledningsvis beslutsfattande på cyberområdet. Rysslands doktrin vad gäller cybersäkerhet är tillgänglig framför allt i informationsdoktrinen men också i andra strategiska dokument. Dess innehåll delas i analysen nedan upp i fyra huvudsakliga politikområden: att skydda kritisk informationsinfrastruktur; att gynna den inhemska informations- och kommunikationsindustrin; att kontrollera trafikinnehåll på internet; och att nå ett för Ryssland gynnsamt internationellt avtal om informationssäkerhet. Därefter diskuteras även de väpnade styrkornas syn på cybersäkerhet och hur cyberoperationer förhåller sig till telekrig och militära psykologiska operationer. Slutligen kan konstateras att en rad uppmärksammade cyberoperationer har attribuerats till Ryssland. Här finns inga öppna doktriner att tillgå utan analysen av rysk syn på cyberoperationer utgår ifrån landets agerande på området.

Beslutsfattande på cyberområdet

Ett par år efter det att Vladimir Putin blivit president år 2000 hade mediefriheten i Ryssland begränsats avsevärt. Samtidigt var emellertid friheten på internet fortsatt relativt oinskränkt. Så sent som 2014 rankades fortfarande landet som ”delvis fritt” i Freedom House’ årliga rapport om friheten på internet i olika länder.[3] Denna relativa frihet som internetanvändarna kunde åtnjuta var resultatet av att internet länge ignorerades av landets politiska ledning; rikstäckande television och press kontrollerades redan direkt av statliga bolag eller indirekt genom att tevestationer eller tidningar ägdes av så kallade oligarker, affärsmän nära lierade med den politiska makten. Den arabiska våren från sent 2010 och de stora demonstrationerna i Ryssland 2011–2012 innebar att den politiska ledningen riktade sin uppmärksamhet även mot internet. Det är omöjligt att konstatera exakt vilken roll sociala medier spelade under arabiska våren och senare i Ryssland. Det som är möjligt att konstatera är

att politiker och myndigheter drog slutsatsen att kontrollen över internet behövde ökas.

Även om internet förblev relativt fritt fram till början av 2010-talet, hade krafter hela tiden funnits inom det ryska politiska systemet som ville begränsa den frihet som nya informations- och kommunikationsteknologier innebar. Bland de myndigheter som ville öka kontrollen fanns främst Federala säkerhetstjänsten (FSB), men också Federala tjänsten för teknisk exportkontroll (FSTEK). Inte minst hade myndigheter som dessa ärvt inneboende misstänksamhet mot yttrande- och kommunikationsfrihet från sin föregångare, KGB (den sovjetiska säkerhetstjänsten), som hade varit ansvarigt för bl a kryptering och avlyssning av kommunikationer inom landet.[4] Dessutom fanns starka krafter inom säkerhetsrådets kansli som hade en liknande agenda och bara några månader efter att Putin hade valts till president i mars 2000 låg en första informationssäkerhetsdoktrin på hans bord för underskrift.[5]

Denna första informationssäkerhetsdoktrin innehöll många av de huvudteman som återkom i den version som antogs 2016. Den stora skillnaden låg i det genomslag som de båda fick i praktiken. Även om nya säkerhetsbehov som en följd av de nya informations- och kommunikationsteknologierna behandlades i dokumentet 2000, ledde det till exempel inte till att Ryssland fick lagar som reglerade skydd av infrastruktur. FSB kunde i viss utsträckning övervaka den trafik som passerade ryska servrar, men mycket trafik rörde sig utanför Rysslands geografiska gränser och var dessutom ofta krypterad.

Den arabiska våren och demonstrationerna 2011–2012 blev i praktiken startskottet för ryska myndigheters insatser för att öka kontrollen över det ryska internet. Efter det att Putin åter hade valts till president våren 2012, gjordes också förändringar inom presidentadministrationen, som fick ett direktorat för användande av informationsteknologi och utveckling av valdemokrati. Dessutom blev en före detta kommunikationsminister, Igor Sjtjegolev, presidentrådgivare med ansvar för att leda det nya direktoratets arbete.[6] Samtidigt blev det kommunikationsministeriet och dess underlydande myndighet, Roskomnadzor (Federala tjänsten för övervakning av kommunikationer, informationsteknologi och massmedia), allt viktigare i arbetet med att tygla internet i Ryssland.

De största ägarna av internetföretag och de statliga företagen dominerar idag sektorn och tenderar att stödja regeringens politik.[7] Ytterligare stöd finner regeringen hos så kallade GONGO:s (*government-controlled non-governmental organizations*) regeringskontrollerade organisationer. Till exempel har ”Ligan för ett säkert internet” varit mycket aktiv i att föreslå tuffare lagstiftning och German Klimenko var en av grundarna av ”Internetutvecklingsinstitutet”, beskrivet som en plattform för dialog mellan företagare och tjänstemän. Klimenko blev presidentrådgivare (*sovjetnik*) för internetutveckling 2016 och har även efter att han lämnade den posten 2018 öppet stött den förda politiken. Det ryska parlamentet har också varit aktivt i att föreslå ytterligare åtgärder för att öka kontrollen över internet och ledamöter i både överhuset, federationsrådet, och underhuset. Duman, uttalar ofta sitt stöd för regeringens politik på området.

Samtidigt är den ryska regeringen och dess tentakler, i form av ministerier och myndigheter, inte alltigenom monolitiska. Remissvaren från olika ministerier och lagförslag om ökad kontroll över internet visar tydligt att det finns olika mål och preferenser. Myndigheter som FSB tenderar att vara för sådan lagstiftning, medan t ex finansministeriet och ministeriet för ekonomisk utveckling har invändningar.[8] Det finns också en betydande grad av konkurrens mellan olika underrättelse- och

säkerhetstjänster, vilket kan resultera i att lagstiftning försenas väsentligt.[9] Tidigare fanns dessutom ett betydande motstånd mot ökad kontroll från internetföretagen, men denna kritik har blivit alltmer dämpad allteftersom staten i praktiken har stärkt sitt direkta eller indirekta ägande inom sektorn. De största företagen är också väl medvetna om att de är beroende av den politiska makten och att de i slutänden brukar kompenseras av regeringen för eventuella kostnader. I takt med ett hårdnande politiskt klimat har tendensen varit att kontrollförespråkarna får igenom sin politik trots protester och de kostnader det medför för staten och samhället i stort.

Rysk cybersäkerhet

Enligt den ryska Informationssäkerhetsdoktrinen från 2016 är Ryssland föremål för informationsoperationer som syftar till att underminera landets position internationellt liksom även dess politiska system och ”samhälleliga säkerhet”. Samma syn återkommer i den nationella säkerhetsstrategin, militärdoktrinen, konceptet för samhällelig säkerhet och utrikespolitiska konceptet.[10] Detta tema är starkt återkommande liksom det om hur så kallade färgrevolutioner som demonstrationerna på Majdan i Kiev 2013–2014 är iscensatta av Väst och hotar Rysslands säkerhet.[11] Och då är det som Moskva definierar som skadlig information ett verktyg i en operation för att underminera Ryssland. Nästan lika starkt framhävs faran för att vara beroende av västlig teknik, och att den globala infrastrukturen för internet framför allt finns belägen på västligt territorium. Ryssland har vidare som uttalat mål att nå ett internationellt avtal som bättre speglar landets intressen på informationssäkerhetsområdet.

