Nyckelaktörerna för rysk cybersstrategi: 2000–2020

Carolina Vendil Pallin

FOI-R--5025--SE

Oktober 2020

Carolina Vendil Pallin

Nyckelaktörerna för rysk cybersstrategi: 2000–2020

Titel	Nyckelaktörerna för rysk cybersstrategi: 2000–2020
Title	Key Actors in Russian Cyber Strategy: 2000–2020
Rapportnr	FOI-R--5025--SE
Månad	Oktober
Utgivningsår	2020
Antal sidor	100
ISSN	1650-1942
Kund	Försvarsdepartementet
Forskningsområde	Säkerhetspolitik
FoT-område	Inget FoT-område
Projektnr	A112001
Godkänd av	Malek Finn Khan
Ansvarig avdelning	Försvarsanalys

Bild/Cover: ITAR-TASS, Alexei Nikolskyi

Detta verk är skyddat enligt lagen (1960:729) om upphovsrätt till litterära och konstnärliga verk, vilket bl.a. innebär att citering är tillåten i enlighet med vad som anges i 22 § i nämnd lag. För att använda verket på ett sätt som inte medges direkt av svensk lag krävs särskild överenskommelse.

This work is protected by the Swedish Act on Copyright in Literary and Artistic Works (1960:729). Citation is permitted in accordance with article 22 in said act. Any form of use that goes beyond what is permitted by Swedish copyright law, requires the written permission of FOI.

Sammanfattning

Ett antal viktiga brytpunkter är tydliga vid en analys av hur rysk cyberstrategi har formulerats och implementerats under perioden 2000–2020. Det är tidpunkter då landets politiska ledning har tvingats göra avdömningar för att justera landets strategi men också för att koordinera och sätta byråkratin i rörelse för att verkställa fattade beslut.

Ett antal aktörer inom det ryska politiska systemet, främst den Federala säkerhetstjänsten och Säkerhetsrådets kansli, var tidigt aktiva vad gäller att beskriva internet som ett hot samt att betona behovet av mer statlig kontroll och minskat beroende av utländsk teknologi. Ryssland fick en Informationssäkerhetsdoktrin redan 2000 som innehöll dessa målsättningar, men få kraftfulla och samordnade åtgärder vidtogs före 2011. Efter dess inskränktes friheten på internet i landet gradvis och från och med 2014 accelererade denna utveckling i takt med att alltfler i det politiska systemet accepterade den hotbild som ursprungligen främst säkerhetstjänster framhöll.

Denna studie identifierar, förutom de krafter som har varit drivande för mer kontroll, också de krafter som har verkar återhållande och företrätt andra målsättningar på cyberområdet, som t.ex. delar av näringslivet och internetanvändare. Även externa krafter i form av t.ex. den internationella teknologiutvecklingen har tvingat regeringen att omformulera eller justera sina målsättningar.

Nyckelord: Ryssland, cyber, strategi, doktrin, Putin, beslutsfattande, säkerhetspolitik, internet

Summary

An analysis of how Russia has formulated and implemented its cyber strategy 2000–2020 makes it possible to identify critical moments, when the country's political leadership adjusted this strategy as well as coordinated and put the bureaucracy in motion.

A number of actors in the Russian political system, especially the Federal Security Service and the Security Council apparatus, described the internet as a threat from the very beginning and called for more state control and reduced dependency on import of foreign technology. Many of these tenets were present in the Information Securty Doctrine in 2000, but Russia was slow in coordinating policy. Many key measures were delayed or proved impossible to implement. However, from 2011 freedom on the internet became increasingly circumscribed. From 2014, this development gathered speed as actors inside the political system accepted the notion that information technology and the information it carried could constitute a national security threat.

Apart from the forces that argued in favour of increased control and security measures, this study identifies a number of actors, such as domestic internet users, that championed another policy It also discusses other external forces, for example international technology development, that has forced the government to calibrate its cyber strategy.

Keywords: Russia, cyber, strategy, doctrine, Putin, decision making, security policy, internet

Förord

Denna studie fokuserar på ryska aktörer som är delaktiga i att forma och genomföra rysk cyberstrategi. Den ingår i ett större arbete med att studera rysk cybersäkerhet och cyberoperationer som en del av studierna inom Rysslandsprojektet vid FOI.

Rapporten ventilerades vid ett mindre seminarium över videolänk den 1 april 2020. Professor Bo Petersson var extern granskare och fil.dr. Johan Engvall var seminarieordförande. Deras kommentarer, kritik och uppmuntran har varit värdefullt i arbetet med att färdigställa rapporten. Dessutom har kollegor på FOI lämnat utmärkta synpunkter på förstautkastet, bland dem kan särskilt nämnas Jakob Hedenskog, docent Gudrun Persson och Erik Zouave.

I denna studie står beslutsfattande och vilka aktörer som har varit tongivande i fokus. Studien ansluter till och bygger på tidigare FOI-studier, artiklar och bokkapitel om rysk cyberstrategi, t.ex. om rysk politik och internetutveckling (Franke och Vendil Pallin 2012), om rysk informationskrigföring (Franke 2015), om hur kontrollen över internet ökat genom statligt ägande eller genom personer som står den politiska makten nära (Vendil Pallin 2017a), om innehållet i Informationssäkerhetsdoktrinen från 2016 (Vendil Pallin 2018b), om lagen som syftar till att skapa ett suveränt internet (Vendil Pallin 2019b) och översikter om rysk cyberstrategi (Vendil Pallin 2019a; 2020).

Johan Norberg
Projektledare för Rysk utrikes-, försvars- och säkerhetspolitik (RUFS)
FOI, Kista, den 31 augusti 2020

Rapporten i korthet

Rysk cyberstrategi är ett resultat av en stor mängd aktörers tankearbete och planer, även om det ibland kan tyckas bara vara ett fåtal. En strategi behövs när hinder och svårigheter ska övervinnas. Den kan därmed analyseras i termer av olika krafter som påverkar dess innehåll, realiserar dess målsättningar eller förhindrar processen genom inaktivitet, konkurrerande målsättningar eller motstånd. En analys av vilka aktörer som formar, implementerar och på andra sätt påverkar rysk cyberstrategi förklarar strategins målsättningar och hur dessa har utvecklats över tid. Analysen visar varför regeringen vidtar vissa konkreta åtgärder vid en viss tidpunkt, men också varför vissa mål är svårare än andra att förverkliga.

Denna studie undersöker vilka som är de viktiga aktörerna för rysk cyberstrategi men också hur den omgivande miljön påverkar utformningen och implementeringen av strategin. Den identifierar brytpunkter där cyberstrategin har anpassats och hur olika aktörers inflytande har ändrats över tid.

Studiens analytiska ramverk fokuserar på framväxten av strategier och hur olika krafter påverkar processen. För det första dömer en ledning av strategin vid vissa brytpunkter, som identifieras i studien. För det andra är organisatoriska krafter (landets byråkrati i vid mening) drivande i såväl strategiformulering som implementering. Dessutom påverkar, för det tredje, externa krafter genom att tillsammans utgöra den miljö i vilket rysk cyberstrategi formuleras och genomförs. Enligt denna modell är krafterna som formar rysk cyberstrategi:

- Rysslands politiska ledning, i vilken presidenten spelar en central roll, men också landets Säkerhetsråd och andra delar av Presidentadministrationen;
- organisatoriska krafter som omfattar byråkratin i form av ministerier och myndigheter, men också parlamentet, delar av näringslivet och samhällsorganisationer som står regeringen nära;
- samt externa krafter såväl inom Ryssland i form av t.ex. samhällsorganisationer, folkopinion och potentiellt politiskt motstånd, som utanför landet i form av bland annat globala internetföretag, internationell teknologisk utveckling och internationella ramverk.

Studien identifierar kritiska skeden, brytpunkter, där rysk cyberstrategi delvis formulerats om eller där uppsatta mål faktiskt också realiseras och gör det möjligt att dela in åren 2000–2020 i perioder. För samtliga perioder analyseras nyckelområden inom rysk cyberstrategi som skydd av kritisk rysk informationsinfrastruktur; åtgärder för att minska Rysslands beroende av import; ökad kontroll över internetanvändare; Rysslands agerande för att få gensvar för sin syn på cybersäkerhet internationellt; och förekomsten av ryska cyberoperationer.

Under den första perioden, 2000–2011/2012 förespråkade Säkerhetsrådet kansli och landets underrättelse- och säkerhetstjänster mer kontroll. Samtidigt hade

landet en dynamisk internetsektor som t.ex. utvecklade unika applikationer för den ryska marknaden. Friheten på internet var också betydande. Under denna inledande period tycks den högsta politiska ledningen ägnat relativt lite uppmärksamhet åt cyberfrågor.

Under den andra perioden, 2011–2013, blev cyberfrågor en allt viktigare fråga för Presidentadministrationen och den politiska ledningen började se information på internet som en potentiell källa till politisk instabilitet. Regeringen vidtog åtgärder för att öka kontrollen och övervakningen genom blockering av webbplatser och övervakning av sociala medier. Detta är också perioden då Ryssland lanserar ett förslag till internationellt avtal om informationssäkerhet med fokus på regeringars rätt att kontrollera innehåll inom sin internetsfär.

Annekteringen av Krim 2014 påverkade direkt rysk cyberstrategi och är startpunkten för en tredje period. Säkerhetsrådets och Federala säkerhetstjänstens (FSB:s) syn på cyber och internet blev alltmer allmänt accepterad inom det politiska systemet och i samhället i stort. Ett möte i Säkerhetsrådet den 1 oktober 2014 blev en signal om att den politiska ledningen förväntade sig att målsättningarna omsattes i handling. En ny Informationssäkerhetsdoktrin kom 2016. Snart följde även formella dokument, handlingsplaner och lagar, som en lag om skydd av kritisk informationsinfrastruktur. Kontrollen över det som definierades som ett ryskt ”suveränt” internet ökade också markant och Ryssland lyckades vinna visst stöd för sin syn på informationssäkerhet internationellt. Det hårdnande klimatet fick dock negativa konsekvenser för andra delar av strategin. När en målkonflikt uppstod, t.ex. mellan målet att stimulera en rysk internetindustri och målet att öka statens kontroll över industrin vann som regel kontrollivrarna efter 2014. Under den tredje perioden stod det klart att Ryssland hade byggt upp en förmåga att genomföra cyberoperationer. Denna cyberförmåga var en del av strategin, något som den politiska ledningen varken kommunicerat öppet eller ens erkänt att den existerade.

Nästa period kommer att präglas av dels pandemin 2020 och dess efterverkningar, dels det teknikskifte som äger rum på cyberområdet. Båda dessa externa krafter kan påskynda trender och intensifiera tendenser som redan varit tydliga. Övervakning och möjligheter att kontrollera trafikflöden och innehåll tycks öka. Eventuellt kommer internet alltmer att splittras globalt, med olika regionala internetsfärer som domineras av länder som Kina respektive USA. Kinas växande roll internationellt kommer att ha konkreta konsekvenser för utformningen av rysk cyberstrategi även framöver. Vilka aktörer inom Rysslands politiska system som framöver får mest inflytande kommer att fortsatt bestämma hur landet väljer att möta utmaningar och dra nytta av de möjligheter som uppstår på cyberområdet.

Innehållsförteckning

Förkortningar

5G	femte generationens mobila nätverk för dataöverföring
AI	artificiell intelligens
ANO	autonom, icke-kommersiell organisation *avtonomnaja nekommertjeskaja organizatsija*
APKIT	Föreningen för data- och IT-företag *Assotsiatsija predprijatij kompjuternych i informatsionnych technologij*
BRICS	Brasilien, Ryssland, Indien, Kina och Sydafrika
CERT	*computer emergency response team*
CFR	*Council on Foreign Relations*
CSIS	*Center for Strategic and International Studies*
CSTO	*Collective Security Treaty Organization*
DNS	domännamnsystem *domain name system*
EU	Europeiska unionen
FAPSI	Federala agenturen för regeringskommunikationer och information *Federalnoje agenstvo pravitelstvennoj svjazi i informatsii pri prezidente*
FN	Förenta nationerna
FRII	Utvecklingsfonden för internetinitiativ *Fond razvitija internet-initiativ*
FSB	Federala säkerhetstjänsten *Federalnaja sluzjba bezopasnosti*
FSO	Federala skyddstjänsten *Federalnaja sluzjba ochrany*
FSTEK	Federala tjänsten för teknisk och exportkontroll *Federalnaja sluzjba po technitjeskomu i eksportnomu kontrolju*
GONGO	*government-operated non-governmental organization*
GosSOPKA	Statligt system för att upptäcka, förhindra och oskadliggöra konsekvenser av datorattacker *Gosudarstvennaja Sistema obnaruzjenija, predotvrasjtjenija i likvidatsii posledstvij kompjuternych atak*
GRU	Generalstabens Huvuddirektorat för underrättelser

	Glavnoje razvedyvatelnoje upravlenije
GUSP	Huvuddirektoratet för särskilda program *Glavnoje upravlenije spetsialnych programm*
ICT	informations- och kommunikationsteknologi *information and communication technology*
IP	Internetprotokoll
IRI	Institutet för internetutveckling *Institut razvitija interneta*
IRR	*internet routing registry*
IT	informationsteknologi
Minkomsvjaz	Ministeriet för digital utveckling, samband och masskommunikation *Ministerstvo tsifrovogo razvitija, svjazi i massovych kommunikatsij* (tidigare Ministeriet för samband och masskommunikation *Ministerstvo svjazi i massovych kommunikatsij*)
MKS	Media-Kommunikationsförbundet *Medija-kommunikatsionnyj sojuz*
MVD	Inrikesministeriet *Ministerstvo vnutrennych del*
Nasdaq	*National Association of Securities Dealers Automated Quotations*
NGO	*non-governmental organization*
NII	vetenskapligt forskningsinstitut *nautjno-issledovatelskij institut*
NKTsKI	Nationellt koordineringscentrum för datorincidenter, CERT.GOV.RU *Natsionalnyj koordinatsionnyj tsentr po kompjuternym intsidentam*
NSA	*National Security Agency*
Osse	Organisationen för säkerhet och samarbete i Europa
OZI	Sällskapet för att skydda internet *Obsjtjestvo zasjtjity interneta*
RAEK	Föreningen för elektronisk kommunikation *Assotsiatsija elektronnych kommunikatsii* *The Russian Association for Electronic Communications* (RAEC)

Förbundet RATEK	Föreningen för handelsföretag och tillverkare av elektriska hushålls- och datorutrustning *Assotsiatsija torgovych kompanij i tovaroproizvoditelej elektrobytovoj i kompjuternoj techniki*
ROTsIT	Regionalt samhällscentret för internetteknologi *Regionalnyj obsjtjestvennyj tsentr internet teknologij*
SCO	*Shanghai Cooperation Organization*
SORM	System for operativa förundersökningsåtgärder (*Sistema technitjeskich sredstv dlja obespetjenije funktsij operativno-rozysknych meroprijatij*)
TOR	*The Onion Router*
VPN	virtuellt privat nätverk
WADA	*World Anti-Doping Agency*

1 Inledning

En bit in i sitt årliga linjetal till parlamentet i januari 2020 släppte Vladimir Putin något av en bomb: konstitutionen skulle ändras på en rad punkter. Åhörarna i Centrala utställningssalen på Manegetorget vaknade till. Det var omöjligt att i detalj förstå hur den politiska makten i landet skulle fördelas utifrån talet. Putin skulle av allt att döma ha kvar en dominerande ställning, men hur skulle resten av makten omfördelas? Vad skulle det här innebära för åhörarnas egen institution i systemet och för dem personligen?

Även i ett politiskt system där en person dominerar är andra aktörer viktiga. Fördelningen av makt, resurser, befogenheter och skyldigheter mellan dessa är inte bara ett spel för gallerierna. Reaktionerna på Putins linjetal 2020 speglar väl detta förhållande. Hur det politiska systemet utformas, hur beslutsgången ändras och resurser och makt fördelas får konsekvenser både för de som befinner sig i systemet, för vilken politik som blir resultatet och för samhället i stort.

Hur beslutsfattande sker har stor inverkan även på enskilda politikområden. Den övergripande frågeställningen i denna studie är vilka aktörer som har varit tongivande i att utforma rysk cyberstrategi. Genom att studera vilka krafter inom byråkratin som har det tyngst vägande ordet inom detta område är det möjligt att se hur maktbalansen förändrats över tid. Det finns också ett antal viktiga brytpunkter i hur rysk cyberstrategi har formats och implementerats.