Samtliga dessa teman betonades vid ett möte i säkerhetsrådet i oktober 2014.[12] Det kan vara värt att minnas situationen som landet då befann sig i. Ryssland hade annekterat Krim, attackerat Donbasområdet i östra Ukraina militärt, och styrkor under rysk kontroll hade skjutit ned ett civilt passagerarplan, MH-17. Den ryska motelden i form av desinformation om MH-17 var intensiv, samtidigt som västliga sanktioner hade införts och fler väntade. För Ryssland var det av största vikt att behålla ett folkligt stöd för den förda politiken men också att skydda egna informations- och kommunikationssystem. Den ryska politiska ledningen blev akut medveten om hur beroende landet var av internationell infrastruktur för t ex överföring av pengar (*Swift*), men också av den globala infrastrukturen för internet. Tanken på att skapa en parallell infrastruktur för internet inom Rysslands gränser hade fötts och mycket talar för att huvudlinjerna för 2016 års Informationssäkerhetsdoktrin drogs upp vid detta möte.

Rysk infrastruktur

När cybersäkerhet diskuteras tänker många på behovet av att skydda kritisk informationsinfrastruktur från attacker, haveri eller handhavandemisstag som gör att information så att informationen inte längre är pålitlig (integritet), konfidentiell eller tillgänglig.[13] Även i Ryssland fanns redan 2000 en medvetenhet om vikten av att skydda kritisk informationsinfrastruktur.[14] Samtidigt tycks frågan inte ha varit tillräckligt högt prioriterad för att få till stånd lagstiftning på området. Under många år tilläts rivalitet mellan olika delar av den ryska byråkratin, främst mellan FSB och andra ministerier och myndigheter, försena en lag om kritisk informationsinfrastruktur. I praktiken hade FSB redan fått nyckelansvar i den process (*Gosudarstvennaja Sistema obnaruzjenija, predotvrasjtjenija i likvidatsii posledstvij kompjuternych atak*, GosSOPKA), som

reglerar hur cyberattacker ska upptäckas, förhindras, bekämpas. Även FSTEK har en viktig roll då den är utvärderar om tillräckliga åtgärder vidtas samt bestämmer vad som är kritisk informationsinfrastruktur.[15]

Informationsdoktrinen från 2016 underströk återigen att informationshot måste upptäckas i tid och bekämpas samt att utländsk kontroll över hanteringen av kritisk informationsinfrastruktur inte borde vara tillåten.[16] Först 2017 antogs den lag som reglerar skyddet av kritisk informationsinfrastruktur och även stipulerar hur processen för incidenthantering ska ser ut inom federala och regionala myndigheter, inklusive statliga företag.[17]

Ryssland är således bekymrat för att landet utsätts för cyberattacker. Väldigt ofta ligger fokus på cyberattacker ”från utlandet” och då uttalat eller underförstått ”från väst”, samt utan någon differentiering mellan vad som är t ex cyberkriminalitet och avancerade cyberattacker utförda av en annan stat.[18] Den dominerande andelen av attacker torde utgöras av cyberkriminalitet och annan verksamhet som har föga att göra med attacker från annan stat, vilket är fallet för Ryssland precis som för andra länder. Något som sällan eller aldrig nämns från ryskt officiellt håll är att även Kina bedriver cyberoperationer gentemot Ryssland, detta trots det samarbete på cyberområdet mellan de båda länderna som den politiska nivån istället gärna framhåller och prisar.[19]

Förutom cyberattacker oroade sig dock den ryska politiska ledningen sig alltmer för hur beroende landet var av den globala infrastrukturen för internet. Under 2019 antogs en lag om ett ryskt, suveränt internet, ibland refererat till som att Ryssland skulle vara i färd med att bygga ett ryskt internet, ett RuNet.[20] I själva verket kodifierade lagen en rysk ambition att kunna vara oberoende av denna globala infrastruktur, som i stor utsträckning befinner sig i väst. Lagförslaget lanserades under rubriken ”ett suveränt internet”. Det var också ytterligare ett steg mot att binda RuNet till ryskt territorium, att nationalisera det ryska segmentet och därmed öka regeringens kontroll över infrastrukturen, men också över innehållet i trafiken. Lagen innebär att trafiken dirigeras och måste passera specifika noder. Det definierar vad som är gränsövergångar och internetknutpunkter (*internet exchange points*, IXP), och trafiken ska kunna styras centralt om ett hot uppstår. Dessutom ska RuNet kunna fungera autonomt från det globala internet, d v s Ryssland inför möjligheten till en så kallad *kill switch*. Det fanns ett betydande motstånd mot lagen såväl inom regeringen som i samhället i stort, men den politiska ledningen ställde sig otvetydigt bakom det och därmed var saken avgjord.[21] Putin uttalade sitt stöd för lagstiftningen vid ett möte med massmedierna: ”Ja, på det stora hela, ju mer suveränitet vi har, inklusive inom den digitala sfären, desto bättre.”[22]

Minska beroende av utländsk teknik

Det var inte bara beroendet av den globala infrastrukturen som oroade – Ryssland är i hög grad beroende av import av såväl hårdvara som programvara. Informationssäkerhetsdoktrinen från 2016 anger att ett nationellt intresse är att utveckla den inhemska IT-industrin och att minska den avhängighet av utländsk IT som gör Ryssland ”beroende av andra länders geopolitiska intressen”. Enligt doktrinen använder ”vissa länder” sitt teknologiska övertag för att dominera informationssfären.[23] Liknande farhågor och målsättningar fanns redan i doktrinen från 2000, men relativt få framsteg kunde noteras när nästa doktrin publicerades.[24] Den här gången, 2016, knöt den ryska regeringen

ihop olika åtgärder för att öka oberoendet av utländsk IT till ett större program på området, programmet Digital ekonomi, och till den importsubstitutionspolitik som också resulterat i ett regeringsprogram.[25] Vidare inrättades register över vad som godkänts som ”rysk” mjukvara respektive hårdvara och statliga myndigheter och företag ålades att i första hand använda godkända ryska produkter.

Även efter första informationssäkerhetsdoktrinen vidtogs en del åtgärder för att på konstgjord väg gjuta liv i den ryska produktionen av datakomponenter, programvara och annan utrustning.[26] Samtidigt är det tydligt att det är svårt att framtvinga innovationer uppifrån, statliga stödprogram till trots. Ryssland står således inför en rad problem. Det stod snart klart att t o m ministerier och myndigheter visade sig vara ovilliga att övergå till rysk programvara. Den ryska revisionskammaren konstaterade i början av 2019 att federala myndigheter fortsatte att använda sig av ickerysk programvara, 96 procent använde programvara som inte fanns i det ”ryska” registret och 82 procent använde dessutom servrar som fanns i utlandet.[27] Att etablera en rysk produktion av komponenter och hårdvara som skulle stå sig i internationell konkurrens har visat sig än svårare.

Den symbios mellan näringsliv och politiska makten som etablerats i Ryssland gör också att de stora företagen med goda statliga kontakter tar hand om den dominerande delen av de statliga subventioner och stimulanspaket som regeringen sjösätter. Detta tillsammans med ett ogynnsamt företagsklimat hindrar en dynamisk innovationssektor från att växa fram, en sektor som skulle kunna driva en utveckling nerifrån. Tvärtom har förutsättningarna försämrats. ICT-sektorn var tidigare relativt dynamisk jämfört med andra delar av ryskt näringsliv. Ryssland var ett av få länder där konkurrenskraftiga ryska alternativ till marknadsdominerande sociala medier och sökmotorer utvecklades. Pavel Durov, som skapade det som ofta kallas ”ryska Facebook”, VKontakte, tvingades bort från företaget och lever numera i USA, ägaren av det framgångsrika Yandex tvingades under 2019 att acceptera en ”överrock” för styrning av företaget som ökar statens kontroll.[28] Det ständigt ökade statliga behovet av kontroll över ICT-sektorn och landets ekonomi och politik lägger i praktiken en rad hinder i vägen för att nå målet att minska beroendet av utländsk program- och hårdvara.

Kontroll över trafikinnehåll

Framgången med att ersätta import med inhemsk produktion lyser således med sin frånvaro, medan statens kontroll över innehåll och hur trafiken dirigeras på internet har ökat. I och med att lagen om ett suveränt internet antogs 2019 uppmärksammades framför allt möjligheten att stänga av det ryska segmentet av internet från omvärlden. I själva verket var de delar av förslaget som ökade kontrollen över trafiken väl värda att notera. Ryssland skärper kontrollen över trafik som kommer in i eller lämnar landet och kan i och med lagändringen installera teknisk utrustning som kan filtrera och blockera trafik vid noder som all trafik tvingas passera. Det innebär ytterligare ett verktyg för den ryska staten för att bedriva övervakning och kontroll över internet och ska läggas till en lång rad av åtgärder som landet vidtagit för att inskränka friheten på internet.

Ryssland är långt ifrån ensamt. Andra auktoritära länder inför liknande lagstiftning eller har redan gjort det. Även demokratiska länder har vidtagit åtgärder för att kunna kontrollera trafiken på internet. Den stora skillnaden mellan auktoritära länder och demokratiska är bristen på oberoende

granskning av statens förehavanden i länder som Ryssland och att dessa inte är rättsstater där medborgare, organisationer och företag kan hävda sina rättigheter i domstol.[29] För många kom lagförslagen om ett ”suveränt internet” som en överraskning, men de ligger väl i linje med den färdplan som dragits upp i programmet ”Digital ekonomi” under rubriken ”Informationssäkerhet”.[30]

Till den skärpta lagstiftningen och en ökad benägenhet att väcka åtal mot innehåll på internet ska även läggas de mer informella signaler som förekommer i Ryssland idag. Det kan vara påtryckningar i form av reprimander på jobbet, att en frispråkig websida utsätts för överlastningsattacker eller trakasserier, våld eller hot om våld. Enligt människorättsorganisationen Agora har till och med mord begåtts för att tysta frispråkiga skribenter på internet. Agora listar de olika åtgärderna för att begränsa friheten på internet årligen och ökningen under perioden 2011–2019 är slående, se Tabell 1. Under 2011 noterade Agora 500 begränsningar och under 2018 över 660 000. En första markant ökning kan ses 2015–2016 och sedan ytterligare en skarp sådan 2018 då antalet blockerade websidor ökade drastiskt.

Trafikinnehållet kontrolleras således genom en blandning av tekniska åtgärder och censur. Ryska myndigheter övervakar i större utsträckning trafiken och har möjlighet att stänga ned den, enskilda websidor, såväl som servrar och all trafik lokalt i ett område. Ett ökat inslag av censur finns idag i Ryssland på internet genom att myndigheter ingriper mot otillåtet innehåll, men troligen är det än mer kostnadseffektivt för regeringen att uppmana till självcensur genom informella påtryckningar. Dessa åtgärder syftar till att öka den psykologiska informationssäkerheten och Informationssäkerhetsdoktrinen från 2016 anger även i paragraf 8 att informationsteknologi ska användas ”för att bevara Ryska federationens multinationella folks kultur samt historiska och andliga moraliska värden”. Ryssland tycks vara berett att bära betydande kostnader, både direkta och indirekta sådana, för att uppnå dessa mål.

Internationellt avtal om informationssäkerhet

Ryssland arbetar också aktivt för att få till stånd ett avtal om informationssäkerhet som bättre speglar landets intressen på området. Redan 2011 lanserade Ryssland ett förslag till en konvention för internationell informationssäkerhet och landet är mycket aktivt inom Förenta nationerna för att få gehör för den ryska synen.[31] Det går en skiljelinje inom FN mellan västländernas syn på informationssäkerhet och den som Ryssland tillsammans med många andra auktoritära länder driver. Medan väst fortsatt vill se en så kallad *multistakeholder*-modell där stater samverkar med privata aktörer och icke-vinstdrivande organisationer för att komma överens om hur internet ska regleras internationellt, vill Ryssland tillsammans med länder som Kina att stater ska ha den dominerande rollen och att varje land ska ha rätt att utveckla sin mer eller mindre geografiskt bestämda informationssfär utan inblandning från omvärlden. Det finns också en konflikt om ansvaret för hur internets globala infrastruktur ska styras och hanteras. Vidare vill väst inom ramen för internationell informationssäkerhet främst diskutera frågor som främst har att göra med informationstrafikens funktionalitet, medan Ryssland vill förhandla om trafikens informationsinnehåll.[32]

Det finns små utsikter för att dessa två synsätt ska kunna gå att kombinera eller att en kompromiss skulle kunna mäklas fram inom en nära framtid. Dock har Ryssland varit desto med framgångsrikt i att bygga

Begränsning									
	2011	**2012**	**2013**	**2014**	**2015**	**2016**	**2017**	**2018**	**2019**
Mord	1	–	1	1	–	–	1	0	0
Våld (hot)	10	3	23	26	28	50	66	59	57
Regleringsförslag	5	49	75	87	48	97	114	82	62
Åtal	38	103	226	132	202	298	411	384	200
/varav resulterade i fängelsedom					/18	/32	/48	/45	/38
Administrativa påtryckningar	173	208	514	1 448	5 073	53 004	22 523	4 402	3 917
Restriktioner att nå material	231	609	236	947	1 721	35 019	88 832	488 609	161 490
Domstolsåläggande	–	124	624	72	7 300	24 000	2 196	161171	272 785
Cyberattacker	31	47	63	10	30	122	15	20	32
Civilrättsliga åtgärder	11	26	37	60	49	170	39	58	79
Statlig nedstängning	*noterades ej*								8
Påtryckningar på IT-industrin och programmerare	*noterades ej*								12
Övrigt	–	28	34	168	570	3 343	1 509	8 057	339
Totalt:	**500**	**1 197**	**1 833**	**2 951**	**15 021**	**116 103**	**115 706**	**662 842**	**438 981**

Tabell 1. Agoras årliga rapporter om friheten på internet, 2011–2019.

Källa:

Agora och Radio Svoboda ”Svoboda interneta 2019: plan ’Krepost’”, Agoras årliga rapport om friheten på internet, 4 februari 2020, *https://2019.runet.report/assets/files/Internet_Freedom%202019_The_Fortress.pdf* (2020-02-05); Agora: ”Svoboda interneta 2018: delegirovanije repressij”, Agoras årliga rapport om friheten på internet, 5 februari 2019, *https://guides.files.bbci.co.uk/bbc-russian/AGORA_Freedom-of-the-Internet-2018.pdf* (2020-01-13). Tabellen bygger även på data en tidigare rapport, Agora: ”Svoboda interneta 2017: polsutjaja kriminilizatsija”, 5 februari 2018, *https://meduza.io/static/0001/Agora_Internet_Freedom_2017_RU.pdf* (2020-01-13).