1.1 Frågeställningar

Tidigare studier av aktörer inom rysk cyberstrategi har tenderat att fokusera på ett fåtal huvudaktörer som Federala säkerhetstjänsten (FSB), Federala tjänsten för teknisk och exportkontroll (FSTEK) (se t.ex. Tomas 1998). Ofta nämns också Ministeriet för digital utveckling (*Minkomsvjaz*)[1] och dess myndighet Federala tjänsten för övervakning av kommunikationer, informationsteknologi och massmedia (*Roskomnadzor*). Som kommer att framgå av denna studie är framför allt FSB och Säkerhetsrådets kansli (*apparat*) viktiga aktörer, men deras inflytande har varierat över tid och vilket genomslag deras målsättningar får är en funktion av beslut som landets högsta politiska ledning tar.

Denna studie undersöker således vilka som är de viktiga aktörerna för rysk cyberstrategi i det ryska politiska systemet, hur de relaterar till varandra och hur deras tyngd i systemet har ändrats över tid. Vidare formas Rysslands cyberstrategi inte i

[1] Hela namnet är Ministeriet för digital utveckling, samband och masskommunikation. Namnet är långt och ändrades dessutom 2018 – tidigare var namnet Ministeriet för samband och masskommunikation. Därför hänvisas till detta ministerium antingen som Minkomsvjaz eller som Ministeriet för digital utveckling, när perioden efter 2018 beskrivs, i enlighet med hur det oftast benämns i rysk media. För en utförligare beskrivning av ministeriet (Minkomsvjaz) och dess myndighet Roskomnadzor, se s. 64.

ett vakuum utan ett antal externa krafter utgör tillsammans den miljö i vilken den formas och utvecklas.

Frågeställningarna är:

- *Vilka brytpunkter kan identifieras där en anpassning av cyberstrategin har ägt rum?*
- *Vilka aktörer (organisatoriska krafter) deltar i formandet av rysk cyberstrategi och hur påverkar externa krafter strategin?*

1.2 Definitionen av ”rysk cyber” och källor

Rysk cyberstrategi kan tolkas både som avgränsad till att endast handla om militär cyberstrategi och som väsentligt bredare till att omfatta alltifrån cybersäkerhet till hur staten finansierar bredbandstillgång i mindre befolkningstäta regioner. I denna studie ligger fokus på cyberstrategi i säkerhetspolitisk bemärkelse; således bredare än bara militärt men smalare än det som snarare kan beskrivas som Rysslands politik på det digitala området.

En betydande del av Rysslands politik på cyberområdet finns formulerad i en rad dokument där Informationssäkerhetsdoktrinen – den senaste antogs i december 2016 – spelar en central roll. Ordet ”cyber” nämns dock sällan eller aldrig i ryska dokument och officiella uttalanden. I ryskt tänkande är ”cyber” en del av en större enhet kallad ”information” där allt ifrån telekrig och hackerattacker till propaganda och vilseledning ingår. Så långt finns likheter med hur termerna används i t.ex. USA. I Ryssland är cyberaspekter en delmängd av informationssäkerhet och informationskrigföring. Cyberoperationer är som regel en integrerad del av en större informationsoperation. Det finns ingen ”cyberportfölj” eller cyberdomän i det ryska tänkandet utan snarare en större informationsdomän där en kamp pågår även när inget krig har inletts (Giles 2016: 8; Jonsson 2019: 105ff; Persson 2017: 5). Däremot skiljer ryska författare inom området på teknisk informationskrigföring (eller informationskonfrontation, *informatsionnoje protivoborstvo*) och psykologisk sådan (Konceptuell syn på Ryska federationens Väpnade styrkors verksamhet i informationsrymden 2011; se även t.ex. Lilly & Cheravitch 2020: 132–5; Kari 2019: 16).

Här studeras således främst det man i rysk litteratur om informationssäkerhet och informationskrigföring skulle kalla teknisk sådan. Samtidigt är det omöjligt att förstå ryskt tänkande utan att ständigt minnas hur nära förknippad den är med den psykologiska informationssäkerheten och informationskrigföringen. Därmed ingår även ökad kontroll över informationsflöden, men då främst cyberbaserade sådana, i analysen.

Den officiella politiken på cybersäkerhetsområdet finns främst tillgänglig i Informationssäkerhetdoktrinen och andra strategiska dokument (för en genomgång av hur de olika strategiska dokumenten behandlar detta, se Vendil Pallin 2018b).

Dessutom finns ryska regeringsprogram som beskriver mer i detalj hur de uppsatta målen ska uppnås och när. Ett av de viktigaste dokumenten på det området är programmet ”Digital ekonomi” (2017) där en viktig del är digital säkerhet. Officiella dokument som förekommer ofta i texten liksom även federala lagar refereras till i svensk översättning för att spara utrymme i texten.[2]

Dessutom formar officiella uttalanden, tal och pressmeddelanden på hög nivå rysk cyberstrategi och beslutsfattande på området finns beskrivet i lagar och förordningar för de olika ministerierna och myndigheterna. Rapporteringen i rysk media, som t.ex. dagstidningarna *RBK*, *Vedomosti* och *Kommersant* samt nyhetsbyrån *Meduza* kompletterar källmaterialet för att förstå hur beslutsfattande sker, vilka överväganden som styr ryska företag och den roll som parlamentet spelar – vilket inte är den roll i maktdelningen som beskrivs i konstitutionen (Vendil Pallin 2018a). Att följa hur ett enskilt ärende vandrar i ministerier och parlament i form av remissvar och uttalanden samt hur myndigheter och statliga företag verkställer, eller inte verkställer, fattade beslut ger viktiga ledtrådar om aktörernas roll och relativa makt inom cyberområdet (Vendil Pallin 2019b).

Den offensiva delen av rysk cyberpolitik redovisas inte i öppna ryska policydokument. Den ryska officiella politiska linjen är tvärtom att landet aldrig blandar sig i andra länders inre angelägenheter. Icke desto mindre finns goda grunder för att anta att Ryssland har en handlingsplan för att utveckla även sin offensiva cyberförmåga. En rad länder har attribuerat cyberoperationer antingen som utförda från ryskt territorium, som regel från Moskva, eller t.o.m. som utförda av ryska underrättelse- och säkerhetstjänster (Vendil Pallin 2019a). Attribuering sker som regel baserat på en rad indikatorer och är en tidskrävande process (Karlzén 2019: 27ff). Ryssland har ihärdigt förnekat delaktighet i samtliga fall där landet har blivit utpekat. Det ligger i sakens natur att beslutsfattande på detta område är svårare att kartlägga – i Ryssland liksom i andra länder. Därmed är det framför allt sekundärkällor som finns tillgängliga på detta område. Till exempel har den amerikanska databasen ”Cyber Operations Tracker” som byggts upp av *Council on Foreign Relations* (CFR) använts för att översiktlig beskriva vilka cyberoperationer som Ryssland har legat bakom – direkt eller genom så kallade *proxies*. CFR:s databas innehåller cyberoperationer där en nation är aktör (*state sponsor*) och bygger i sin tur på databaser från bland andra *Center for Strategic and International Studies* (CSIS) och *Kaspersky Lab* (se även mer om Kaspersky Lab s. 64, 70). Dessutom har t.ex. amerikanska myndigheter pekat ut ryska officerare inom militära underrättelsetjänsten (*Glavnoje razvedyvatelnoje upravlenije*, GRU)[3] som ansvariga för

[2] I litteraturlistan redovisas de därför separat inledningsvis och i svensk översättning snarare än med ryska originaltitlar.

[3] *Glavnoje razvedyvatelnoje upravlenije* översätts ”Huvudunderrättelsedirektoratet”. GRU döptes om till bara ”Huvuddirektoratet” (*Glavnoje upravlenije*) 2010, men såväl rysk som utländsk media benämner det fortfarande oftast som GRU och därför har den benämningen använts även i denna rapport.

konkreta cyberoperationer och estniska underrättelsetjänsten uppger i sin årsrapport vilka myndigheter som ligger bakom cyberattacker.

Såväl säkerhetsfirmor som specialiserar sig på informationsteknologi (IT), tankesmedjor som länders myndigheter och underrättelsetjänster kan ha skäl för att peka ut ett enskilt land. Det kan vara kommersiellt lukrativt; vid en given tidpunkt kan det vara lättare för tankesmedjor att få anslag för vissa studier; utpekande av enskilda länder kan vara en del i ett diplomatiskt spel eller en del i en förhandling. Med tanke på samtliga dessa invändningar är det viktigt att det finns mer än en källa för attribuering av ryska cyberoperationer och att de är så långt möjligt sinsemellan oberoende. Där ryska cyberoperationer diskuteras i studien har således endast de operationer där det finns bra underlag för utpekande tagits med. För denna studies ändamål är inte det absoluta antalet operationer det viktiga; snarare är tendensen till ökad förmåga av intresse liksom även konsekvenserna av att Ryssland ses av andra länder som en stat som ägnar sig åt cyberoperationer.

1.3 Studiens upplägg

Kapitel 2 beskriver ett analytiskt ramverk för att analysera framväxten av en rysk cyberstrategi som inte är låst till att endast studera befintliga dokument. Eftersom frågeställningarna fokuserar på aktörers roller och på krafter inom det politiska systemet, använder sig denna studie av dels teorier om organisationers och byråkratiers roll i utformningen av politik och strategi, dels av en modell som sätter framväxten av strategier och aktörskrafter i centrum. Modellen lyfter också fram vikten av att en ledning dömer av, anpassar eller helt ändrar strategin vid kritiska skeden. Kapitlet presenterar slutligen översiktligt externa krafter som kan inverka på hur rysk cyberstrategi formuleras och genomförs (eller inte kan genomföras).

Kapitel 3 föreslår en indelning i perioder för formandet av rysk cyberstrategi under perioden 2000–2020. Identifierade kritiska skeden där strategin delvis formulerats om eller där uppsatta mål faktiskt också realiseras blir brytpunkter för de olika faserna. För samtliga perioder lyfts följande frågor fram:

- skydd av kritisk rysk informationsinfrastruktur;
- åtgärder för att minska Rysslands beroende av import;
- ökad kontroll över internetanvändare och företag;
- Rysslands agerande för att få gensvar för sin syn på cybersäkerhet internationellt;
- förekomsten av ryska cyberoperationer;
- vilka externa krafter som varit drivande;
- organisatoriska krafter inom byråkratin.

Ryssland har betydande resurser och dess cyberstrategi griper igenom snart sagt varje politikområde. Att gå igenom varje skede, varje företags agerande och varje lagförslags vandring genom byråkratin skulle ha resulterat i omfattande text och riskerat att skymma huvudbudskapet. Genomgången är därmed schematisk snarare än uttömmande.

Kapitel 4 utgör något av en katalog över viktiga institutioner i Ryssland på cyber-området uppdelat i centrala aktörer respektive mer perifera sådana i det politiska systemet och baseras på genomgången i kapitel 3. Kapitlet analyserar de viktigaste aktörerna inom den ryska regeringen, byråkratin och dess förlängda armar i form av t.ex. regeringsstyrda organisationer, parlamentsledamöter och statliga företag samt hur deras roll skiftar under de olika perioderna.

Kapitel 5 består av övergripande slutsatser utifrån studien som helhet. Dessutom föreslår kapitlet ytterligare områden för fördjupade studier om rysk cyberstrategi.

2 Analytiskt ramverk

Ordet strategi har kommit att användas så ofta att det i viss mån har urholkats, men när ett land formulerar en strategi är det som regel fråga om långsiktiga mål och berör något som är centralt för landet i fråga; det rör sig om att ”se skogen snarare än träden” (Freedman 2013: ix). En plan eller vägkarta för att nå utstakade mål behövs onekligen, men en strategi är mer än en plan. En strategi krävs när det finns hinder på vägen som ska övervinnas, andra aktörer som ska förmås att ändra sitt agerande (Freedman 2013: xi) och innehåller t.ex. idéer om hur resurser ska användas offensivt och defensivt och vilka allianser som är gynnsamma. Den kan förespråka avskräckning eller vilseledning och list (Freedman 2013: 9, 23; Posen 1984: 15–18). Utanför det beslutsfattande systemet finns en extern miljö som ibland är gynnsam för strategin, ibland motarbetar den – en omgivande miljö som tvingar fram omvärderingar och sätter gränser (Mintzberg & Walters 1985: 269).

Schematiskt skulle man kunna tänka sig en modell där strategi formuleras enligt principen att landets ledning bestämmer huvudinriktningen och att en byråkrati bryter ned strategin i konkreta planer och implementerar dessa. Henry Mintzberg (1994: 334ff) har dock övertygande visat att en sådan modell för strategigenerering bara existerar i teorin. Det som brukar benämnas ”strategisk planering” tenderar att ha mer att göra med att ”programmera” en centraliserad institution, enligt Mintzberg. Han menar också på att denna programmering oftast begränsar sig till att vara förknippad med budgetprocessen för att realisera en given strategi (1994: 78–81).

Ledningen för en organisation eller ett land måste ha gett en strategi sitt godkännande för att resten av systemet ska se den som giltig och värd att ägna kraft och möda att genomföra. Samtidigt innebär inte det att ledningen måste formulera strategin i sin helhet; betydande element i den kan ha formulerats på gräsrotsnivå eller mellannivå i organisationen och sedan sipprat uppåt. En strategi behöver inte heller vara ett skrivet dokument för att existera, men målsättningarna bör kommuniceras åtminstone till organisationen som ska förverkliga den, ofta också till motståndare och allierade, för att den ska få önskad effekt. Det kan ske i termer av både ord och praktiskt agerande (Freedman 2013: 23). Exakt hur en strategi avser att kombinera åtgärder och verktyg för att nå dessa målsättningar kan dock vara information som endast vissa nyckelaktörer får ta del av. I Rysslands fall är Informationssäkerhetsdoktrinen (2016) en god utgångspunkt för att förstå vilka beståndsdelar som ingår i landets defensiva cyberstrategi, men det är samtidigt tydligt utifrån landets agerande att det även finns en offensiv del av strategin, att landet har utvecklat en förmåga att genomföra cyberoperationer.

2.1 Ledning och organisatoriska krafter

I sin bok *The Essence of Decision* föreslog Graham Allison (1971) att hur beslut fattas kan analyseras enligt tre olika modeller: rationella aktörsmodellen (*rational actor model*); organisationers beteenden (*organizational behavior*); och förhandlingspolitik på regeringsnivå (*governmental politics*). Hans slutsats var att beroende på vilken modell analytikern väljer kommer olika frågor att stå i centrum och svaren kommer att se delvis olika ut (se även Allison & Zelikow 1999; Halperin, Clapp & Kanter 2006).

Den rationella aktörsmodellen skulle innebära att vi frågade varför Rysslands regering valde att genomföra en cyberoperation, givet olika alternativa beslut och svaret skulle handla om att alternativet som valet föll på maximerade nyttan och minimerade kostnaderna. Den modell som fokuserar på organisationers beteende skulle snarare hitta svaret i t.ex. FSB:s organisationskultur och standardiserade processer inom organisationen. En modell som försöker hitta förklaringen i förhandlingspolitik på regeringsnivå kommer att tolka Rysslands agerande som ett resultat av en förhandling eller ett ”spel” mellan t.ex. FSB och Utrikesministeriet.

Det finns mycket som talar för att använda flera perspektiv för att förstå hur rysk cyberstrategi formas – inte minst då den spänner över såväl inrikes- som utrikespolitik. Till exempel är bristen på framgång vad gäller att bryta Rysslands importberoende på cyberområdet svår att förklara som ett rationellt val av den ryska regeringen, men det är också svårt att förstå varför kontroll och övervakning av internet accelererade efter 2014 utan att klättra upp i analysnivån och diskutera hur Rysslands regering såg på landets position internationellt.

Barry R. Posen (1984) bygger vidare på hur man kan använda olika perspektiv för att förstå beslutsfattande och föreslår i en analys av hur beslut fattades i mellankrigstiden att olika analytiska ramverk kan användas för att förklara olika skeden i beslutsfattande. Hans slutsats blir att förhandlingspolitik tenderar att dominera så länge som inte en fråga ställs på sin spets. När en landets ledning uppfattar att vitala värden står på spel, emellertid, tenderar rationella aktörsmodellen att bättre förklara hur beslutsfattande sker (Posen 1984: 60). Hans slutsats är också väl i linje med Allisons och Halperins (1972: 58) bedömning av när rationella aktören (Model I) är mer användbar och när byråkratiska processer och maktkamper dominerar:

> In general, Model I is more useful in explaining actions where national security interests dominate, where shared values lead to a consensus on what the national security requires, and where actions flow rather directly from decisions. The bureaucratic politics model is more useful where there is data on the interests of players and the rules of the game, where organizational and domestic interests predominate or where one wishes to treat the details of action.