* Agoras data om restriktioner för tillgänglighet på internet är baserad på officiell statistik. Enligt organisationen RosKomSvoboda blockerades i själva verket väl över tio miljoner resurser under 2018. RosKomSvoboda: ”Raspredelenije blokirovok sajtov po vedomstvam”, *https://reestr.rublacklist.net/visual* (2020-01-13).

** I kategorin ”Övrigt” ingår alltifrån att någon avskedats från sitt jobb p g a sitt inlägg på internet till att Ryssland begärt och i mycket begränsad omfattning även fått ut persondata från företag som Google och Facebook (se tabellen som finns som bilaga till Agoras rapport om 2018, *https://guides.files.bbci.co.uk/bbc-russian/AGORA_Freedom-of-the-Internet-2018_Table.xlsx* (2020-01-13).

allianser på området med länder som Kina, de centralasiatiska länderna och auktoritära länder som delar Rysslands vilja att kontrollera information inom sina respektive politiska system. Ryssland har aktivt drivit på dessa frågor inom regionala organisationer som Collective Security Treaty Organization (CSTO), Shanghai Cooperation Organization (SCO) och även inom BRICS (bestående av länderna Brasilien, Ryssland, Indien, Kina och Sydafrika). SCO har tagit fram en ”Internationell uppförandekod för informationssäkerhet”, som SCO-länderna cirkulerade inom FN 2015. Detta inspel fick föga stöd inom FN kanske delvis för att det så uppenbart speglade kinesiska och ryska intressen genom formuleringar om digital suveränitet och om att stater ska avhålla sig ifrån att använda ICT för att ”blanda sig i andra staters inre angelägenheter i syfte att underminera deras politiska, ekonomiska och samhälleliga stabilitet”.[33]

Under 2018 och 2019 kunde Ryssland också notera viss framgång inom FN. Dels lyckades Ryssland få igenom en resolution som innehöll tretton ”internationella regler, normer och principer” en slags uppförandekod 2018, om än utan de mest kontroversiella formuleringarna i SCO:s uppförandekod.[34] Dels antogs den resolution om cyberkriminalitet som Ryssland lagt fram in FN:s Generalförsamling tillsammans med ytterligare 26 länder, bland vilka kan nämnas Angola, Belarus, Kina, Nordkorea, Syrien och Venezuela.[35]

Rysk militär cybersäkerhet

För att reda ut vilken del av allt detta som Rysslands Väpnade styrkor ansvarar för får man återigen borra i den ryska terminologin på området. Som nämndes inledningsvis diskuterar ryska dokument som regel det som i väst benämns cybersäkerhet endast som en del av det större begreppet informationssäkerhet. Det gäller även på det militära området. I informationssäkerhetsdoktrinen från 2000 listas alla slag av underrättelseverksamhet; telekrig och intrång i datornätverk; informationspsykologisk påverkan; och ”verksamhet mot Rysslands intressen inom den militära sfären” som huvudsakliga hot.[36]

Informationssäkerhetsdoktrinen från 2016 är något mer kortfattad, men återigen omfattar tänkandet både teknisk och psykologisk informationssäkerhet. Bland de strategiska mål som listas är de militära att utveckla ett system för väpnade styrkornas och annans trupps informationssäkerhet ”inklusive styrkor och medel för informationskonfrontation”, men också att ”neutralisera informationspsykologisk påverkan”.[37] Det är således ofta omöjligt att skilja ut specifika cyberstrategier eller enskilt cybertänkande.[38] Försvarsministeriets eget dokument ”Konceptuell syn på Ryska Federationens Väpnade styrkors verksamhet i informationssfären” från 2011 anger en lång rad aktiviteter som Väpnade styrkornas staber och förhand bör ägna sig åt inom ”informationsrymden”. Bland dessa ingår:

- underrättelseverksamhet;
- operativ vilseledning (*maskirovka*);
- telekrig;
- samband;
- dold och automatiserad ledning;
- stabers informationsarbete;
- skydd av egna informationssystem från påverkan från påverkan genom telekrig, datorer eller annan form av påverkan.[39]

I och med att allt mer informationsteknologi ingår i väpnade styrkornas utrustning och ledningssystem har de också blivit mer sårbara för cyberattacker. Det noterades i ”Konceptuell syn…” redan 2011 och utvecklingen

efter det torde ha gjort frågan än mer aktuell. Sedan hösten 2016 finns ett ”militärt internet”, *Zakrytyj segment peredatji dannych, ZSPD*, som inte är uppkopplat mot internet och har cirka 180 000 användare. Endast godkänd utrustning får användas och terminalerna är spärrade mot att ansluta t ex vanliga USB-stickor eller externa hårddiskar. I praktiken är det ett militärt intranät. Försvarsministeriet bygger också ut infrastruktur i form av ett rikstäckande datanätverk (*Multiservisnaja transportnaja set svjazi*, MTSS) för samband och säker dataöverföring i form av bland annat fiberoptisk kabel genom Arktis; ett nätverk som ZSPD ska integreras i. Vidare ska det finnas ett IT-säkerhetscentrum i varje militärdistrikt som dygnet runt bevakar trafiken i nätet för att bekämpa cyberattacker.[40]

Försvarsministeriet har med andra ord vidtagit omfattande åtgärder för att skydda sina egna IT-system, men det kan vara värt att notera att fram till att MTSS är i full funktion använder försvarsministeriet fortfarande nät som drivs av statliga Rostelekom, samt att en koordinerande IT-säkerhetsfunktion skulle upprättas i samtliga militärdistrikt först 2019. IT-säkerhetsförband (kompanier) har dock även tidigare funnits i varje militärdistrikts sambandsbrigad.[41]

I ryska och internationella medier har det förekommit uppgifter om att Ryssland har satt upp ”cybertrupper”. Alla sådana rapporter bör tas med en nypa salt. Återigen spökar den ryska terminologin, och när försvarsministern Sergej Sjojgu i en redovisning inför parlamentet, duman, i februari 2017 på en direkt fråga svarade att ”informationsoperationstrupper” hade bildats inom väpnade styrkorna är det ännu inte alldeles klart vad Sjojgu avsåg, men en närläsning av vad som faktiskt sades leder tankarna till propagandaförband.[42] Troligen ligger många av de funktioner som kan definieras som cyberrelaterade inom telekrigstrupperna. Den ryska definitionen av telekrig har ändrats och omfattar idag attack mot och skydd av ”informationstekniska objekt”. Bland de uppgifter som telekrigstrupperna har finns ”funktionell attack” som dels kan innebära högenergivapen, dels datanätverksoperationer. Cybersäkerhet ingår troligen som en av uppgifterna inom ramen för de åtgärder man vidtar för att hindra t ex teknisk underrättelseinhämtning.[43]

Den exakta uppdelningen mellan FSB och Väpnade styrkorna samt andra tjänster som t ex Federala skyddstjänsten (som bl a ansvarar för säkra regeringssamband inklusive presidentens) är svår att fastställa. Helt klart finns en betydande rivalitet och de väpnade styrkorna har fått se FSB ta huvudansvaret för nationell cybersäkerhet.[44] Det är också främst underrättelse- och säkerhetstjänsterna genomför offensiva cyberoperationer.