I den genomgång av olika skeden av beslutsfattande om rysk cyberstrategi som följer har dessa olika analysmodeller varit en inspiration för att välja ett teoretiskt

ramverk. Dels ska den analytiska modellen identifiera tillfällen då den politiska ledningen har sett sig föranledd att gripa in och fatta avgörande beslut, att ändra inriktningen på strategin. Dels ska modellen tillåta en analys av hur strategin växer fram gradvis mellan dessa avdömningar av den politiska ledningen. Henry Mintzberg (1978: 947) beskriver strategiformulering som en process där lärande och anpassning spelar en betydande roll:

> A strategy is not a fixed plan, nor does it change systematically at pre-arranged times solely at the will of the management. The dichotomy between strategy formulation and strategy implementation is a false one under certain common conditions, because it ignores the learning that must often follow the conception of an intended strategy.

Mintzberg (1978) har föreslagit en modell för att analysera strategiers utveckling inom företag och politiskt beslutsfattande som lägger tyngdpunkt på att se strategi som en dynamisk process snarare än ett statiskt dokument eller en plan. Enligt hans analytiska ramverk finns en avsiktlig strategi (*intended strategy*). Om den sedan realiseras så blir det Rysslands förverkligade strategi enligt en rak process (*deliberate strategy*). Det mest vanliga och troliga är dock att delar av den avsiktliga strategin inte kommer att genomföras, samtidigt som element tillkommer under resans gång (*emergent strategy*). Han delar också in de krafter som påverkar strategin i (1) en ledning, (2) organisatoriska krafter, och (3) externa krafter (Mintzberg 1978: 941).

Landets ledning dikterar således inte en strategi uppifrån – inte ens i Ryssland som ofta beskrivs som ett system där presidenten bestämmer och där Putinismen regerar. Strategier växer enligt detta ramverk fram i en miljö som består av dels *externa krafter*, dels *organisatoriska krafter* i form av en vidsträckt byråkrati, som försöker implementera och finputsa strategin löpande. *Ledningen* har en roll i att döma av och hitta en väg framåt givet externa krafter och det organisatoriska systemets förmåga och återkoppling. En strategi kommer till i en process som flödar både uppifrån och ner och nerifrån och upp enligt denna analysmodell (se Figur 1).

Exakta gränser mellan ledning, byråkrati och extern miljö är ofta svåra att dra. Vissa ministerier eller myndigheter kan vara emot konkreta nya förslag som är i linje med den övergripande cybersäkerhetsstrategin medan företag som åtminstone i teorin är privata och förlorar på t.ex. striktare statlig kontroll över internet är alltför beroende av staten för att öppet opponera. I teorin skulle parlamentet kunna vara en extern kraft som granskar den verkställande makten. I Ryssland har det dock sällan varit fallet under perioden som undersöks (Vendil Pallin 2018a). En rad samhällsorganisationer är så kallade GONGO:er (*government-operated non-governmental organizations*) och ligger bakom initiativ till ny lagstiftning som är i linje med regeringens cybersäkerhetsstrategi samtidigt som korruption inom Ryssland i vissa fall hjälper strategin på vägen och i andra förhindrar att den implementeras. Verkligheten är således mer komplicerad än vad Figur 1 kan ge bilden av.

Figur 1. Schematisk indelning av aktörer

Anmärkning: Figuren bygger på Mintzberg 1978 samt på hur Rysslands politiska system är uppbyggt och fungerar både formellt och i praktiken (Vendil Pallin 2018a).

Icke desto mindre kan det politiska systemet schematiskt delas in i:

- Rysslands politiska ledning, i vilken presidenten spelar en central roll, men också landets Säkerhetsråd och delar av Presidentadministrationen;
- organisatoriska krafter som omfattar byråkratin i form av ministerier och myndigheter, men också parlamentet, delar av näringslivet och samhällsorganisationer som står regeringen nära;
- samt externa krafter såväl inom Ryssland i form av t.ex. samhällsorganisationer, folkopinion och potentiellt politiskt motstånd, som utanför landet i form av bland annat globala internetföretag, internationell teknologisk utveckling och internationella ramverk.

Det analytiska ramverket kommer således att dela in åren 2000–2020 i fyra perioder. De inleds och avslutas när det går att identifiera att rysk cyberstrategi torde ha ändrats och ledningen gjort en avdömning. Under de olika perioderna används det analytiska ramverket dessutom för att diskutera hur organisatoriska och externa krafter har påverkat strategin gradvis och bidragit till att vissa element mer eller mindre har fallit bort medan andra har tillkommit. I kapitel fyra sammanfattas vilka de centrala aktörerna, de organisatoriska krafterna, har varit samt i viss mån hur deras inflytande har ökat eller avtagit under de olika perioderna. Det finns dock all anledning att översiktligt inleda med att också diskutera de externa krafterna.

2.2 De externa krafterna

Internet är till sin natur globalt och inte primärt uppbyggt för att ta hänsyn till var territoriella gränser råkar gå. Ryssland vill ha kontroll över det som man ser som ett ryskt segment av internet, men i realiteten påverkas landet av en rad internationella krafter i form av internationell händelseutveckling samt andra länders, internationella företags och organisationers agerande. Dessutom finns en rad krafter inom landet som kan motverka rysk cyberstrategi. Tillsammans utgör de alla externa krafter som ledningen och de organisatoriska krafterna måste ta hänsyn till.

Internationella aktörer

En rad multinationella företag utmanar Ryssland när landets cyberstrategi ska genomföras genom sin blotta existens och affärsidé. *Facebook* och *Google* har vid flera tillfällen kallats upp till Minkomsvjaz för att tvingas följa rysk lagstiftning och därmed blockera det som Ryssland anser vara olagligt innehåll. Ofta har dessa företag vägrat (Balasjova, Parfenteva & Kozlov 2019). Företagen tvingas väga emellan att bibehålla någorlunda goda relationer med Rysslands regering och att samtidigt bevara sitt varumärke och sin image som bl.a. försvarare av ett fritt internet. Den ryska lagstiftningen om att företag ska tvingas lagra data som ryska medborgare delar med sig av på ryskt territorium 2014 (se period tre, s. 39ff) var ett led i Rysslands agerande för att ”nationalisera” ett segment av internet och utsträcka rysk lagstiftning till att gälla även för internationella företag, ett försök att öka kontrollen över den externa miljön.

Ryssland behöver även ta hänsyn till hur andra länder agerar bilateralt med Ryssland liksom inom internationella organisationer som Förenta nationerna (FN) och Organisationen för säkerhet och samarbete i Europa (Osse). Västliga länder har t.ex. konsekvent motsatt sig Rysslands förslag om ett internationellt avtal om informationssäkerhet. Samtidigt har Ryssland byggt allianser med länder som delar den ryska synen på informationssäkerhet och behovet av att kontrollera trafikinnehåll. Främst har detta skett inom organisationer som *Shanghai Cooperation Organization* (SCO) och multilateralt med BRICS-länderna där förutom Ryssland även Brasilien, Indien, Kina och Sydafrika ingår.

Det är dock inte bara landets internationella cyberrelationer som påverkar rysk cyberstrategi. Konkurrens mellan länder om ekonomiskt inflytande, handelskrig och embargon får ofta både direkta och indirekta konsekvenser för Rysslands möjligheter att utveckla sin IT-industri; det kan t.ex. begränsa vilka partners som är tillgängliga för samarbete och vilka komponenter Ryssland kan importera. Än mer allvarliga händelser som väpnade konflikter och krig har också stor betydelse. De cyberangrepp som ägde rum framför allt mot den georgiska regeringen i kriget mellan Ryssland och Georgien 2008 var väl samordnade med Rysslands militära operation (Valeriano, Jensen & Maness 2018: 118–19). I samband med kriget med

Ukraina har Ryssland använt sig av cyberoperationer i en utsträckning som har fått en rad analytiker att beskriva Ukraina som ett laboratorium där Ryssland prövar ut sina cyberverktyg (Greenberg 2019; Patterson 2017). Båda dessa militära operationer har inneburit praktiska erfarenheter av cyberoperationer i kombination med användning av militärt våld, men Ryssland har också fått erfara hur särskilt ryskt agerande i Ukraina också resulterat i västliga sanktioner riktade direkt mot Ryssland och en ökad misstänksamhet mot ryskt agerande och t.o.m. mot enskilda ryska internetföretag.

Teknikutveckling, handelspolitik och företagsklimat

Den internationella miljön består dock inte bara av aktörer, internationella organisationer samt relationer och rivalitet mellan dessa. Ryssland kan inte hejda den teknologiska utvecklingen utan måste göra sitt bästa för att hänga med eller åtminstone inte hamna alltför långt efter. Cyberområdet kan här sägas angränsa till en rad teknologier som ses som avgörande för framtiden, bland vilka kan nämnas artificiell intelligens (AI), autonoma system och den femte generationen av mobila nätverk för dataöverföring (5G).

Ett uttalat ryskt mål har varit att minska landets beroende av utländsk teknologi på cyberområdet. Även här måste Ryssland ta externa krafter i beaktande. Regeringen må skapa frikostiga subventionssystem för att stimulera inhemsk produktion av maskinvara, programvara och operativsystem, men den globala konkurrensen kommer att sätta gränser för hur framgångsrik rysk politik är. Att producera elektroniska komponenter är t.ex. dyrt i små serier och Ryssland som marknad är ofta inte tillräckligt stort. Ett annat exempel är att den ryska regeringen t.o.m. har haft svårt att övertyga sina egna tjänstemän om fördelarna med rysk programvara snarare än utländsk trots diverse åtgärder.

De största multinationella IT-företagen, som Apple, Facebook och Google, har dessutom en så pass dominerande ställning att ryska användare troligen skulle ge uttryck för missnöje om de inte längre tilläts använda Apple-produkter och Facebook- och Googletjänster. Att ha den senaste Apple-produkten, att följa internationella artister på *Instagram* och använda meddelandetjänster som används av kollegor och vänner internationellt har en betydande dragningskraft, det man kan kalla en mjuk makt. I vissa fall har ryska alternativ förmått erbjuda konkurrenskraftiga alternativ (som de ryska sociala nätverken *vKontakte* och *Odnoklassniki*), men långtifrån på alla områden och sällan i form av produkter och program som kommenderats fram på statligt initiativ.[4]

[4] T.ex. var det statliga bolaget Rostelekoms försök att skapa en sökmotor allt annat än framgångsrikt (Vendil Pallin 2017a: 26).

Externa krafter i inrikespolitiken

Det finns även externa krafter inom Ryssland som inverkar på landets cyberstrategi. Rysslands politiska system må vara auktoritärt, men den politiska ledningen kan ändå inte kosta på sig att ignorera tecken på betydande missnöje inom eliterna eller ens bland befolkningen. Det finns ryska NGO:er som är öppet kritiska mot regeringens cyberpolicy. Deras direkta inflytande på rysk cyberstrategi kan tyckas svagt, men det finns flera exempel på hur de kan väcka den inhemska opinionen och även praktiskt bidra till att t.ex. hjälpa internetanvändare att använda sig av anonymiseringstjänster [5] eller kartlägga omfattningen av internetblockeringar som myndigheterna kanske helst skulle vilja förblev okänd.[6]

De flesta ryska företag verksamma på cyberområdet är försiktiga att kritisera regeringen öppet. De är väl medvetna om att sådan kritik kan leda till minskade möjligheter att vinna statliga upphandlingar. Framför allt små företag har emellertid betalat ett högt pris för de regleringar av internet som inneburit kostsamma pålagor och då ofta utan att få den kompensation som de dominerande bolagen kan räkna med. De mindre företagens brist på entusiasm för Rysslands fokus på kontroll och detaljreglering kan leda till problem för regeringen när det gäller att förverkliga cyberstrategin, inte minst på importsubstitutionsområdet. Till det ska läggas de strukturella problem som den ryska ekonomin dras med. Korruption, avsaknaden av en rättsstat, en förhållandevis liten sektor för små- och medelstora företag, ett kärvt innovationsklimat samt en företagskultur där bolagsjättarna bedriver rovjakt på mindre och framgångsrika företag (Japparova 2020) skapar en ogästvänlig miljö för en egen livskraftig produktion av alltifrån komponenter till operativsystem.

Oppositionen är stukad i Ryssland, men det finns ett antal oppositionella aktivister och då inte minst i de stora städerna. En yngre och urban generation har vant sig vid att fritt kunna använda internet och för flera av dem kan motstånd mot regeringens ökade kontroll växa till ett mer generellt missnöje med det politiska systemet. Ett exempel på detta är den demonstration som Rysslands libertarianska parti anordnade den 10 mars 2019 för att protestera mot de nya lagarna om ett ”suveränt internet” (Sarkisian & Karliner 2019). Den hotar inte Rysslands politiska system, men den utgör en signal till ledningen om missnöje.

Det finns också organisationer som anordnar konferenser och sammanställer material om repressionen på internet. Bland dessa kan nämnas Agora, som fokuserar på mänskliga rättigheter och ger ut en årlig rapport om friheten på internet (se Tabell 1, s. 47). Det finns ett nära samarbete mellan många av de organisationer och partier som följer utvecklingen av friheten på nätet i Ryssland. Sällskapet för

[5] Det kan ske genom t.ex. att ansluta sig till ett virtuellt privat nätverk (VPN) eller använda TOR (*The Onion Router*). Sådana anonymiseringstjänster gör det möjligt för en användare att använda e-post, surfa på internet eller chatta utan att utomstående kan se vem som kommunicerar med vem.

[6] Se t.ex. Roskomsvobodas sida ”VPN love”, https://vpnlove.me/ (3 mars 2020) och organisationens kartläggning av olika myndigheters blockering av webbsidor Roskomsvoboda, ”Rejestry”.

internetanvändare (OZI, *Obsjtjestvo zasjtjity interneta*) grundades i april 2013 efter att lagen som tillåter blockering av webbsidor med otillåtet innehåll – de ”svarta listorna” – trädde i kraft (se s. 39ff). Organisationen samlade IT-experter, företrädare från Agora, Piratpartiet och RosKomSvoboda,[7] men också företrädare från t.ex. Wikimedia.[8]

Förutom de olika organisationerna som arbetar för digitala rättigheter i Ryssland finns en rad enskilda aktivister för ett fritt internet som har lyckats nå ut till relativt många med sina budskap. Endast vissa av dem har lierat sig med den politiska oppositionen, men samtliga har en expertis inom IT och dessutom en relativt stor publik i form av t.ex. prenumeranter och läsare av bloggar – inte minst bland mer avancerade internetanvändare. Det gör att ryska myndigheter näppeligen kan ignorera dem.

[7] Piratpartiet grundade webbsidan RoskomSvoboda i samband med att lagen om svarta listor kom 2012. Sedan dess har webbsidan utvecklats till en egen organisation som fortsätter att arbeta för digitala rättigheter. RosKomSvoboda samarbetar också med Agora och har än idag en sida, ”Rejestry”, där samtliga blockerade webbsidor, bloggare och media samt nyhetsaggregatorer listas (https://reestr.rublacklist.net/).

[8] Roskomsvoboda tillhandahåller det material som tidigare fanns på www.freerunet.ru, Roskomsvoboda, https://roskomsvoboda.org/5296/. Se även OZI :s webbsida, https://ozi-ru.org.

3 Faser i ryskt beslutsfattande 2000–2020

Den första doktrinen som berör rysk cyberstrategi kom i september 2000. Även om cyberfrågor existerade innan dess även i Ryssland, är det svårt att hitta tecken på att en sammanhållen strategi existerade. En första och lång period inleds med därmed 2000 då Putin valdes till president. Denna första period avslutas 2011 då bl.a. regimkritiska demonstrationer i Moskva får landets politiska ledning att få upp ögonen för internet som mobiliserande politisk kraft. Period två är betydligt kortare, 2011–2014 och kännetecknas av ett yrvaket behov av att främst tygla friheten på internet. Startpunkten för period tre inleds i kölvattnet på annekteringen av Krim, efter vilken uppfattningen växer sig än starkare att en intensiv kamp pågår mellan Ryssland och Väst inom informationssfären, inklusive cybersfären. Genomgången nedan avslutas med att undersöka tecken på att en fjärde fas eventuellt tar sin början 2018/2019. Tidigare perioder har inletts på grund av att den politiska ledningen uppfattat ett ökat internet-relaterat hot. Denna period kan dock komma att kännetecknas av att ny cyberrelaterad teknologi lovar ökade möjligheter att forma det politiska systemet och uppnå den stabilitet som den politiska ledningen önskar, men också av de förändrade förutsättningar som pandemin medförde 2020.[9] Det är också under denna sista period som en tendens till ett splittrat internet, ett ”splinternet” (*The Economist – The World in 2020*: 109–110), kan skönjas och där pandemin 2020 kan komma att accelerera införandet av fler teknologier som gör intensifierad övervakning möjlig.

3.1 Den första perioden: 2000–2011

Samma år som Putin tillträdde som president antogs Rysslands första Informationssäkerhetsdoktrin (2000). Putin hade sedan han flyttat från S:t Petersburg till Moskva, innan han blev president bl.a. varit chef för FSB (från juli 1998), sekreterare i Säkerhetsrådet (från mars 1999) och därefter premiärminister (från augusti 1999). Putin torde därmed ha varit väl insatt i den doktrin som han skrev under som president i september 2000.

Informationssäkerhetsdoktrinen 2000

I doktrinen fanns många av de som skulle bli de viktigaste målen för Rysslands säkerhet på cyberområdet. Den framhåller behovet av att stärka kritisk

[9] Indelningen i faser ovan är också relativt väl i linje med hur andra forskare tenderar att identifiera viktiga brytpunkter. Till exempel finner Martti Kari (2019: 89–91) i sin studie av rysk strategisk kultur i cyberrymden att det är möjligt att dela in rysk hotuppfattning på området i tre perioder: en från 1990–2011, en från 2011–2014 och slutligen en från annekteringen av Krim 2014 och framåt. Se även Lonkila, Shpakovskaya & Torchinsky 2019.

informationsinfrastruktur samt att göra landet mindre beroende av import av hård- och mjukvara. Där finns långa avsnitt om vikten av att skydda landets andliga värden, att upprätthålla moral samt stärka patriotismen, men också formuleringar om ryska medborgares rättigheter och friheter vad gäller att söka information och uttrycka sig samt om rätten till personlig integritet. Vid den här tidpunkten var dock ett av Rysslands mål på det internationella området att ”förbjuda utveckling, spridning och användande av ’informationsvapen’”, en formulering som troligen syftade på cyberoperationer (Informationssäkerhetsdoktrinen 2000).

Rysslands åtgärder på cybersäkerhetsområdet

Samtidigt är det tydligt att ytterst lite hände på flera av de områden som lyftes fram som prioriterade. Ingen lag om skydd av kritisk informationsinfrastruktur antogs. Ryssland förblev beroende av import av programvara och operativsystem samt alltifrån komponenter till mobiltelefoner och servrar. Om något så växte beroendet i takt med att den teknologiska utvecklingen accelererade på området, men villkoren för innovation och att starta nya företag inom internetbranschen var relativt goda även i Ryssland. I den Strategi för utvecklingen av informationssamhället som antogs i februari 2008 finns visserligen formuleringar om vikten av att stärka patriotism och moraliska värderingar samt ett avsnitt om informationssäkerhet, men i de riktmärken för 2015 återfinns inga målsättningar som berör dessa områden. Snarare ligger fokus på att öka tillgänglighet genom utbyggnad av bredband, satsningar på IT-relaterad utbildning och investeringar i sektorn.

Först 2011 är det möjligt att skönja resultatet av en mer sammanhållen aktivitet vad gäller att föra fram Rysslands syn på informationssäkerhet internationellt. Då kom ett ryskt förslag till en internationell konvention om informationssäkerhet (*Convention on International Security* 2011). Det ryska Försvarsministeriet producerade samma år ett dokument: Konceptuell syn på Ryska federationens Väpnade styrkors verksamhet i informationsrymden. Arbetet på båda dessa dokument påbörjades sannolikt tidigare under den här första perioden, men redan då hade målsättningarna förändrats något jämfört med de som förelåg i Informationssäkerhetsdoktrinen 2000. I förslaget till en internationell konvention fanns de första konturerna till det som skulle blir Rysslands position vad gäller internationella ramverk på cyberområdet. Försvarsministeriets dokument innebar en uppdatering där bl.a. en tydligare åtskillnad gjordes mellan cybersäkerhet (informationsteknisk säkerhet) och informationspsykologisk sådan.

Under den här perioden förblev internet relativt fritt – inte minst jämfört med hur central kontroll etablerades gradvis över rikstäckande media. Samtidigt som Säkerhetsrådet antog den första informationssäkerhetsdoktrinen satt t.ex. ägaren till mediabolaget Media-MOST Vladimir Gusinskij i förhör (Odnokolenko 2000). Han tvingades samma sommar att sälja sina bolag till Gazprom Media och lämnade landet. I doktrinen fanns bland annat formuleringar om hur utländska tjänster

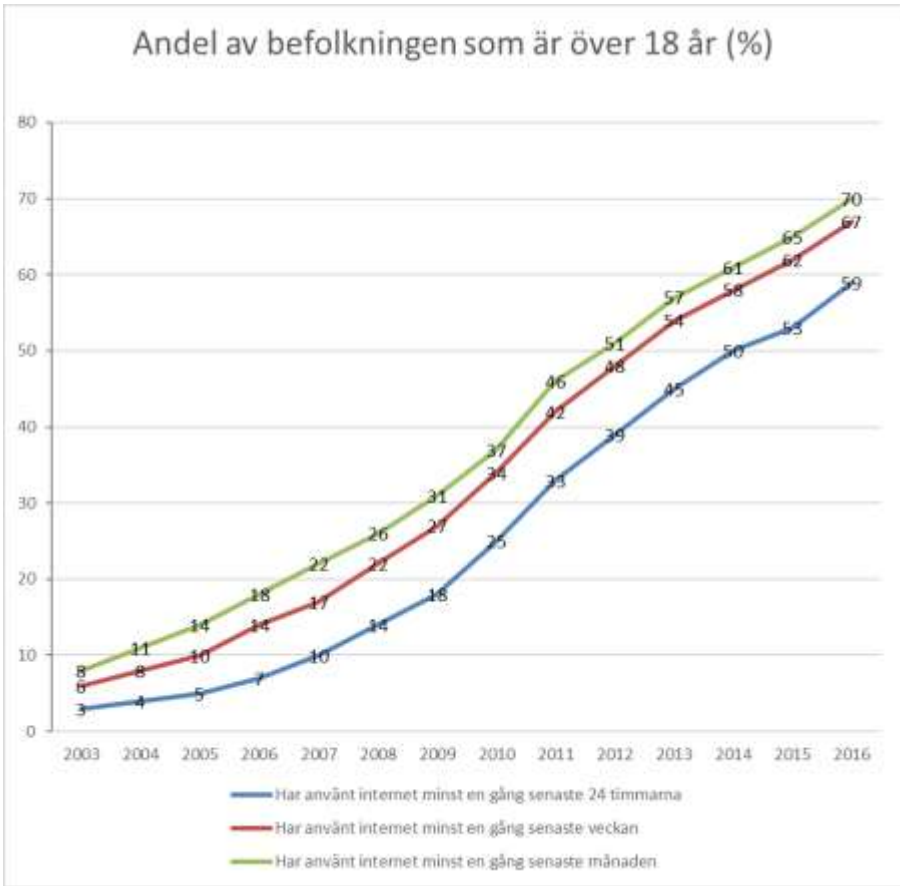
kunde utnyttja massmedia i Ryssland och att det utgjorde ett nationellt säkerhetshot, t.o.m. ett militärt sådant (Informationssäkerhetsdoktrinen 2000). Minkomsvjazi fick i uppdrag att anpassa lagstiftningen.

Enligt en artikel i tidningen *Segodnja*, som då fortfarande ägdes av Gusinskij, hade vice sekreteraren i Säkerhetsrådet, Vladislav Sjerstiuk, uttalat att ett ”blodigt krig” redan pågick på ”informationskrigsfronten” (Odnokolenko 2000), men eftersom antalet internetanvändare var relativt litet i Ryssland var det sannolikt framför allt massmedia som Sjerstiuk siktade in sig på. Sjerstiuk hade också en nyckelroll i att Informationssäkerhetsdoktrinen togs fram (Soldatov & Borogan 2015: 226).

Internetanvändningen i Ryssland började öka på allvar först kring mitten av denna period. Medan under tio procent av befolkningen över arton hade använt internet den senaste månaden 2003, hade en fjärdedel använt internet de senaste 24 timmarna 2010, se Figur 2. Internetanvändningen var mest utbredd bland en yngre, välutbildad del av befolkningen som bodde i storstäderna (Franke & Vendil Pallin 2012: 36–8).

Den första rapporten från *Freedom House* om friheten på internet, *Freedom on the Net*, publicerades 2009 och Ryssland fick då fortfarande betyget ”delvis fritt”. Det förekom också förslag på ökad reglering, men huvudsakligen använde myndigheterna lagstiftning om extremism och terrorism för att komma åt oönskat innehåll på internet (Franke & Vendil Pallin 2012: 55). Under 2008 föreslog en ledamot i Federationsrådet att webbsidor med mer än 1 000 besökare per dag skulle registreras som massmedier. Initiativet föll i temporär glömska, men återuppstod och antogs under period tre (se ”bloggarlagen”, s. 46) (Lonkina, Shpakovskaya & Torchinsky 2019: 21).

Samtidigt skedde dock en utveckling i det tysta inom de områden som underrättelse- och säkerhetstjänster kontrollerade. Redan 1998 hade FSB inlett en uppgradering av sitt system för övervakning av kommunikation som går under förkortningen SORM, Systemet for operativa förundersökningsåtgärder (*Sistema technitjeskich sredstv dlja obespetjenije funktsij operativno-rozysknych meroprijatij*). Det som brukar benämnas SORM-2 ersatte den första generationen av SORM. Denna övervakningsutrustning var samtliga internetoperatörer ålagda att både installera och bära kostnaden för (Soldatov & Borogan 2015: 398).



Figur 2. Internetanvändning i Ryssland 2003–2016

Källa: FOM 2016.

Tidiga försök att accelerera utvecklingen med regeringsinitiativ uppifrån (Tomas 2010: 269) verkar ha gett relativt lite utslag i produktion och innovation (Pynnöniemi & Marti 2016). Det fanns dock fortfarande en betydande innovationskraft inom vissa sektorer av internetföretagande i Ryssland under den här perioden. I takt med att antalet användare snabbt växte grundades en rad framgångsrika ryska internetföretag. Som ett av få länder i världen fick Ryssland inhemska konkurrenter till det sociala nätverket Facebook i form av Odnoklassniki, som nådde en miljonpublik 2006, och vKontakte, som gjorde det året efter och snabbt dessutom gick om Odnoklassniki. Pavel Durov, som låg bakom vKontakte, fortsatte att driva företaget som delägare (även om affärsmannen Alisjer Usmanov tidigt visade intresse och förvärvade en betydande andel i bolaget, se även nedan s. 46). Det ryska företaget *Yandex* grundades redan på 1990-talet och från 2000 började företaget ta marknadsandelar på allvar på den

växande inhemska internetmarknaden. Den ryska sökmotorn Yandex kunde tävla i popularitet med de internationella jättarna *Yahoo* och Google i Ryssland. Yandex börjad också tidigt att utöka sin verksamhet till att omfatta även andra tjänster (Franke & Vendil Pallin 2012: 39; Vendil Pallin 2017a).

De riktigt stora internetföretagen som tillhandahåller infrastruktur i form av t.ex. bredbandstjänster, serverkapacitet och fiberoptiska kablar, blev dock tidigt nära lierade med staten. Liksom ryskt näringsliv i övrigt rättade sig dessa efter statens behov och krav. De vinster som fanns att göra för lojala företag var redan betydande i termer av statliga kontrakt samtidigt som straffet för att inte vara följsam kunde innebära att företag helt stängdes ut från en lukrativ marknad. Samtliga dessa bolag tenderade under perioden att allt oftare uttala sitt otvetydiga stöd eller att bli alltmer försiktiga i sin kritik mot staten på cyberområdet. Enligt journalisten Andrej Soldatov kritiserade de den förda politiken på cyberområdet senast 1998, när regeringen införde den andra generationen av övervakningsutrustning, SORM-2 (”Polnyi Albats”, 8 april 2019).

Rysslands mest kända IT-säkerhetsföretag, Kaspersky Lab, grundades på slutet av 1990-talet av Eugene Kaspersky tillsammans med hans dåvarande fru Natalia Kaspersky och ytterligare en kollega. Eugene Kaspersky fick sin utbildning vid ett institut som drevs av FSB:s föregångare, KGB (*Komitet gosudarstvennoj bezopastnosti*) och det finns flera indikationer på att företaget bibehöll nära band med det som blev FSB (*The Economist*, 19 februari 2015). Företaget utvecklade programvara och lösningar för IT-säkerhet till företag och enskilda användare och tog även steget ut i världen till att sälja sina lösningar internationellt under den här perioden.

Under den här perioden bildades också branschorganisationer för olika delar av Rysslands näringsliv som var aktiva inom IT-sektorn. Ryska föreningen för elektronisk kommunikation (*Rossijskaja assotsiatsija elektronnych kommunikatsii*, RAEK) bildades 2006 och blev snabbt en av de mest inflytelserika. RAEK sammanställer rapporter om RuNets utveckling inom olika internetsegment, ordnar konferenser och delar ut priset ”RuNet Premium” (Turovskij 2016).

Cyberoperationer

Att Ryssland inledningsvis eftersträvade ett internationellt avtal som förbjöd ”informationsvapen” återspeglade troligen att landet ansåg sig ligga efter i utvecklingen på området. Det finns flera exempel på mer avancerade cyberoperationer som har kopplats till Ryssland efter det – något som tyder på att den offensiva cyberförmågan byggdes upp gradvis redan under denna första period. Andra indikationer finns också. FSB tog 2008 över det vetenskapliga forskningsinstitutet Kvant, (*NII Kvant*) och samma år köpte institutet in ett spionprogram från *Hacking Team*, ett italienskt företag som är har kritiserats för att sälja sina produkter till auktoritära regeringar (se t.ex. Marczak *et al.* 2014).

Under denna period förekom två cyberattacker som fick stor uppmärksamhet och hade kopplingar till Ryssland: överlastningsattackerna mot Estland 2007 och liknande attacker mot georgiska ministerier och myndigheter i samband med kriget mellan Ryssland och Georgien i augusti 2008. Angreppen var inte sofistikerade och det är svårt att fastställa om de utfördes av hackare på uppdrag av Ryssland eller om de rörde sig om så kallade patriotiska hackare och Ryssland helt enkelt hade stor nytta av deras verksamhet. Brandon Valeriano, Benjamin Jensen och Ryan Maness (2018: 118–19) klassificerar cyberattackerna mot Georgien 2008 som ryska i sin kvantitativa studie (se även Jensen, Valeriano & Maness 2019). Attackerna sammanföll i tid med ryska politiska och militära mål och Ryssland gjorde inget för att beivra t.ex. attackerna mot Estland trots att de i flera fall kunde kopplas till Kreml närstående personer och organisationer (Maurer 2018: 97–8).

En mer sofistikerad attack genomfördes mot amerikanska militära nätverk 2008, vilket ledde till att USA bildade ett cyberkommando. Genom ett externt dataminne med skadlig kod som någon i personalen på en amerikansk bas i Mellanöstern hittade och stoppade in i en bärbar dator, fick en grupp, som senare bl.a. benämnts som *Turla*, tillgång till militära dokument. Den estniska underrättelsetjänsten har kopplat Turla till FSB (Estonian Foreign Intelligence Service 2018: 53) och 2016 uppgav USA att den skadliga koden i fråga (*agent.BTZ*) kunde kopplas till rysk underrättelsetjänst (U.S. DHS and FBI 2016).

Ledningen och organisatoriska krafter

Den politiska ledningens uppmärksamhet gentemot internet kan bäst beskrivas som välvilligt likgiltig under den första perioden. Länge betraktade den inte cyber som en arena där politiska krafter kunde mobiliseras (Kari 2019: 89). Inom Presidentadministrationen fanns inget enskilt direktorat med IT-säkerhet eller IT-utveckling som ansvarsområde.[10] Inte heller tycks någon av presidentens rådgivare ha varit ansvarig för dessa frågor specifikt. Säkerhetsrådet var viktigt som motor för Informationssäkerhetsdoktrinen och hade redan 2000 en avdelning inom sitt kansli samt en interdepartemental kommission för informationssäkerhet (Vendil Pallin 2001). Efter att doktrinen antagits kännetecknades perioden dock snarare av bristen på samordning än det motsatta på cyberområdet.

Fram till 2003 var Federala agenturen för regeringskommunikationer och information (*Federalnoje agenstvo pravitelstvennoj svjazi i informatsii pri prezidente*, FAPSI) ansvarig myndighet för många av de frågor som faller inom ramen för cyberstrategin. När FAPSI upplöstes fördelades dess uppdrag med tillhörande materiel och personal, på framför allt FSB och Federala skyddstjänsten (FSO). FSO tog bland annat över signaltrupper och säkerheten inom regeringskom-

[10] I rapporten benämns *upravlenije* genomgående ”direktorat” medan den lägre organisatoriska nivån i rysk byråkrati, *department*, benämns ”avdelning”.

munikationsnäten (Vendil Pallin 2006: 69). FSB fick ett utökat ansvar för signalspaning, en uppgift som hamnade hos FSB:s 16:e Centrum för radioelektronisk spaning mot kommunikationsnätverk (Giles 2011: 53; Grebennikov 2019). I och med detta skapades troligen grogrund för rivalitet om mandat och resurser på cyberområdet mellan olika myndigheter.