Ryska cyberoperationer i praktiken

Ryssland befinner sig troligen i toppskiktet vad gäller att kunna genomföra cyberoperationer. Andra länder som också bedömts vara bland de mest aktiva och kunniga på detta område är USA och Kina och bland dessa tre är USA definitivt den ledande cybermakten.[45] Det finns också en klar länk mellan att vara skicklig på cyberförsvar och att kunna genomföra offensiva cyberåtgärder.[46]

Vad är då en sofistikerad attack? Att en attack är lyckosam i att ta sig in i ett nätverk säger inte i sig något om hur sofistikerad den är. Snarare kan säkerhetsrutinerna inom det IT-system som attackeras vara dåliga. Den ryska ledande IT-säkerhetsfirman, Kaspersky Lab, uppskattade 2017 att mindre än en procent av alla cyberattacker under ett år genomförs av en ”hackarelit”.[47] Det som är ett mått på om en attack är sofistikerad är

t ex om den kan skräddarsys för det avsedda målet, om den skadliga koden biter sig fast eller är lätt att avlägsna från det attackerade systemet, om attacken kan genomföras snabbt, om få misstag begås under attacken, och om målet med attacken är högt ställt eller inte.[48] Som regel är det framför allt stater som har resurserna och förmågan att genomföra sofistikerade cyberoperationer, och de benämns därför ofta som APT (*advanced persistent threat*) som är i en helt annan liga än t ex de cyberkriminella.

Rysslands officiella ståndpunkt är att landet inte ägnar sig åt försök att blanda sig i andra länders inre angelägenheter. Det finns således ingen öppen doktrin för landets offensiva cyberoperationer. Icke desto mindre har Ryssland pekats ut som liggande bakom en rad cyberoperationer. Även om absolut attribuering av en cyberattack alltid kommer att vara svår att göra, finns det goda grunder för att anta att Ryssland har genomfört en rad cyberoperationer.

Det är framför allt två så kallade ”tjänster” som har pekats ut som liggande bakom de mest uppmärksammade cyberoperationerna, den militära underrättelsetjänsten, GRU,[49] och FSB. Det är oklart i hur stor utsträckning dessa två koordinerar sina verksamheter, och allt tyder på att det finns en betydande grad av konkurrens mellan dessa två tjänster och då inte minst på cyberområdet.[50] GRU ansvarar sannolikt för de cyberoperationer som brukar attribueras till ATP28 eller Fancy Bear. Bland de som utsatts för attacker av ATP28 kan nämnas anti-dopingsbyrån WADA, militära myndigheter och amerikanska demokratiska partiet. Gruppen ATP28 jobbar sannolikt för FSB och bröt sig också in hos demokratiska partiet i USA, men även Vita huset och State Department. Andra cyberoperationer som har kopplats till Ryssland är de som grupperna TURLA Team, KOALA Team och SANDWORM ligger bakom. Alla dessa har riktat in sig på energisektorn, men också andra sektorer.[51]

Det finns en betydande spännvidd mellan de mest sofistikerade av attackerna som de här grupperna har utfört och inte sällan har undermåligt säkerhetstänkande hos målet för attacken gjort ett intrång relativt okomplicerat. Det faktum att attackerna har avslöjats, och dessutom med hjälp av digitala forensiska metoder blivit spårade till Ryssland, gör också att de inte tillhör toppskiktet av avancerade cyberoperationer. Samtidigt kan det inte uteslutas att Ryssland har utfört operationer eller planterat skadlig kod som inte har upptäckts än. De operationer som landet redan har utfört har också resulterat i erfarenheter och kunskaper som kan användas i framtida operationer.[52]

Ryssland använder sig också av så kallade ”proxies”, personer som genomför olika mindre avancerade cyberattacker antingen mot betalning eller för att de är så kallade ”patriotiska hackare”.[53] I ett par fall när ryska medborgare har dömts utomlands för cyberbrott, har rysk media kallat det för ”juridisk förföljelse” av ryska medborgare.[54] Det som kanske har fått mest uppmärksamhet är hur Ryssland har använt sig av cyberoperationer i kombination med att läcka stulna data för att diskreditera samt för att så split och polarisera – både inom länder och mellan allierade.

I fallet då GRU stal data från demokratiska partiet i USA distribuerades materialet genom ”Glucifer 2.0”, som uppgav sig vara en rumänsk hackare med ”absolut inga band till den ryska regeringen”. Den amerikanska utredningen som följde kunde dock identifiera vilka två GRU-förband som låg bakom operationen och t o m vilka byggnader i Moskva som den utfördes från.[55] Återigen är det tydligt hur nära cyberoperationer är förknippade med psykologiska operationer i ryskt tänkande. Samma helhetstänkande

har varit tydligt när ryska myndigheter har använt sig av cyberattacker i kombination med läckor av information gentemot egna medborgare, främst medlemmar av den politiska oppositionen, för att underminera deras trovärdighet, skrämma till självcensur eller bara skapa en känsla av obehag.[56]

Rysk cyberstrategi i praktiken

För Ryssland är cyber aldrig en enskild domän utan en del av ett större begrepp som inbegriper alltifrån informationsteknik till psykologiskt försvar och krigföring. Det förklarar varför ordet ”cyber” sällan eller aldrig förekommer i officiella dokument och uttalanden. Det innebär också att cybersäkerhetsåtgärder och cyberoperationer som regel planeras och genomförs inom ramen för en större domän, informationssfären eller informationsrymden som den benämns i ryska doktriner och strategier.

Ryssland har stegvis byggt upp sin förmåga att genomföra relativt avancerade cyberoperationer och det är framför allt FSB och GRU som ansvarar för den verksamheten. Trots att attribueringen av flera cyberoperationer varit mycket övertygande har Rysslands politik konsekvent varit att neka. Det är i och för sig inte unikt för cyberområdet. Bevisningen för att Ryssland ligger bakom såväl förgiftningen av Sergej Skripal i Salisbury 2018 som den av Aleksandr Litvinkenko 2006 har envist ifrågasatts av Ryssland som har lanserat mer eller mindre fantasifulla konkurrerande versioner om vad som hänt. Å ena sidan kan man se detta som att Ryssland använder sig av vilseledande information och därmed undergräver sin egen trovärdighet. Å andra sidan kan man se cyberoperationerna som ett komplext signalerande som pågår framför allt inom underrättelsevärlden. Att Ryssland använt sig av någorlunda begränsade operationer och förnekar sin inblandning ger motståndarsidan fler optioner att svara, där annars ett massivt cyberangrepp skulle tvinga fram ett mer omfattande svar.[57]

Ryssland förnekar således alltid att det blandar sig i andra länders inre angelägenheter, även när det är uppenbart att så har skett. Samtidigt är dess politiska ledning väl medveten om att det som händer i cyberrymden inte per automatik stannar i cyberrymden samt att Ryssland är potentiellt sårbart för motåtgärder. En del av motiveringen 2019 till varför lagändringarna för att uppnå ett suveränt internet var nödvändiga var att Ryssland pekats ut som skyldig till hackerattacker i den amerikanska cybersäkerhetsstrategin. Ryssland behövde således ”vidta skyddsåtgärder för att säkerställa att Internet fungerar långsiktigt och pålitligt”.[58]

Ryssland har sedan den nya Informationssäkerhetsdoktrinen antogs i december 2016 arbetat för att stärka sin egen cybersäkerhet. Framför allt har både tekniska verktyg och processer kommit på plats för att stärka skyddet av landets kritiska informationsinfrastruktur och minska dess beroende av internets globala infrastruktur. Att ersätta import av programvara, komponenter och hårdvara torde däremot fortsatt visa sig mycket besvärligt för Ryssland. Dels har landet redan halkat efter betänkligt, dels gynnar inte rysk ekonomi och företags- och innovationsklimat en dynamisk utveckling av egna IT-industrin. Trots statliga stödprogram kommer det här att vara en av de största utmaningarna för Ryssland framöver.