Samma år grundades Informationssäkerhetsinstitutet vid Moskvauniversitetet. Vladislav Sjerstiuk var en drivande kraft bakom att det bildades och blev dess första direktör. Institutet kom att spela en viktig roll i att föra fram rysk syn på informationssäkerhet internationellt (Nocetti 2015: 119). Att tre av dess fyra direktörer och vice direktörer tidigare har arbetet inom Säkerhetsrådets kansli vittnar om dess starka bindning dit (Vendil Pallin & Oxenstierna 2017: 37–39). Redan 2001 startade Säkerhetsrådets kansli ett Nationellt forum för informationssäkerhet, Infoforum. Från början anordnade Infoforum konferenser inom Ryssland, men med tiden även internationella konferenser. Infoforums organisationskommitté samlade de viktigaste tjänstemännen och dumaledamöterna som företräder den syn på informationssäkerhet som Informationssäkerhetsdoktrinen gav uttryck för (Infoforum ”Ob Infoforume”; för en aktuell förteckning över organisationskommitténs medlemmar se Tabell 3, s. 97).

Inom regeringen var Ministeriet för kommunikation och massmedia en av de viktigaste aktörerna t.ex. då en ny federal lag om kommunikationer skulle antas 2003 (Federal lag, 126-FZ). Lagen var omdiskuterad och det fanns t.o.m. tecken på att större internetföretag som *Vympelkom*, genom deputerade i Duman, försökte minska ministeriets inflytande genom att införa ändringar i det ursprungliga lagförslaget (Tjeberko 2003). Lagen kom sedan att ändras och uppdateras vid flera tillfällen under perioden allteftersom utvecklingen på cyberområdet innebar nya utmaningar vad gäller reglering av t.ex. infrastrukturfrågor.

Summering av första perioden

Det är lätt att få intrycket av att det fanns två parallella verkligheter vad gäller rysk cyberstrategi under denna period. Å ena sidan fanns en informationssäkerhetsdoktrin som förespråkade en rad åtgärder för att stärka landets cyberförsvar och som såg okontrollerad informationsspridning som ett hot. Detta synsätt var fast förankrat inom Säkerhetsrådet och dess kansli liksom bland underrättelse- och säkerhetstjänster, som aktivt arbetade för att driva på för mer övervakning, bättre förmåga till att genomföra cyberoperationer och ökad acceptans för rysk syn internationellt. Å andra sidan skedde mycket lite utanför dessa kretsar för att faktiskt koordinera och genomdriva denna syn i praktiska åtgärder, något som bl.a. tillät en betydande grad av rivalitet om resurser och mandat att försena eller rentav paralysera t.ex. arbetet med att bygga processer och system för försvar av informationsinfrastruktur.

En relativt fri internetsektor inom ekonomin visade sig vara innovationskraftig och växte i takt med att internetanvändningen ökade. Friheten på internet var betydande och inom stora delar av regeringen och parlamentet sågs den nya informationsteknologin som en möjlighet snarare än som ett hot. Det är också betecknande att under denna inledande period existerade ingen central funktion inom Presidentadministrationen som hade ansvar för dessa frågor.

3.2 Den andra perioden: 2011–2013

Eftersom det politiska systemet på många sätt roterar kring en person, presidenten, blir frågan om vem som ska inneha den posten alltid central. Vid 2011 hade Dmitrij Medvedev varit president sedan 2008. Internetanvändningen hade stigit radikalt (se Figur 2, s. 34 ovan), främst i större städer. Landet som helhet hade efter ett decennium av hög tillväxt också börjat bli mer och mer beroende av digital teknologi. Moskva vibrerade under första halvåret 2011 av rykten och spekulationer om vem som skulle ställa upp i presidentvalet 2012. Dumavalet i december 2011 sågs av många som en temperaturmätare inför presidentvalet. Vid partiet Enade Rysslands kongress den 24 september samma år föreslog Medvedev att Putin skulle bli partiets presidentkandidat. Beslutet, men också sättet på vilket det tillkännagavs, ledde till betydande missnöje. Landets högsta ledning tillsammans med maktpartiet Enade Ryssland behandlade valen som en formsak, en procedur utan reell betydelse och en hel del av missnöjet med detta bland befolkningen fann sin väg ut på det växande ryska internet lagom inför dumavalen.

Den arabiska våren i Mellanöstern hade redan lett till att den ryska politiska ledningen blev alltmer oroad för att internet skulle kunna utgöra en källa till politisk instabilitet och därmed leda till folkliga resningar även i Ryssland. Enligt Dmitrij Medvedev hade ”de” som låg bakom den arabiska våren förberett ett liknande scenario även för Ryssland (Medvedev 2011). Igor Setjin, som då var vice premiärminister, lovade att undersöka vad Google hade haft för sig i Egypten och hur ”folkets energi hade manipulerats” (*Vedomosti*, 23 mars 2011). Protester i framför allt Moskva mot valfusk i Dumavalet växte därefter snabbt till omfattande demonstrationer som krävde maktskifte vintern 2011–2012. Denna händelseutveckling bidrog till att den ryska politiska ledningen kom att uppfatta mobilisering på internet som ett växande hot mot landets politiska system (Giles 2016: 36ff; Soldatov & Borogan 2015: 163ff, Lonkina, Shapovskaya & Torchinsky 2019: 17ff).

I Rysslands utkast till ”Convention on International Information Security” stod informationssäkerhet snarare än cybersäkerhet i fokus. Varje land skulle ”ha rätt att upprätta suveräna normer och styra sin informationsrymd enligt sina nationella lagar” (§5:5). Ryssland ville således reglera den globala informationssfären enligt territoriella gränser. Vidare var det bara staters regeringar som skulle signera konventionen, vilket gick på tvärs med den *multistateholder*-modell för reglering

av internet som rådde – en modell som innebär att regeringar, internationella organisationer och företag deltar i diskussionen om hur globala internet ska regleras.

Friheten på internet beskärs och övervakningen intensifieras

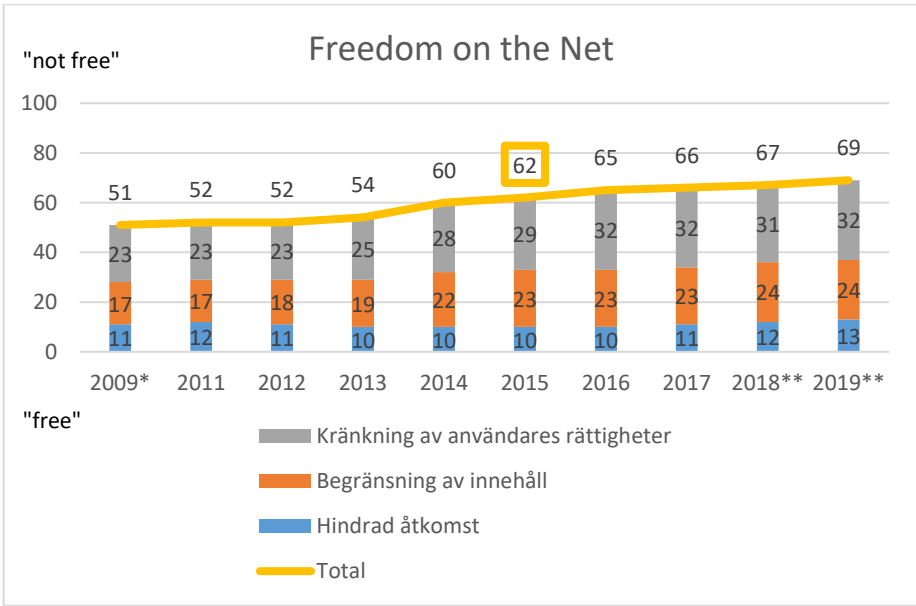
Perioden är kort, bara tre år, och ledtiderna för att anta ny lagstiftning, arbeta fram nya programdokument och sätta ihop regeringsprogram på området samt dessutom se resultaten av dessa är som regel längre. Redan 2011 började dock t.ex. polisen att använda sociala medier och bloggar för att upptäcka tecken på att demonstrationer och proteströrelser planerades. Inom Inrikesministeriet (MVD) började Huvuddirektoratet för att bekämpa extremism, Direktorat E, att leta efter det som kunde beskrivas som samhällshotande verksamhet på internet. Direktorat K, i vilket en Byrå för särskilda tekniska åtgärder ingår, fick ansvaret för att bekämpa brott på internet (*RBK*, 8 december 2011; *BBC News – Russkaja sluzjba*, 8 december 2011).

Under slutet av den här perioden, 2012–2013, infördes också så kallade svarta listor, dvs. myndigheten Roskomnadzors register över webbadresser som innehöll olaglig information och därför skulle blockeras (Sivetc 2019). I början presenterades lagen som ett sätt att skydda barn och unga från skadligt innehåll, men listan över förbjudet innehåll ökade snabbt. Ryssland började också kräva att Google och *YouTube* skulle ta bort innehåll som strider mot rysk lag. Även om Ryssland fortfarande rankades som ”delvis fritt” i Freedom House rankning *Freedom on the Net* under den här perioden (se Figur 3) initierade myndigheter som FSB och Roskomnadzor en rad åtgärder för att minska friheten på internet och öka övervakningen över innehåll och trafikflöden.

Förbundet för ett säkert internet (*Liga bezopasnogo interneta*) var en aktiv organisation vad gäller att initiera ny lagstiftning för att öka statlig kontroll. Minkomsvjaz hade aktivt visat sitt stöd för att en sådan organisation bildades 2011 och den dåvarande ministern, Igor Sjtjegolev, utnämndes till ordförande i styrelsen och behöll denna post även som presidentrådgivare efter 2012 (se längre ned, s. 42). Andra styrelseledamöter var företrädare för några av de största ryska internetföretagen men också för FSB (Andrej Gerasimov från FSB:s Centrum för informationssäkerhet, se s. 64), Inrikesministeriet och de båda parlamentariska kamrarna. Det uttalade målet var att uppmuntra till självreglering av internetmarknaden så att ”farligt innehåll” försvann från internet. (*Vedomosti*, 23 mars 2011; Förbundet för ett säkert internet, ”O Lige”; Förbundet för ett säkert internet 2017).

Ett av förbundets flaggskepp blev dess ”Cybermilis” (*Kiberdruzjina*), ett volontärsällskap som skulle vara aktivt på nätet. Cybermilisen skulle spåra brott på internet och rapportera dessa till rättskipande myndigheter såväl som spåra upp och förstöra farligt innehåll genom Förbundet för ett säkert internets jourlinje.

(Förbundet för ett säkert internet, ”Kiberdruzjina”).[11] Även partiet Enade Ryssland sjösatte ett liknande projekt, Mediagardet (*Mediagvardija*) inom ramen för partiets ungdomsorganisation Unga Gardet (*Molodaja gvardija*). Putin uttryckte sin uppskattning för dess verksamhet vid ungdomslägret Seliger 2013 och i januari 2014 rapporterade Mediagardet att man hade identifierat 2 838 ”extremistiska hemsidor” (Sivkova 2014).



Figur 3. Freedom House – friheten på internet i Ryssland 2009–2019

Källa: *Freedom on the Net* 2009; 2011; 2012; 2013; 2014; 2015; 2016; 2017; 2018; 2019;

Anmärkning: I rankningen är 0 mest frihet på internet och 100 minst. Freedom House benämner länder som har en total upp till och med 30 för ”fria” (*free*); från 31 till och med 60 för ”delvis fria” (*partly free*); och länder med en total från 61 för ”icke fria” (*not free*). Ryssland rankades därmed som ”delvis fritt” till och med 2014 och från 2015 som ”icke fritt”.

* Första året, 2009, som rapporten publiceras anges totalvärdet 51. Dock anges i rapporten för 2011 att värdena för 2009 var lägre än totalen 51.

** Från och med 2018 ”vände” Freedom House på sin skala så att 100 var högsta frihetsrankning och 0 lägsta. I figuren ovan har det räknats om för att tillåta jämförelse över tid i enlighet med ursprungliga skalan där 100 var sämsta rankning på frihet på internet och 0 bästa.

[11] De som gick med i Cybermilisen kunde stiga i graderna allteftersom de rapporterade fler hemsidor till förbundet. Texten om milisen anger bl.a. att frivilliga miliser har en lång historia i Ryssland: ”Förmågan att skapa miliser vittnar om ett sunt samhälle som är kapabelt att bekämpa olika typer av hot.” (Förbundet för ett säkert internet, ”Kiberdruzjina”).

Företag som Yandex kunde fortsatt verka relativt oberoende av statligt ingripande och än så länge var vKontakte i Pavel Durovs ägo. Det fanns dock tecken på att den politiska ledningen blev alltmer intresserad av att styra utvecklingen mer i detalj. Vid ett möte med Agenturen för strategiska initiativ 2012 slog Putin fast att Ryssland behövde en särskild investeringsfond för internetinitiativ ”som är socialt värdefulla och löser viktiga samhällsproblem”. Han lovade att personligen undersöka möjligheterna att finansiera en sådan fond och snart stod det klart att Rosneft och Gazprom sköt till pengar. Resultatet blev Utvecklingsfonden för internetinitiativ (*Fond razvitija internet-initiativ*, FRII) (”Zasedanije nabljutadelnogo soveta…” 2012; Sucharevskaja 2016) och innebar att den statliga kontrollen ökade över hur riskkapital allokerades inom rysk IT-industri.

Kaspersky Lab blev under den här perioden ett av få ryska internetföretag som även nådde stor framgång internationellt. Bland annat gjorde sig Kaspersky Lab ett namn genom att i efterhand kunna kartlägga Stuxnet, det angrepp på Irans uranberikningscentrifuger i Nantanz som ägde rum redan 2009–2010 och som brukar attribueras till USA och möjligen även Israel (Kushner 2013). Även det ryska IT-säkerhetsföretaget Group-IB blev framgångsrikt i att sälja sina tjänster och programvara internationellt. Group-IB skapade den första CERT-tjänsten (*computer emergency response team*) i Östeuropa och specialiserade sig 2011 på cyberbrottslighet (Gershikov 2018).

Teknikberoende och informationsinfrastruktur

Eftersom perioden är kort, är det svårt att se någon betydande förändring i Rysslands importberoende på cyberområdet. Även vad gäller säkerhet för informationsinfrastruktur finns relativt få tydliga tecken på utveckling. Mot slutet av period två inleddes dock arbetet med att skapa en process för att upptäcka och oskadliggöra cyberattacker i och med att FSB tilldelades huvudansvaret för att utveckla denna (Presidentdekret nr. 31s, 15 januari 2013). Därmed inleddes arbetet med att skapa ett Statligt system för att upptäcka, förhindra och oskadliggöra konsekvenser av datorattacker (GosSOPKA, *Gosudarstvennaja Sistema obnaruzjenija, predotvrasjtjenija i likvidatsii posledstvij kompjuternych atak*), men en rad frågor återstod att lösa ut. Bland annat var det inte klart exakt vilka system som skulle skyddas –presidentdekretet angav bara ”informationssystem och informations- och telekommunikationsnät” som var belägna på ryskt territorium eller vid ryska beskickningar i utlandet. Senare skulle det stå klart att framför allt statliga system och nätverk var huvudsakliga objekt som skulle skyddas, medan frågan om t.ex. skydd av näringslivets IT-resurser återstod att lösa. Troligen pågick fortfarande en kamp mellan olika myndigheter om hur ansvar och resurser skulle fördelas.

Cyberoperationer

I efterhand är det också tydligt att Rysslands förmåga att genomföra cyberoperationer fortsatte att öka under denna period. FSB och troligen också Utrikesunderrättelsetjänsten (*Sluzjba vnesjnej razvedki*, SVR) utvecklade sin förmåga att framför allt ta sig in i nätverk och inhämta underrättelser, t.ex. i Tjetjenien och Ukraina men också inom Nato (*Council on Foreign Relations*; F-Secure 2015). Troligen började även GRU att bygga upp sin förmåga efter Georgienkriget, men eftersom GRU förlitade sig på att rekrytera och utbilda egen personal på området snarare än på att rekrytera redan aktiva hackare gick det långsammare (Greenberg 2019: 241).

Cyber blir en angelägenhet för den politiska ledningen

Att cyberfrågor blev en fråga för högsta politiska ledningen återspeglades också organisatoriskt inom Presidentadministrationen. Efter presidentvalet 2012 tillkom ett Direktorat för användande av informationsteknologi och utveckling av valdemokrati. Samtidigt blev före detta kommunikationsminister Igor Sjtjegolev presidentrådgivare (*pomosjtjnik*)[12] med ansvar för arbetet på den nya enheten (Granik & Nagornich 2012). I januari 2016 utsågs dessutom German Klimenko till rådgivare, men med lägre rang (*sovetnik*) inom Presidentadministrationen – troligen framför allt på inrådan från dåvarande förste vice chefen för Presidentadministrationen med ansvar för inrikespolitiska frågor, Vjatjeslav Volodin (Turovskij 2016).

Under den här perioden fick också både FSB och Minkomsvjaz tillsammans med myndigheten Roskomnadzor en ökad roll i cyberfrågor. Samtidigt verkar samordningen mellan olika ministerier och myndigheter inte ha varit betydande. När Försvarsministeriet 2011 publicerade sitt dokument Konceptuell syn på Ryska federationens Väpnade styrkors verksamhet i informationsrymden, inleds denna visserligen med ett citat från Informationssäkerhetsdoktrinen från 2000, men i övrigt finns bara två generella hänvisningar till den.

Under den här perioden företrädde Federationsrådet i huvudsak en mjukare linje och publicerade ett eget utkast till cybersäkerhetsstrategi för Ryssland (Federationsrådet 2014). Förutom att utkastet sorterade ut cyberaspekter snarare än att behandla hela informationssäkerhetskomplexet, var det också en text som var betydligt mer företagarvänlig. Bland annat betonade utkastet vikten av att hitta en balans mellan aktörers skyldighet att tillhandahålla cybersäkerhet och vikten av att inte införa för många förbud och regleringar på området (se även Franke 2015: 20–22). FSB var starkt emot detta dokument bland annat eftersom det refererade

[12] På ryska finns två ord för rådgivare, *pomosjtjnik* och *sovetnik*, där de som har graden *pomosjtjnik* inom rysk förvaltning har en högre rang än de som är *sovetnik*. I denna text översätts båda med det svenska ordet ”rådgivare” med den ryska titeln anges inom parentes.

till ”cybersäkerhet” snarare än ”informationssäkerhet”. Bland företag verksamma inom internetsfären var man däremot positiv till Federationsrådets utkast (Rosjtjina 2014). Dokumentet tog sig aldrig förbi utkaststadiet.

Även i Duman kunde under den andra perioden ett presidentförslag om ökade befogenheter för FSB på cyberområdet leda till debatt 2013. Enligt lagförslaget skulle FSB få möjlighet att bedriva förundersökningar på internet om agerande som innebar hot mot Ryska federationens informationssäkerhet. Regeringspartiet Enade Ryssland ställde sig bakom förslaget med hänvisning bl.a. till hotet från hackare och skadlig kod, liksom även Utskottet för säkerhet och korruptionsbekämpning, medan såväl Kommunistpartiet, Vladimir Zjirinovskijs Liberaldemokratiska parti som partiet Rättvist Ryssland ställde kritiska frågor. Som så ofta förelåg i debatten en betydande oklarhet vilka befogenheter det rörde sig om – befogenheter att bekämpa cyberattacker eller något mer generellt rörande informationssäkerhet i största allmänhet. Bland dem som också uttalade sig kritiskt återfanns företagsorganisationen RAEK:s direktör, Sergej Gribennikov (Basjlykova 2013).[13]

Summering av andra perioden

Perioden är relativt kort – inte minst jämfört med föregående – och troligen resulterade flera åtgärder som initierades 2011–2013 i synliga förändringar först under påföljande år. Det mest tydliga resultatet var att cyberfrågor lyftes till att bli en fråga för Presidentadministrationen. Dels finns flera citat från tiden som tyder på att den politiska ledningen i större utsträckning såg information på internet som en potentiell källa till politisk instabilitet, dels fick Presidentadministrationen för första gången både ett direktorat och en rådgivare med ansvar för dessa frågor. Även om internet i Ryssland fortsatt rankandes som ”delvis fritt” under perioden, kan de första stegen mot en ökad kontroll och övervakning skönjas i form av blockering av webbplatser och att FSB och MVD började övervaka sociala medier för att tidigt upptäcka demonstrationer och proteströrelser. Under den här perioden börjar också regeringen använda sig av organisationer som Förbundet för ett säkert internet. Ett av syftena med detta är att ge intryck av att det finns en efterfrågan från civilsamhället på mer övervakning och förbud, trots att organisationer som dessa är tydligt kontrollerade av regeringen.

Bilden är dock inte entydig. Fortfarande arbetade Federationsrådet på en cyberstrategi som låg närmare många internetföretags syn på hur internet skulle regleras än den syn som dominerade inom myndigheter som FSB och FSO. Få kraftfulla åtgärder och koordinerade åtgärder för att minska importberoende eller för att

[13] Troligen förelåg en viss sammanblandning av olika typer av dokument och befogenheter i debatten. De lagändringar det rörde sig om (Federal lag 369-FZ, 21 december 2013) utökade FSB:s möjligheter att bedriva förundersökningar på cyberområdet, en ändring som initierats av presidenten. Som nämnts ovan hade FSB redan i januari samma år fått i uppgift att utveckla en process för att bekämpa cyberattacker (se ovan s. 35).

skydda rysk informationsinfrastruktur kan noteras. Snarare fattades beslut i stuprör. Rysslands utkast till internationell konvention från 2011 markerar ett viktigt steg i försöken att vinna acceptans internationellt för rysk syn där regeringar har större makt och informationssäkerhet snarare än cybersäkerhet står i centrum. Det dokument om konceptuell syn på informationsrymden som Försvarsministeriet publicerade samma år ger också intryck av att vara koordinerat främst inom den egna sfären snarare än vara ett resultat av en koordinerad process med andra ministerier och myndigheter.

3.3 Den tredje perioden: 2014–2018/2019

Den första oktober 2014 samlades det ryska Säkerhetsrådets ständiga medlemmar för att diskutera landets informationssäkerhet. Ryssland hade annekterat Krim i mars samma år och gick vidare med att destabilisera stora delar av östra Ukraina. Väst protesterade, men det som ökade det politiska trycket på Ryssland var reaktionerna efter att ett malaysiskt passagerarplan hade skjutits ned över östra Ukraina den 17 juli 2014. Senare utredningar skulle slå fast att en rysktillverkad markrobot hade avfyrats från ett område som kontrollerades av pro-ryska rebeller, men den ryska omedelbara reaktionen var att förneka all inblandning, precis som Ryssland förnekade att man alls var inblandat i kriget i östra Ukraina. När mötet i Säkerhetsrådet ägde rum var Ryssland under betydande press. Såväl USA som Europeiska unionen hade infört sanktioner mot Ryssland. Vladimir Putins inledningsord vid mötet lade fast huvudlinjerna för den framida inriktningen av rysk cyberpolitik, t.ex. nämnde han behovet av att det ryska segmentet av internet skulle kunna fungera ”suveränt” utan att vara beroende av den globala infrastrukturen. Enligt Putin hade också cyberattackerna ökat det senaste halvåret:

> Våra respektive myndigheter noterar en stadig ökning av datorattackerna mot ryska informationsresurser. Jag måste säga att under den senaste tiden, det senaste halvåret, har antalet attacker ökat flerfalt; det går inte ens att jämföra med föregående år. Dessutom har metoderna, medlen och taktiken för att genomföra sådana attacker förfinats och deras intensitet beror direkt på det rådande internationella läget. (”Zasedanije Soveta Bezopasnosti”, 1 oktober 2014)

Putins uttalande i Säkerhetsrådet den dagen är ett tydligt exempel på hur externa krafter i form av det internationella läget drev på utformningen av rysk cyberstrategi. Europeiska unionen (EU) hade redan efter annekteringen av Krim infört sanktioner mot Ryssland, men de begränsades till att drabba enskilda ryska makthavare. Efter nedskjutningen av MH17 blev dock sanktionerna mer kännbara för Ryssland – de utsträcktes t.ex. till att gälla oljeföretag, teknologiöverföring till Ryssland och tillgången till finansiella marknader. När mötet ägde rum i Säkerhetsrådet i oktober 2014 fanns troligen även en rysk rädsla för att Väst i en framtida konflikt skulle kunna skära av Ryssland från den globala infrastruktur på internet som landet var fortsatt beroende av. Tanken på att skapa ryska kopior av t.ex.

rotservern för .ru, DNS-katalogen[14] och IRR-katalogen (*internet routing registry*, en katalog för hur trafiken dirigeras) hade kanske existerat redan tidigare inom t.ex. FSB och Säkerhetsrådets kansli, men i oktober 2014 lyftes den också till avdömning av den politiska ledningen (Vendil Pallin 2018b). På flera områden fick implementeringen av många av de områden som pekades ut i Informationssäkerhetsdoktrinen från 2000 nu ny kraft. Skapandet av ett, vid behov, fristående nationellt internet och en s.k. *kill switch* eller huvudströmbrytare för att stänga av förbindelser med omvärlden, blev ett av de långsiktiga målen för rysk cyberstrategi.

Informationssäkerhetsdoktrinen 2016

Vid mötet i Säkerhetsrådet lade rådets ständiga medlemmar dessutom fast det som skulle bli huvudlinjerna i nästa Informationssäkerhetsdoktrin (2016). Tematiskt var de prioriterade områdena: att skydda kritisk informationsinfrastruktur; att minska Rysslands importberoende på cyberområdet; att öka kontrollen och övervakningen över innehållet inom det som definieras som ett ryskt segment av internet; samt att fortsätta ansträngningarna internationellt för att få genomslag för den ryska synen på informationssäkerhet (Vendil Pallin 2018b).

Mycket känns igen från Informationssäkerhetsdoktrinen från 2000, men nu sjösatte regeringen även konkreta program på området. Ett av de viktigaste blev regeringsprogrammet ”Digital ekonomi”, som kom 2017. Det var inte bara detaljerat utan kom med betydande finansiella anslag. Inom ramen för programmet fanns en underrubrik ”Digital säkerhet” där de flesta av de frågor som är av intresse för denna rapport återfinns.

Informationssäkerhetsdoktrinen (2016) utarbetades i Säkerhetsrådet och då mer specifikt inom dess kansli och dess Avdelning för säkerhet inom informations- och informationsteknologiområdet. Det var också inom en av Säkerhetsrådets kommissioner, den Interdepartementala kommissionen för informationssäkerhet, som arbetet koordinerades och förankrades bland berörda ministerier och myndigheter samt utvalda vetenskapliga instanser och näringslivsrepresentanter (*RIA Novosti*, 24 juni 2016; se vilka som ingår i kommissionen i Appendix Tabell 4, s. 99). Precis som Vladislav Sjerstiuk som vice sekreterare i Säkerhetsrådet höll i framtagandet av doktrinen år 2000, leddes arbetet med 2016 års doktrin troligen av den vice sekreterare som då ansvarade för informationssäkerhet, Sergej Buravlev. Han kom från FSB och ingick redan 2005 i organisationskommittén för en av Sjerstiuks årliga konferenser i Garmisch-Partenkirchen (se Tabell 2, s. 63 för samtliga vice sekreterare med ansvar för informationssäkerhet). Buravlev torde därmed också ha varit ordförande i den interdepartementala kommissionen för informationssäkerhet.

[14] DNS – domännamnsystemet som översätter domännamn, som t.ex. kremlin.ru till en IP-adress.

Turbofart på kontrollåtgärder

Under den här perioden accelererade kontrollen över internet i Ryssland. Från och med 2015 började Ryssland rankas som ett ”icke fritt” land i de rapporter om friheten på internet som sammanställs och publiceras av Freedom House (se Figur 3, s. 40). I de sammanställningar som Agora gör av antal åtgärder för att förhindra friheten på internet är ökningen som följde 2014 tydlig (se Tabell 1. s. 47). Redan 2014 antogs ”bloggarlagen”, som ställde krav på den som tillhandahåller information på internet att lagra data i sex månader. I förarbetet angav Dumaledamöterna bakom förslaget att det skulle skydda medborgarnas rättigheter men också ”få ordning på spridandet av information och utbyte av data mellan internetanvändare” (Förslag till federal lag 428884-6, 15 januari 2014).

En av de dumaledamöter som stod bakom bloggarlagen, Irina Jarovaja, var även så pass pådrivande bakom en uppsättning av lagändringar 2016 att hela ”paketet” fick hennes namn i ryska medier. Jarovaja-paketet innebar en rad lagändringar som bl.a. ålade internetoperatörer att lagra trafikdata i minst ett år och trafikinnehåll i sex månader med hänvisning till samhällets säkerhet och terrorhot. Lagändringarna drevs igenom med vissa justeringar trots att t.ex. de tekniska möjligheterna inte fanns för att lagra mängden data som föreskrevs (Federal lag 375-FZ, 6 juni 2016; Lehtisaari 2019: 61–2; Rozjkov & Tisjinja 2017).

De så kallade svarta listorna över förbjudna webbplaster blev allt längre. Dessutom kom förslag från Förbundet för ett säkert internet och en dumaledamot om att skapa ”vita listor”, dvs. snarare än att förbjuda vissa webbplatser skulle det finnas listor över vilka webbplatser som är tillåtna medan allt annat filtrerades bort (Zykov 2017). Förslaget förverkligades inte, men liksom tidigare förslag kan det mycket väl återkomma senare i delvis ny form. Till det ska läggas att internetanvändare även fortsatt kunde åtalas för information de lagt ut som bedömdes som extremistisk, att bloggare hotades och oppositionella webbsidor utsattes för t.ex. överlastningsattacker (se Tabell 1, s. 47).

Inte bara användare märkte av ett kärvare klimat. Flera av landets internetföretag kände också av det. Alisjer Usmanov hade redan gjort en förmögenhet inom informations- och kommunikationsteknologi (ICT) och stod Kreml nära. När hans företag *Mail.ru* tog över sociala nätverket vKontakte från Pavel Durov 2014 blev det mycket uppmärksammat. Det blev dessutom ett exempel på en mer övergripande utveckling där ”de stora fem” fick allt större inflytande samtidigt som mindre företag hade svårt att växa och utveckla sin verksamhet (Vendil Pallin 2017a: 24).

Tabell 1. Agoras årliga rapporter: Friheten på internet 2011–2019

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
Administrativ press	173	208	514	1 448	5 073	53 004	22 523	4 402	3 917
Blockeringar	231	609	236	947	1 721	35 019	88 832	488 609	161 490
Domstolsåläggande	-	124	624	72	7 300	24 000	2 196	161 171	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/ 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**

Källa: Agora 2019a; Agora och Radio Svoboda (2020). Tabellen bygger även på data två tidigare rapporter, Agora 2017; 2018.

* Agoras data om restriktioner för tillgänglighet på internet är baserad på officiell statistik. Enligt organisationen RosKomSvoboda (2020) blockerades väl över tio miljoner resurser under 2018.

** I kategorin ”Övrigt” ingår alltifrån att någon avskedats från sitt jobb pga. 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 i Agora (2019a).

Inte alla försök att kontrollera internet var lyckosamma. Pavel Durov tog med sig sitt nya projekt när han lämnade Ryssland, en ny meddelandetjänst som döptes till *Telegram* och med en kryptering som FSB inte hade tillgång till. Efter flera försök att på olika sätt tvinga Durov att lämna över krypteringen till ryska myndigheter började Roskomnadzor blockera de webbsidor som tjänsten Telegram använde sig av från och med april 2018. Det visade sig bli ett kostsamt beslut. Durov svarade med att använda lösningar som 'gömde' Telegram bakom anonymiseringstjänster (VPN) och neutrala webbadresser. Roskomnadzor hade till slut blockerat över 15 miljoner IP-adresser.[15] Den skarpa ökningen av blockerade webbsidor som märks i Agoras statistik 2018 är främst ett utslag av dessa försök att blockera Telegram (Sivetc 2019: 47ff, se även Tabell 1). Kostnaderna för ryskt näringsliv blev omfattande och ryska internetanvändare kunde plötsligt inte nå ett stort antal webbsidor. Dessutom anordnades uppmärksammade protester – t.ex. i form av att protesterande kastade vita pappersflygplan från fönster som stöd för Telegram, som har en vit papperssvala som logotyp. Roskomnadzors blockering av Telegram var således allt annat än framgångsrik. Meddelandetjänsten Telegram fortsatte att fungera och dess antal abonnenter ökade som ett resultat av uppmärksamheten (Vendil Pallin 2019b: 2).