Och kanske spökar också återigen den ryska definitionen av informationssäkerhet för att hindra att viktiga beslut tas på cybersäkerhetsområdet och utvecklingen av landets IT-industri. Ryssland arbetar aktivt för att göra sin kritiska infrastruktur mindre sårbar för cyberangrepp, men ofta uppfattar landets politiska ledning informationspsy-

kologiska hot som mer allvarliga och akuta. Åtgärder för att öka kontrollen över den egna befolkningen, att ge ryska myndigheter mer befogenheter för att bevaka innehållet och kunna styra trafiken på internet prioriteras som regel framför åtgärder som skulle gynna funktionalitet och dynamisk utveckling av IT-industrin och internetbranschen.

Fram tonar en bild av ett Ryssland som på en gång är både allt skickligare på att genomföra cyberoperationer och alltmer oroad över sin egen säkerhet. För att förstå denna ekvation är det av vikt att vara medveten om ryskt tänkande på området och fortsatt följa de åtgärdsprogram som regeringen antar, hur de implementeras och hur målkonflikter mellan t ex funktionalitet och kontroll löses ut samt vilken del av byråkratin som går segrande ur framtida strider om ansvarsområden och befogenheter på cyberområdet.

Författaren är fil dr, forskningsledare och ledamot av KKrVA.

Noter

1. Artikeln är skriven som en del av KKrVA:s projekt SES för avdelningarna *V och VI*.
2. *Informationssäkerhetsdoktrinen [på ryska], antagen med presidentdekret nr 646,* 2016-12-05, *http://static.kremlin.ru/media/acts/files/0001201612060002.pdf*, (2017-08-11); ”Kontseptualnyje vzgljady na dejatelnost vooruzjennych sil Rossijskoj Federatsii v informatsionnom postranstve”, Ryska federationens försvarsministerium, 2011, *http://ens.mil.ru/science/publications/more.htm?id=10845074@cmsArticle,* (2018-01-19).
3. *Freedom on the Net 2015 – Russia*, *https://freedomhouse.org/report/freedom-net/2014/russia*, (2019-12-11).
4. Soldatov, Andrei och Borogan, Irina: *The Red Web: The Struggle Between Russia's Digital Dictators and the New Online Revolutionaries*, Public Affairs, New York 2015, s 45ff.
5. *Informationssäkerhetsdoktrin* [på ryska], antagen med presidentinstruktion nr 1895, 2000-09-09, *http://www.scrf.gov.ru/Documents/Decree/2000/09-09.html*, (2000-09-15).
6. Granik, Irina och Nagornych, Irina: ”Elektronnaja demokratija vziata pod upravlenije”, *Kommersant*, 2012-07-02, *https://www.kommersant.ru/doc/1971860*, (2019-09-11).
7. Vendil Pallin, Carolina: ”Internet control through ownership: the case of Russia”, *Post-Soviet Affairs*, vol 33, nr 1 2017, s 16-33. Se även Andrei Soldatovs kommentarer i radioprogrammet ”Polnyi Albats”, *Echo Moskvy*, 2019-04-08, *https://echo.msk.ru/programs/albac/2403407-echo*, (2019-04-23).
8. Vendil Pallin, Carolina: *Ryssland nationaliserar internet – lagförslaget om ett ”suveränt internet”*, FOI Memo 6016, 2019-02-27.
9. Kari, Martti: *Russian Strategic Culture in Cyberspace*, JYU Dissertations 122, University of Jyväskylä – Faculty of Information Technology, Jyväskylä 2019, s 90. Se även Galeotti, Mark: *Putin's hydra: Inside Russia's intelligence services*, ECFR Policy Brief, nr 169, maj 2019, *https://docmimic.com/T3iXDXtD1/ecfr-169-putins-hydra-inside-the-russian-intelligence-services-1513.html*, (2018-03-31) och Soldatov, Andrei och Rochlitz, Michael: ”The Siloviki in Russian Politics”, i Treisman, Daniel (red): *The New Autocracy: Information, Politics, and Policy in Putin's Russia*, Brookings Institution Press, Washington DC 2018, s 89-108.
10. Op cit, *Informationssäkerhetsdoktrinen*, se not 2; *Nationella säkerhetsstrategin* [på ryska], antagen med presidentdekret nr 683, 2015-12-31, *http://www.scrf.gov.ru/security/docs/document133/*, (2017-09-26), *Militärdoktrinen* [på ryska], antagen med presidentinstruktion nr 2976, 2014-12-25, *http://www.scrf.gov.ru/security/military/document129/*, (2017-09-26); *Koncept för samhällelig säkerhet* [på ryska], antaget 20 november 2013, http://kremlin.ru/acts/news/19653, (2016-12-07); *Utrikespolitiskt koncept* [på ryska], antaget med presidentdekret nr 640, 30 november 2016,

http://static.kremlin.ru/media/events/files/ru/ZIR5c3NHwMKfbxUqKvNdqKhkA4vf3aTb.pdf, (2017-09-26). Se även Franke, Ulrik: *War by Non-Military Means: Understanding Russian Information Warfare*, FOI-rapport, FOI-R--4065--SE, 2015, s 11-22 samt Hedenskog, Jakob; Persson, Gudrun och Vendil Pallin, Carolina: "Rysk säkerhetspolitik" i Persson, Gudrun (red): *Rysk militär förmåga i ett tioårsperspektiv – 2016*, FOI-rapport, FOI-R--4367--SE 2016, s 98ff.

11. Andra exempel på demokratiska omvälvningar som benämns färgrevolutioner i Ryssland är rosrevolutionen i Georgien 2003 och orangea revolutionen i Ukraina 2004–2005.
12. "Zasedanije Soveta Bezopasnosti", Rysslands presidents hemsida, 2014-10-01, *http://kremlin.ru/events/president/news/46709*, (2017-09-18).
13. Dessa tre brukar framhållas som grundläggande krav för informationssäkerhet, the CIA Triad, se t ex Whyte, Christopher och Mazanec, Brian: *Understanding Cyber Warfare: Politics, Policy and Strategy*, Routledge, London och New York 2019, s 23.
14. Op cit, *Informationssäkerhetsdoktrinen* från 2000, se not 5.
15. Kari, Martti J: *Russian Strategic Culture in Cyberspace*, JYU Dissertations 122, University of Jyväskylä – Faculty of Information Technology, Jyväskylä 2019, s 44ff. För en kritisk analys av denna aspekt av *Informationssäkerhetsdoktrinen* från 2016 op cit och det utkast till lagstiftning om kritisk informationsinfrastruktur som då förelåg, se Demidov, Oleg: "Gosobezopasnost: kak ustrojena novaja strategija borby s kiberugrozami", *RBK*, 2016-12-07, *http://www.rbc.ru/opinions/politics/07/12/2016/5848251b9a79473c64458637*, (2016-12-12).
16. Op cit, *Informationssäkerhetsdoktrinen* från 2016, se not 2, paragraf 23.
17. Op cit, Kari, Martti J, se not 15, s 59-60.
18. Se t ex "Patrusjev rasskazal o roste tjisla chakerskich atakach na gosresursy v 2016 godu", *Interfax*, 2017-03-03, *http://www.interfax.ru/russia/552138*, (2017-09-18) och Tjernenko, Jelena: "Ugrozy informatsionnoj bezopasnosti stanovjatsia vse boleje isosjtjrennymi i massjtabnymi" (intervju med Oleg Chramov), *Kommersant*, 2017-05-22, *https://www.kommersant.ru/doc/3303678*, (2017-08-17).
19. Rozjdestvenskij, Ilja: "'Russkije chakery': ot zaverbovannych prestupnikov do sotrudnikov 'zakrytykh' NII", *Republic*, 2017-12-05, *https://republic.ru/posts/88117*, (2017-12-06).
20. Se t ex Obminska, Ania: "Ryssland har börjat testa sitt självständiga internet", *NyTeknik*, 2019-12-27, *https://www.nyteknik.se/digitalisering/ryssland-har-borjat-testa-sitt-sjalvstandiga-internet-6982850*, (2020-01-08).
21. Op cit,Vendil Pallin, Carolina, 2019, se not 8.
22. "Vstretja s predstaviteljami rossijskich informagenstv i petjatnych SMI", *Prezident Rossii*, 2019-02-20, *http://kremlin.ru/events/president/news/59865*, (2019-03-05).
23. Op cit, *Informationssäkerhetsdoktrinen*, 2016, se not 2, paragraferna 8, 17 och 19. Se även paragraferna 24-27.
24. Pynnöniemi, Katri och Kari, Martti: "Russia's New Information Security Doctrine: Guarding a besieged cyber fortress", *FIIA Comment*, nr 26, 2016, *https://www.fiia.fi/en/publication/russias-new-information-security-doctrine*, (2017-08-17) och Mersjtjerjakova, Anastasija: *Sravnenije Doktrin IB RF 2000 goda v 2016 goda*, Nautjnotechnitjeskij tsentr "Atlas" – Novosibirskij filial, 2016-12-12, *https://atlas-nsk.ru/news/186*, (2017-09-26).
25. "Ryska Federationens digitala ekonomi – program" [på ryska], antagen med regeringsorder nr 1632, 2017-06-28, *http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf*, (2017-09-14).
26. Tomas, Timothy: "Russian Information Warfare Theory: The Consequences of August 2008" i Blank, Stephen J och Weitz, Richard (red): *The Russian military today and tomorrow: Essays in memory of Mary Fitzgerald*, Strategic Studies Institute, US Army War College, Carlisle 2010, *http://ssi.armywarcollege.edu/pdffiles/pub997.pdf*, (2018-01-10), s 269.
27. Kodatjigov, Valerij: "Tjinovniki ne spesjat perechodit na rossijskij soft", *Vedomosti*, 2019-02-01, *https://www.vedomosti.ru/politics/articles/2019/02/01/792990-chinovniki-rossiiskii-soft*, (2019-02-04).
28. Op cit, Vendil Pallin, Carolina, se not 7, s 16-33, Baletskaja, Ksenija: "'Jandeks' vmeste s tjinovnikami pridumal novuju strukturu upravlenija kompaniej", *Vedomosti*, 2019-11-18, *https://www.vedomosti.ru/technology/articles/2019/11/18/816461-yandeks-s-chinovnikami*, (2019-11-18) och *Meduza:* "'Tjtoby nas ne trjaslo'. 'Jandeks' pridumal novuju strukturu upravlenija, kotoraja ustroit gosudarstvo", 2019-11-18, *https://meduza.io/featu-*

re/2019/11/18/chtoby-nas-ne-tryaslo-yandeks-pridumal-novuyu-strukturu-upravleniya-kotoraya-ustroit-gosudarstvo, (2019-11-18).

29. Inför att lagen infördes hade Ryssland genomfört tester av olika leverantörers utrustning för s k djup paketinspektion (*deep packet inspection*, DPI) som kan hitta, identifiera och blockera eller omdirigera datamängder som skickas över internet genom att automatiskt granska både innehåll och adressinformation i paket av data snarare än bara i adressinformationen, op cit, Vendil Pallin, Carolina, se not 8.
30. Op cit, ”Ryska Federationens digitala ekonomi – program”, se not 25.
31. ”Convention on International Information Security”, Ryska Federationens utrikesministerium, 2011-09-22, *http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666*, (2017-03-10).
32. Demidov, Oleg: *Globalnoje upravlenije Internetom i bezopasnost v sfere ispolzovanija IKT*, PIR-PRESS, Moskva 2016 och Nocettti, Julien: ”Contest and Conquest: Russia and Global Internet Governance”, *International Affairs*, vol 91, nr 1 2013, s 111-130.
33. ”Letter Dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General”, FN:s Generalförsamling, A/69/723, 2015-01-13, *https://undocs.org/A/69/723*, (2020-01-14).
34. ”Developments in the Field of Information and Telecommunications in the Context of International Security”, FN:s Generalförsamlings 73:e session, resolutionsutkast, A/C.1/73/L.27.Rev.1, 2018-10-29, *https://undocs.org/A/C.1/73/L.27/Rev.1*, (2020-01-14).
35. ”Countering the Use of Information and Communications Technologies for Criminal Purposes”, FN:s Generalförsamlings 74:e session, resolutionsutkast, A/C.3/74/L.11/Rev.1, 2019-11-05, *https://undocs.org/en/A/C.3/74/L.11/Rev.1*, (2020-01-14).
36. Op cit, *Informationssäkerhetsdoktrinen* från 2000, se not 5.
37. Op cit, *Informationssäkerhetsdoktrinen* från 2016, se not 2.
38. Giles, Keir: *Handbook of Russian Information Warfare*, Fellowship Monograph, Research Division – NATO Defense College, nr 9 2016, *http://www.ndc.nato.int/download/downloads.php?icode=506*, (2020-01-16), s 8. Se även Jonsson, Oscar: *The Russian Understanding of War: Blurring the Lines between War and Peace*, Georgetown University Press, Washington DC 2019, s 105ff och Persson, Gudrun: ”The War of the Future: A Conceptual Framework and Practical Conclusions Essays on Strategic Thought”, *Russian Studies*, NATO Defense College, 03, 2017-07-17, s 5.
39. Op cit, ”Kontseptualnyje vzgljady…”, 2011, se not 2.
40. Op cit, Kari, Martti, se not 9, s 67-68; Ramm, Aleksej och Stepovoj, Bogdan: ”Komanda unitjtozjit: v vojennych okrugach pojavjatsia tsentry kiberzasjtjity”, *Izvestija*, 2019-12-18, *https://iz.ru/950558/aleksei-ramm-bogdan-stepovoi/komanda-unichtozhit-v-voennykh-okrugakh-poiaviatsia-tcentry-kiberzashchity*, (2020-01-20); Zykov, Vladimir och Ramm, Aleksej: ”V Rossii pojavilsia vojennyj internet”, *Izvestija*, 2016-10-19, *https://iz.ru/news/639221*, (2020-01-20); Se även McDermott, Roger N: ”Russia’s Military Undertaking Growing Role in Creation of ‘Sovereign Internet’”, *Eurasia Daily Monitor*, vol 16, nr 48, 2019, *https://jamestown.org/program/russias-military-undertaking-growing-role-in-creation-of-sovereign-internet/*, (2019-05-10).
41. Kosachenko, Aleksej m fl: ”Set sjpionam: v armii sozdajut spetspodrazdelenija antichakerov”, *Izvestija*, 2019-08-08, *https://iz.ru/907124/aleksei-kozachenko-aleksei-ramm-bogdan-stepovoi/set-shpionam-v-armii-sozdaiut-spetcpodrazdeleniia-antikhakerov*, (2020-01-23).
42. ”Stennogramma zasedanii 22 fevralja 2017 g”, Ryska federationens statliga Duma, 2017-02-22, *http://transcript.duma.gov.ru/node/4606/*, (2018-01-04).
43. Kjellén, Jonas: *Russian Electronic Warfare: The Role of Electronic Warfare in the Russian Armed Forces*, FOI-rapport, FOI-R--4625--SE, 2018, s 21-5. Se även McDermott, Roger N: *Russia’s Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum*, ICDS-rapport, Tallinn 2017, *https://www.icds.ee/fileadmin/media/icds.ee/doc/ICDS_Report_Russias_Electronic_Warfare_to_2025.pdf*, (2017-09-18), s 4-5 och op cit Franke, Ulrik, se not 10, s 32ff.
44. Op cit, Franke, Ulrik, se not 10.