Även Yandex utsattes för påtryckningar. Företagets aktiekurs störtdök när rykten cirkulerade om att Sberbank skulle köpa in sig med en större aktiepost i oktober 2018 liksom när Duman hade lagt fram ett lagförslag om att begränsa utländskt ägande i internetresurser i juli 2019. I juni 2019 krävde FSB att Yandex skulle lämna över sin kryptering för användares kommunikation, något som också påverkade aktiekursen (Kolomytjenko 2019a). Yandex befann sig tillslut i en besvärlig situation – å ena sidan var det tydligt att trycket från ryska myndigheter för att öka kontrollen av Yandex bara skulle öka, å andra sidan tydde allt på att investerare snabbt skulle överge Yandex och aktiekursen falla om företaget uppfattades som kontrollerat av ryska regeringen. Resultatet blev en kompromiss i november 2019 som hade förhandlats fram med Presidentadministrationen. En internationell fond i ett offshorebolag i Kaliningrad tog över ledningen. Företagets grundare och direktör, Arkadij Volozj, behöll ett betydande inflytande, men en särskild styrelse kunde efter överenskommelsen gå in och ta över ledningen om det bedömdes nödvändigt av "nationella säkerhetsskäl". Samma dag som överenskommelsen blev offentlig drogs lagförslaget om utländskt ägande tillbaka i Duman (Baletskaja 2019; *Meduza* 2019).

Lagförslaget om ett "suveränt internet" 2018–2019

Redan 2014, vid mötet i Säkerhetsrådet i oktober, förekom de första tecknen på att Ryssland övervägde möjligheten att vid behov avskärma det ryska segmentet av

[15] IP – internetprotokoll, det centrala protokoll för kommunikation på internet, som bl.a. bestämmer att varje dator på internet ska ha en unik adress, en IP-adress.

internet från omvärlden. Månaden innan hade en övning, enligt källor inom underrättelse- och säkerhetstjänsterna, visat på sårbarheter. Minsvjaz hade under övningen undersökt om det som man definierade som ett ”ryskt” internet kunde fungera även om det var avskärmat från internets globala infrastruktur. Som ett resultat av övningen inleddes på initiativ från Säkerhetsrådet en process för att göra Ryssland mer oberoende av internets rotstruktur globalt, men också för att öka kontrollen över kablar som korsade rysk gräns och hur trafiken dirigerades i rysk infrastruktur (*Vedomosti*, 19 september 2014; Sucharevskaja & Juzbekova 2016; Nikkarila & Ristolainen 2017).

Det hela kulminerade i lagen om ett suveränt internet. Remissgången i samband med lagförslaget 2018–2019 illustrerar att Rysslands ministerier och myndigheter fortfarande inte utgjorde ett helt monolitiskt system. Tvärtom existerade en rad motsättningar inom det organisatoriska systemet för att formulera och implementera rysk cyberstrategi (Vendil Pallin 2019b). Det rådde dock föga tvivel om att lagen skulle godkännas i Duman och träda i kraft – liksom tidigare lagar som begränsar friheten på internet har gjort (Agora 2019b).

I december 2018 lades ett lagförslag fram i Statsduman om ändringar i lagarna ”Om samband” (Federal lag 126-FZ) och ”Om information, informationsteknologier och om skyddet av information” (Federal lag 149-FZ). Syftet var att skapa möjligheten att skärma av ryska internet från det globala samt öka möjligheterna att övervaka och blockera trafik på internet som rör sig fysiskt på infrastruktur inom Rysslands geografiska gränser. I lagförslaget reglerades hur trafiken på internet i Ryssland skulle dirigeras och vad som är ”gränsövergångar” för ryska internet. Dessutom infördes möjligheter att installera teknisk utrustning som kan identifiera avsändaren av konkret trafik på internet. Förslaget hade av allt att döma tagits fram utan att samråd hade ägt rum med näringslivet och kritiserades genast av experter, men också i ett remissvar från arbetsgruppen ”Kommunikation och IT” från regeringens expertråd. Förslagsställarna hade angett att medel för att genomföra förslaget redan fanns anvisade i budgeten för programmet ”Digital ekonomi” medan expertrådets arbetsgrupp uppskattade kostnaderna för förslaget till 134 miljarder rubel, dvs. mer än vad som rymdes i gällande budget. Arbetsgruppen noterade också att förslaget inte definierade vilka konkreta hot som det skulle motverka samt att Roskomnadzor tilldelades befogenheter som gick emot rådande lagstiftning. Expertrådet pekade också på tekniska problem när styrningen av trafiken överlämnas till Roskomnadzor och att det riskerar att leda till att internettrafiken bromsas. Ytterligare kritik mot förslaget levererades den 16 januari 2019 från Aleksej Kudrin, ordförande för Revisionskammaren och före detta finansminister. Han menade att ständigt ändrade spelregler avskräcker investerare i den digitala sektorn och att förslaget behövde diskuteras brett i Ryssland (Vendil Pallin 2019b).

Bland de som tillstyrkte förslaget fanns Ministeriet för digital utveckling, Roskomnadzor, FSO och FSTEK. Den 23 januari tillstyrkte också Statsdumans

Utskott för säkerhet och bekämpande av korruption förslaget och rekommenderade att det skulle antas i första läsningen i Statsduman. I slutänden antogs lagen och idén att göra Rysslands internet ”suveränt” fick också övervägande stöd från ministrar, tjänstemän och företrädare för de stora internetbolagen (Vendil Pallin 2019b).

Infrastruktur och teknikberoende

Först året efter att Informationssäkerhetsdoktrinen antagits fick Ryssland en lag om skydd av kritisk informationsinfrastruktur (Federal lag 187-FZ, 26 juli 2017). I och med att den antogs sommaren 2017 stod det klart att FSB och FSTEK även fortsatt skulle inneha nyckelroller i att bekämpa cyberattacker. Detta blev formellt fastställt i och med att Putin skrev under ett presidentdekret som bekräftade FSB:s roll i december samma år (Presidentdekret nr. 620, 22 december 2017). GosSOPKA blev officiellt det system av processer som skyddar statliga nätverk och tillsammans med lagen om skydd av kritisk infrastruktur började även ett system för att skydda andra nätverk, t.ex. finansiella växa fram (Demidov 2016; Tjernenko 2017).

Redan tidigare hade Rysslands regering vidtagit flera åtgärder för att försöka minska Rysslands beroende av import på cyberområdet, men få faktiska resultat kunde noteras. I och med sanktionerna som följde på Rysslands krigföring i Ukraina blev så kallad importsubstitution ett ledord, så även på cyberområdet. Från och med 2015 fanns lagstiftning på plats som skulle stimulera framför allt statliga myndigheter att använda rysktillverkade cyberprodukter (Federal lag 188-FZ, 29 juni 2015). Statliga register över det som klassades som rysk hård- respektive mjukvara upprättades och även här är gränsen mellan vad som är en statlig myndighet och en samhällsorganisation oklar. Stiftelsen för informationsdemokrati (*Fond informatsionnoj demokratii*) drev projekt som i huvudsak beställts av federala, regionala och lokala myndigheter. Stiftelsens direktör, Ilja Massuch, utsågs dessutom 2018 till att leda ett centrum som har en nyckelroll för planerna på importsubstitution på IT-området (Jastrebova 2018b).

Återigen var resultaten troligen en besvikelse för den ryska politiska ledningen. I början av 2019 använde 96 procent av de federala myndigheterna fortfarande program som inte finns i det officiella register över rysk programvara som upprättats. Cirka 82 procent använde e-post-servrar producerade utomlands och i stort sett samtliga myndigheter använde databasservrar från *Microsoft, Oracle* eller andra utländska producenter (Kodatjigov 2019).

Ledning och organisatoriska krafter

Inom Presidentadministrationen spelade Direktoratet för användande av informationsteknologi och utveckling av valdemokrati en nyckelroll när detaljerna för de

olika linjerna i programmet ”Digital ekonomi” (2017) med tillhörande handlingsplan (*pasport*, oklart datum) utarbetades och då främst inom programlinjen ”Internet+Suveränitet”. Samma avdelning var dessutom ansvarigt för att utarbeta dokumentet Strategi för utvecklingen av informationssamhället i Ryska Federationen 2017– 2030 (2017) och då troligen i samarbete med Säkerhetsrådets kansli, som publicerade ett utkast av strategin 2016 (Sergina 2016).

Efter presidentvalet 2018 stöptes Presidentadministrationen om. Sergej Kirijenko efterträdde Vjatjeslav Volodin som förste vice chef för Presidentadministrationen med ansvar för inrikespolitiska frågor. Ingen presidentrådgivare ansvarade längre för cyberfrågor utan Kirijenko tog över även detta område. Det direktorat som hade varit ansvarigt för IT-frågor stöptes i juni 2018 om till Direktoratet för utveckling av informations- och kommunikationsteknologi samt kommunikationsinfrastruktur och fick i samband med detta en ny förordning. Detta direktorat var pådrivande i att få igenom lagen om ett suveränt internet (Novyj 2020; Presidentdekret nr. 334, 14 juni 2018).

I takt med mer omfattande lagstiftning för att kontrollera internet började Roskomnadzor växa väsentligt som myndighet (Sjadrina 2014). Andra myndigheter, framför allt FSB, men även Inrikesministeriet fortsatte dessutom att samla in data från t.ex. sociala medier inför stora demonstrationer (Rozjdestvenskij & Pintjuk 2019). Även FSO tycks ha intensifierat sin övervakning av internet. En av enheterna inom FSO försökte 2014 att upphandla mjukvara som kunde utföra automatiska sökningar efter information på internet. Enligt tidningen *Izvestija* ville FSO samma år söka igenom blogginlägg dagligen och då framför allt kartlägga hur dessa blogginlägg uttryckte sig om ryska myndigheter. Baserat på dessa sökningar skulle FSO skapa en databas bestående av blogginlägg som innehöll negativa attityder och publiceringar från oppositionen (Kasjevarova 2014).

I februari 2014 fick Utrikesministeriet ett särskilt sändebud för frågor inom internationellt samarbete inom informationssäkerhetssfären. Ambassadör Andrej Krutskich hade en bakgrund inom rustningskontrollförhandlingar och fick i uppgift att koordinera frågor som relaterade till ”politisk användning” av informations- och kommunikationsteknologi (Nocetti 2015: 118). Han deltog bland annat i de årliga möten som Sjerstiuks Informationssäkerhetsinstitut anordnade i Garmisch-Partenkirchen (Soldatov & Borogan 2015, 228–9). Under slutet av denna period nådde Ryssland också framgångar inom FN. Ryssland lade 2019 fram förslag till texter om dels informationssäkerhet, dels bekämpning av cyberbrottslighet i samarbete med Kina och andra länder med auktoritära politiska system och fick visst stöd – dock inte från västliga länder (Vendil Pallin 2020).

Under den här perioden genomförde Ryssland en omfattande militärreform. I den ingick även en modernisering av Väpnade styrkornas ledningssystem. Ett avgränsat militärt system för dataöverföring började troligen användas 2016 (Zykov & Ramm 2016) och en vice chef för Generalstabens 8:e direktorat, Tjänsten för sekretesskydd, Andrej Kolovanov, underströk på en konferens 2017 att det var av

yttersta vikt att de automatiserade ledningssystem som nu infördes inom de väpnade styrkorna hade bästa möjliga skydd mot cyberhot (Infoforum-2017).

Från att ha utvecklat en egen cyberstrategi som gick på tvärs med FSB:s syn, kom Federationsrådet under den här perioden i ökande utsträckning förespråka en syn som gick i linje med den som återfinns i de båda informationssäkerhetsdoktrinerna. Mellan 2012 och 2015 fanns en Tillfällig kommission för att utveckla informationssamhället. Ljudmila Bukova var dess ordförande och var tidigare en politiker som värnade medias frihet. Redan 2015 ansåg hon dock att: ”Vår regering bör styra internet… Det är nödvändigt att bringa RuNet under total statlig kontroll.” (Goldberg and Romanova 2015) Federationsrådets Tillfälliga kommission för informationspolitik och samarbete med massmedia bildades 2016, med uppgift att se över lagstiftningen gällande massmedia (Federationsrådets förordning, nr. 475-SF, 26 oktober 2016). Dessutom bildades 2017 en “Tillfällig kommission för att skydda statlig suveränitet och hindra inblandning i Ryska Federationens inrikespolitik”, som leds av Andrej Klimov. Denna kommission publicerar, bland annat, årliga rapporter om misstänkt utländsk inblandning i rysk inrikespolitik. Enligt rapporten från 2018 är suveräniteten hotad och då särskilt efter 2014 på grund av ett informationskrig som Väst bedriver mot Ryssland. Rapporten beskriver framför allt propagandaåtgärder, men noterar även att informations- och kommunikationsteknologi har skapat nya möjligheter för Washington (Federationsrådet 2018). I rapporten 2019 uppehåller sig kommissionen bland annat vid hur rysk kritisk infrastruktur kan blir föremål för framför allt attacker från USA (Federationsrådet 2019).

Antalet dumaledamöter som lade fram lagförslag om ökad statlig kontroll över internet blev också allt fler. Två ledamöter i Utskottet för informationspolitik, Andrej Alsjevskich och Sergej Bojarskij, initierade 2017 det lagförslag som nämnts tidigare om att skapa en ”vit lista”, ett filter som skulle innebära att endast tillåtna webbsidor visades. De föreslog detta i samarbete med organisationen Förbundet för ett säkert internet (Zykov 2017). Samma utskotts ordförande, Leonid Levin, låg bland annat bakom det initiativ som utvidgade lagen om utländska agenter att även omfatta juridiska personer som spred utländsk information (Tjevtajeva 2019). Han sitter också i styrande organ för ett antal kommissioner och olika organisationer som arbetar inom internetområdet.

Under den här perioden bildades också en rad organisationer med nära band till den verkställande makten. Ett exempel är Institutet för internetutveckling (*Institut razvitija internet*, IRI). Troligen ansvarade Vjatjeslav Volodin för idén när han var förste vice chef för Presidentadministrationen med ansvar för inrikespolitik.[16] Syftet när fonden skapades 2015 var att skapa en plattform för IT-företag och regeringstjänstemän, enligt German Klimenko, som var en av grundarna. En av de

[16] Volodin och hans medarbetare skapade en rad tankesmedjor och GONGO:er (Vendil Pallin & Oxenstierna 2017; Vendil Pallin 2017b).

verksamheter som IRI drev syftade till att främja material på internet som ”stärker civil identitet och andliga-moraliska värderingar hos ungdomar” (IRI ”Ob Institute razvitija interneta”; *RBK*, 20 februari 2017). Sedan Volodin lämnat Presidentadministrationen 2018 fick IRI svårare att hitta finansiering (Golitsyna 2017).

Regionalt samhällscentrum för internetteknologi (*Regionalnyj obsjtjestvennyj tsentr internet teknologij*, ROTsIT) kom till redan på mitten av 1990-talet och var en av grundarna av ett koordineringscentrum för domänerna .ru och .рф. Efter en period då organisationen tappade betydelse återlanserades den 2014. ROTsIT:s nya direktör, Sergej Grebennikov, deklarerade att organisationen skulle fortsätta att försvara internetanvändares intressen, men det skulle ske ”i samarbete med företag och staten, som kan omsätta internetanvändarnas idéer och förslag i verkligheten” (Zykov 2014). I organisationens styrelse ingick förutom Grebennikov dumaledamöterna Leonid Levin och Igor Asjmanov, företrädare för Media-Gvardija men också representanter från Roskomsvoboda (ROTsIT, ”Sostav upgravlenia”).

Cyberoperationer i och bortom Ukraina

Från och med 2014 attribuerades en rad cyberoperationer som sanktionerade eller direkt utförda av ryska myndigheter. Inte sällan blev Ukraina något av ett laboratorium för att utveckla cyberangrepp och det var där som Ryssland först inte bara tog sig in i utan också saboterade industriella styrsystem och lyckades slå ut elektricitetsförsörjningen i stor skala från 2016 (Greenberg 2019). Än mer uppmärksammade blev en rad cyberoperationer som kunde kopplas till försök att påverka val – inte minst intrånget i amerikanska demokratiska partiet inför presidentvalet 2016.

Den största ekonomiska skadan orsakades 2017 av *NotPetya*, en skadlig kod som initialt spreds i Ukraina men snabbt låste datorer över större delen av världen. Som alltid är attribuering av en cyberattack svår att göra. USA pekade 2018 ut FSB:s institut Kvant som en av de ansvariga bakom spridningen av viruset NotPetya och därmed kopplat till FSB (U.S. Department of the Treasury 2018). Ryssland nekade till all inblandning och hävdade att anklagelserna mot Ryssland ingick i en större plan för att försvaga och underminera Ryssland. Samtidigt var underlaget relativt gediget – för cyberförhållanden – för att dra slutsatsen att Ryssland faktiskt legat bakom flertalet av de cyberattacker som de har blivit utpekade som ansvariga för. Målen för cyberattackerna – alltifrån Nato och parlament i Europa till internationella antidopningsförbundet (*World Anti-Doping Agency*, WADA) och den holländska organisationen ansvarig för utredningen av MH17 – stämmer väl överens med ryska intressen; det har funnits spår som gör att IT-säkerhetsföretag kunnat fastställa att koden skrivits i en ryskspråkig miljö och under tider som sammanfaller med kontorstid i Moskva. I flera fall har dessutom framför allt amerikanska myndigheter gått så långt som att peka ut enskilda GRU-förband eller institut kopplade till FSB som ansvariga (*Council on Foreign Relations*; FireEye

2017; Greenberg 2019; U.S. Department of Justice 2018; U.S. Department of the Treasury 2018). Även Tyskland har attribuerat en cyberattack mot parlamentet, *Bundestag*, 2015 som utförd av GRU och dessutom utfärdat en arresteringsorder för en rysk GRU-officer, Dmitrij Badin (*Euronews* 2020).