45. Jensen, Benjamin; Valeriano, Brandon och Maness, Ryan: ”Fancy Bears and Digital Trolls: Cyber Strategy with a Russian Twist”, *Journal of Strategic Studies*, vol 42, nr 2 2019, s 212-234; Valeriano, Brandon; Jensen, Benjamin och Maness, Ryan C: *Cyber Strategy: The Evolving Character of Power and Coercion*, Oxford University Press, New York 2018, s 18-19 och ”Kibervojny 2017: balans sil v mire”, *Zecurion Analytics*, 2017, *http://www.zecurion.ru/upload/iblock/cb8/cyberarmy_research_2017_fin.pdf*, (2018-03-22).
46. Brantly, Aaron Franklin: ”The Cyber Losers”, *Democracy and Security*, vol 10, nr 2 2014, s 132-155.
47. Rozjdestvenskij, Ilja: ”‘Russkije chakery’: ot zaverbovannych prestupnikov do sotrudnikov ‘zakrytykh’ NII”, *Republic*, 2017-12-05, *https://republic.ru/posts/88117*, (2017-12-06).
48. Buchanan, Ben: *The Legend of Sophistication in Cyber Operations*, Cyber Security Project, Belfer Center – Harvard Kennedy School, 2017, *https://www.belfercenter.org/publication/legend-sophistication-cyber-operations*, (2018-11-05).
49. GRU står ”Huvudunderrättelsedirektoratet” (*Glavnyj razvedovatelnyj upravlenije*). I själva verket har militära underrättelsetjänsten döpts om till bara ”Huvuddirektoratet” (*Glavnoje uprav-lenije*), men såväl rysk som utländsk media benämner det fortfarande oftast som GRU.
50. Alperovitch, Dmitri: ”Bears in the Midst: Intrusion into the Democratic National Committee”, *Crowdstrike*, 2016-06-15, *https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/*, (2018-02-21) och Giles, Keir: ”‘Information Troops’ – A Russian Cyber Command” i Czosseck, Christian; Tõugu, Enn och Wingfield, Thomas (red): *3rd International Conference on Cyber Conflict*, NATO CCD COE Publications, Tallinn 2011, s 51ff. Se även Galeotti, Mark: ”Putin’s Hydra: Inside Russia’s Intelligence Services”, *ECFR Policy Brief*, nr 169 2016, *http://www.ecfr.eu./page/-/ECRF_169_-_PUTINS_HYDRA_INSIDE_THE_RUSSIAN_INTELLIGENCE_SERVICES_1513.pdf*, (2018-03-31) och Soldatov, Andrei och Rochlitz, Michael: ”The Siloviki in Russian Politics”, i Treisman, Daniel (red): *The New Autocracy: Information, Politics, and Policy in Putin’s Russia*, Brookings Institution Press, Washington DC 2018, s 84.
51. Muller, Lilly Pijnenburg; Gjesvik, Lars och Friis, Karsten: *Cyber-weapons in International Politics: Possible Sabotage against the Norwegian Petroleum Sector*, NUPI-rapport, Oslo, nr 3 2018, *http://hdl.handle.net/11250/2486814*, (2018-04-10). Se även Vendil Pallin, Carolina: ”Russian information security and warfare” i Kanet, Roger (red): *Routledge Handbook of Russian Security*, Routledge, Abington och New York 2019, s 210-211.
52. Op cit, Jensen, Benjamin m fl, 2019, se not 45, s 219.
53. Maurer, Tim: *Cyber Mercenaries: The State, Hackers, and Power*, Cambridge University Press, Cambridge 2018, s 94-106. Se även Connell, Michael och Vogler, Sarah: ”Russia’s Approach to Cyber Warfare”, *CNA Occasional Paper*, mars 2017, *https://www.cna.org/cna_files/pdf/DOP-2016-U-014231-1Rev.pdf*, (2019-05-09), s 10-12.
54. ”Sudebnyje presledovanija rossijan za rubezjom”, *TASS* (odaterad sida), *http://tass.ru/sudebnye-presledovaniya-rossiyan-za-rubezhom*, (2018-02-04). Se även Graff, Garrett M: ”How the FBI Took Down Russia’s Spam King – and His Massive Botnet”, *Wired*, 2017-11-04, *https://www.wired.com/2017/04/fbi-took-russias-spam-king-massive-botnet*, (2018-02-04).
55. *Deputy Attorney General Rod J. Rosenstein Delivers Remarks Announcing the Indictment of Twelve Russian Intelligence Officers for Conspiring to Interfere in the 2016 Presidential Election Through Computer Hacking and Related Offenses*, U.S. Department of Justice, 2018-07-13, *https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-announcing-indictment-twelve*, (2018-07-16).
56. Op cit, Soldatov, Andrei och Borogan, Irina, se not 4, s 19-20; Bradshaw, Samantha och Howard, Philip N: ”The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation”, *Project on Computational Propaganda*, Working paper 2019.2, University of Oxford, *https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/09/CyberTroop-Report19.pdf*, (2019-09-30).
57. För en bra diskussion kring detta, se t ex op cit, Jensen, Benjamin m fl, 2019, se not 45, s 230ff och Bartles, Charles K: ”Russia’s Indirect and Asymmetric Methods as a Response to the New Western Way of War”, *Special Operations Journal*, nr 1 2016, s 6.
58. Lagförslaget citeras i op cit, Vendil Pallin, Carolina, se not 8, s 3.