Att Ryssland alltmer kom att förknippas med cyberoperationer utomlands fick också konsekvenser för ryska IT-säkerhetsfirmor internationellt. Redan 2015 utfärdade amerikanska myndigheter en instruktion om att Kaspersky Labs produkter skulle tas bort från amerikanska federala myndigheter. [17] Förtroendet för Kaspersky Lab sjönk snabbt även i andra länder i takt med att Ryssland pekades ut som liggande bakom en rad cyberattacker och då inte minst den mot demokratiska partiet i USA i samband med valet 2016. Trots olika åtgärder för att reparera förtroende fortsatte Kaspersky Labs vinst på den amerikanska marknaden att minska under 2018 (Jastrebova 2019; Soldatov & Borogan 2018: 22).

Sammanfattning av den tredje perioden

Annekteringen av Krim och det skärpta internationella politiska läget fick konsekvenser för rysk politik i allmänhet och så även för rysk cyberstrategi. Under denna period vann Säkerhetsrådets och FSB:s syn på området alltmer mark. Från mötet i Säkerhetsrådet i oktober 2014 fanns en mer tydlig cyberstrategi som omfattades av i stort sett hela byråkratin, liksom av ett nät av organisationer och internetbolag som stod den politiska makten nära. Även om en ny Informationssäkerhetsdoktrin kom först 2016 var det snarast vid mötet i Säkerhetsrådet den 1 oktober 2014 som den politiska ledningen gjorde en avdömning och justerade cyberstrategin. Resultaten i form av formella dokument, handlingsplaner och lagar lät heller inte vänta på sig efter oktober 2014. Ryssland fick under perioden en lag om skydd av kritisk informationsinfrastruktur, kontrollen och övervakningen över det som definieras som ett ryskt ”suveränt” internet ökade samtidigt som Ryssland också lyckades vinna viss mark internationellt för sin syn på informationssäkerhet. Ryssland vidtog även åtgärder för att minska sitt importberoende, men framgångarna här var mer blygsamma. Samtidigt ökade graden av koordinering väsentligt och de krafter inom byråkratin som tidigare företrätt en delvis mjukare cyberstrategi tystnade eller tog aktivt ställning för den hårdare linjen.

Under den här perioden blev också spänningarna mellan de olika målsättningarna som strategin rymmer tydliga. När balansen rubbades och ökad kontroll och övervakning blev de dominerande ledorden, fick det konsekvenser för t.ex. målsättningen att bygga en livskraftig inhemsk cyberindustri för att minska importberoendet. Den innovationssektor som tidigare fanns på området minskade och de stora företagen tilläts dominera på bekostnad av små- och medelstora. Ryska

[17] Detta skedde efter att israeliska regeringsanställda hackare upptäckte hackningsprogram från den amerikanska federala signalspaningsmyndigheten *National Security Agency* (NSA) på Kaspersky Labs’ datorer. Troligen hade en NSA-anställd använt Kaspersky Labs antivirusprogram på en hemdator (Nakashima 2017).

företag i branschen, t.ex. IT-säkerhetsfirmor, fick också svårare att expandera internationellt i takt med att alltfler uppmärksammade cyberoperationer attribuerades som utförda av FSB och GRU. Det var under den tredje perioden tydligt att Ryssland hade byggt upp en förmåga att genomföra cyberoperationer och att det var en del av strategin som den politiska ledningen varken kommunicerade öppet eller ens erkände existerade.

3.4 En fjärde period i vardande

Putins årliga linjetal i mars 2018 fick stora rubriker främst för uppräkningen av olika nya vapensystem som Ryssland redan hade eller snart skulle införliva i sin arsenal. Mindre uppmärksammat blev att Putin ägnade två tredjedelar av talet till att tala om behovet av att öka ekonomisk tillväxt och att förbättra levnadsvillkoren för befolkningen. Det skulle ske bland annat genom att hänga med i den internationella teknologiutvecklingen. Han utmålade det som en ödesfråga:

> Hastigheten för teknologiska framsteg accelererar kraftigt. Den ökar dramatiskt. De som lyckas surfa på den här vågen kommer att få ett långt försprång. De som inte lyckas göra det kommer att dras ned och drunkna i den här vågen. (Putin 2018)

Att utvecklingen av IT var en central del av detta blev tydligt när Putin undertecknade ett presidentdekret (nr. 204, 7 maj 2018) om tolv ”nationella projekt” för perioden 2019–2024 för att åstadkomma bl.a. ”ett genombrott i den vetenskapligt-teknologiska och social-ekonomiska utvecklingen” i Ryssland. Ett av de nationella projekten gick under rubriken ”Digital ekonomi”. Regeringsprogrammet ”Digital ekonomi” uppgraderades således till ett nationellt projekt och budgeten väntades växa avsevärt (Jastrebova 2018c). Till exempel lagen om ett suveränt internet som antogs 2019 visade sig också medföra betydande kostnader – en expertgrupp uppskattade dem till 134 miljarder rubel (Vendil Pallin 2019b: 5).

Rysslands AI-strategi

Ett av de teknologiområden där utvecklingen onekligen accelererade kraftigt var artificiell intelligens. Satsningen på AI var en av de största inom programmet ”Digital ekonomi” – totalt 125 miljarder rubel till 2024. I september 2019 flyttades ansvaret för AI inom programmet från Minkomsvjaz till Ministeriet för ekonomisk utveckling. En dragkamp om ansvaret följde liksom om finansieringen och vad som skulle prioriteras inom AI, en fråga som blev än mer akut med de förändrade ekonomiska förutsättningarna våren 2020 (Stepanova 2020). Månaden efter kom Rysslands första strategi på området, Nationell strategi för utveckling av AI för perioden till 2030 (2019). AI skulle integreras i redan gällande strategier och regeringsprogram, särskilt ”Strategin för att utveckla informationssamhället 2017–2030, programmet ”Digital ekonomi” och Strategin för vetenskaplig-teknisk utveckling”.

Målsättningen i AI-strategin från 2019 var att Ryssland ska vara ett av de ledande länderna på området till 2030. Det övergripande målet var att bidra till befolkningens välstånd och den nationella säkerheten samt att göra den ryska ekonomin konkurrenskraftig. Om Ryssland inte lyckades hålla sig framme inom AI, varnade strategin, skulle landet komma att ”släpa efter ekonomiskt och teknologiskt”. Förutom satsningar på inhemsk produktion av t.ex. mikroprocessorer pekade strategin på behovet av att Ryssland utbildade en kader av specialister på området. Något som skulle kunna bli gränssättande för huruvida Ryssland kan bli ledande inom AI är tillgången till stora datamängder. Ett helt avsnitt av strategin behandlade hur större mängder data skulle kunna bli tillgängliga och kvalitativt bättre att arbeta med. Samtidigt angav strategin att ryska statliga myndigheter och organisationer skulle få prioriterad tillgång till de nya moderniserade plattformarna för stora datamängder.

Generellt var strategin skriven som en önskelista över åtgärder för forskare och utvecklare inom AI-området. Frånvarande var aspekter som har att göra med nationell säkerhet, t.ex. i termer av hur AI kan användas av en motståndare för att undergräva politisk stabilitet i ett samhälle eller militära utvecklingsområden. Det var således en i huvudsak civil strategi för vetenskaplig utveckling inom ett enskilt teknologiområde. Av totalt sju federala projekt inom ramen för det nationella projektet ”Digital ekonomi” placerades tre hos Ministeriet för ekonomisk utveckling och fyra hos Ministeriet för digital utveckling (Krasnusjkina 2019). Den ryska nationella strategin för AI var dessutom närmare knuten till Strategin för ekonomisk-social utveckling till 2030 än till något av de viktigaste dokumenten som behandlar nationell säkerhet och listas på Säkerhetsrådets hemsida. Militär forskning på området pågår – och ligger eventuellt längre fram än den civila (Markotkin & Tjernenko 2020). Troligen utvecklas även koncept för hur AI kan användas inom underrättelse- och säkerhetstjänsternas ansvarsområden. Detta tycks dock ske i väl avskilda spår.

Som nämnts ovan tog Sergej Kirijenko, i egenskap av förste vice chef för Presidentadministrationen med ansvar för inrikespolitiska frågor, även över ansvaret för cyberfrågor 2018 (se s. 50). Kirijenko tycks inte ha uppfattat ny informationsteknologi som enbart ett hot mot rysk politisk stabilitet. Under hans egid lanserades satsningar på att öka mängden positiva nyheter på internet – något som Putin tillstyrkte när gruppen ”Ryssland – ett möjligheternas land” träffades i oktober 2019 (*Vedomosti*, 4 oktober 2019). Dessutom sjösatte Kirijenko en större satsning för att stärka den andliga-moraliska fostran bland unga även på internet (Parfenteva & Astafurova 2019).

En formulering i slutet av AI-strategin är värd att uppmärksamma. I det avsnitt som behandlar lagrummet stipulerade strategin att utvecklingen av AI kräver gynnsamma legala villkor för att få tillgång till data ”inklusive genom att skapa en experimentell legal regim”. En sådan experimentell yta föreslog Rysslands största bank, Sberbank, att man skulle skapa i Moskvaregionen med en särskild legal

regim. Bland de som skulle ingå i projektet fanns, förutom Sberbank, Presidentadministrationen och bolaget bakom Mail.ru (Kolesnikov 2019). Ryssland har visserligen egna ryska sociala nätverk som vKontakte och Odnoklassniki, men mängden data som underlag för AI-utveckling bleknar ändå vid en jämförelse med USA och Kina. Experimentet i Moskvaregionen var således ett försök att överkomma den nackdel som Ryssland har i termer av tillgång till stora datamängder. En av tankarna var att mer kvalitativa data skulle kunna kompensera bristen på kvantitet.

Enligt analytikern Konstantin Gaaze (2019) var ett av målen med projektet också att utveckla en ”rysk variant på Cambridge Analytica”. Genom tankarna bakom *nudge economics* skulle Moskvas invånare ’knuffas’ till att ta rätt beslut.[18] Stora datamängder kombinerat med AI-teknologi skulle kunna innebära nya möjligheter att kontrollera inrikespolitiken och opinionen genom att stimulera fram önskade beteenden och åsikter snarare än genom att främst förbjuda och blockera oönskade (Gaaze 2019). Försöken att blockera användningen av meddelandetjänsten Telegram under 2018 slutade, som noterats ovan, inte lyckligt för Ryssland och det har funnits tecken på att andra övervakningsåtgärder har varit alltför tids- och resurskrävande för att tillämpas fullt ut. Till exempel har flera analytiker uttryckt tvivel kring huruvida flera av de repressiva möjligheter som olika lagar har gett möjlighet till utnyttjas i praktiken. Såväl teknisk infrastruktur som analytiska resurser sätter gränser (se t.ex. intervju med Andrei Soldatov, Habersetzer 2020). De politiska övervakningsmöjligheter som AI utlovar är lockande för auktoritära länder generellt (Johnson 2019: 148) och Ryssland är troligen inte ett undantag här.

Ryssland i världen

Som nämnts ovan lyckades Ryssland 2018 vinna stöd för en FN-resolution som innehöll tretton ”internationella regler, normer och principer”, en slags uppförandekod på informationssäkerhetsområdet. Året därpå antogs dessutom det utkast till resolution om cyberkriminalitet som Ryssland lagt fram i FN:s Generalförsamling tillsammans med ytterligare 26 länder, bland vilka kan nämnas Angola, Belarus, Kina, Nordkorea, Syrien och Venezuela. De som brukar benämnas som

[18] *Nudge theory* förknippas främst med ekonomen Richard H. Thaler. Även beteendevetaren Daniel Kahnemans idé om två mänskliga system för beslutsfattande – ett snabbt och lättpåverkat (system 1), ett långsammare som tar in information och avväger den (system 2) – kan nämnas i sammanhanget. Idén är att små ”knuffar” kan uppmuntra till ett visst beteende (och då främst genom att påverka system 1). Det kan innebära att en kommun väljer att göra miljövänliga val ”förinställda”, t.ex. att kommuninvånare aktivt måste välja att lämna avfall osorterat medan default-valet är källsortering. Mindre tallrikar kan göra att en portion kan uppfattas som mer riklig och därmed uppmana till mindre mattintag. På internet skulle det t.ex. kunna vara att en användare i sitt flöde får intrycket att ”alla andra” i ett socialt nätverk gör ett visst val och därmed ”knuffas” i riktning mot att göra samma val. Det skulle också kunna vara att ryska sökmotorer är default på alla mobiltelefoner medan användare skulle bli tvungna att aktivt ladda ner utländska alternativ. Se t.ex. (Kahneman 2012: 20–21) och intervjun med Richard Thaler i *Modern Psykologi* (Hammarkrantz 2017).

västländer röstade i huvudsak emot dessa ryska initiativ. Ryssland har dock tillsammans med Kina blivit alltmer skickligt på att bygga allianser för att påverka internationella ramverk och det är tydligt att denna trend gäller även på cyberområdet. I sin nya roll som vice ordförande i Säkerhetsrådet gjorde också Dmitrij Medvedev klart att Ryssland avsåg att fortsätta att driva frågan om att minska USA:s dominans vad gäller internets globala styrning – pikant nog spred han filmen från Säkerhetsrådets videomöte genom sin Facebooksida (”Dmitrij Medvedev provel sovesjtjanije…”, 12 augusti 2020; *Facebook*, 12 augusti 2020). I början av 2020 fick Utrikesministeriet dessutom en Avdelning för internationell informationssäkerhet (Tjernenko 2020).

Covid-19

Många planer var under omstöpning pga. pandemin och den ekonomiska kris den medförde för Ryssland i maj 2020. Så även planerna för rysk digital utveckling. Av 231 resultat som skulle vara uppnådda inom nationella projektet ”Digital ekonomi” under första kvartalet 2020 hade endast sex stycken uppnåtts helt, 150 befann sig i olika stadier av genomförande medan ett regeringscentrum för utvärdering bedömde att så många som 66, dvs. en tredjedel, var omöjliga att genomföra. För nio resultat hade inte nödvändiga uppgifter för en bedömning lämnats in. Underrubriken ”Informationssäkerhet” utgjorde inget undantag – där hade tretton resultat ej uppnåtts. Regeringens utvärderingscentrum föreslog i maj 2020 att en rad projekt inom området ”Informationssäkerhet” skulle uteslutas ur ”Digital ekonomi” och 1,6 miljarder rubel omfördelas till andra projekt inom programmet. Dessa åtgärder hade helt enkelt blivit inaktuella och var inte längre efterfrågade av näringslivet (Tisjina 2020). Den globala pandemin skulle dock komma att påverka Rysslands satsning på digital utveckling mer generellt. I juli 2020 utfärdade Putin ett presidentdekret där ambitionen för de nationella projekten justerades väsentligt. För det nationella projektet på cyberområdet innebar det bl.a. att flera av de mål som tidigare skulle ha uppnåtts 2024 sköts fram till 2030 (Presidentdekret nr. 474, 21 juli 2020). Samtidigt var den digitala utvecklingen fortsatt prioriterad relativt många andra områden. I ett tal till nationen i juli räknade Putin upp åtgärder dels för att bekämpa pandemin, dels för att minska de ekonomiska följdverkningarna av pandemin. En viktig del i det ekonomiska stödpaketet blev en kraftig skatteminskning för IT-företag – enligt Putin till en av de lägsta skattesatserna i världen för IT-företag, jämförbar med de i Indien och Irland (Putin 2020).

Enbart skattelättnader skulle dock inte räcka för att skapa ett företagsklimat som gjorde möjligt för IT-industrin att bli ett draglok i ekonomin. I augusti 2020 publicerade Föreningen för data- och IT-företag, APKIT (*Assotsiatsija predprijatij kompjuternych i informatsionnych technologij*) ett öppet brev. I brevet pekade APKIT (2020) på motsättningen mellan den officiella målsättningen att skapa en bra miljö för IT-företagen samtidigt som företag blev föremål för husrannsakan, företagare greps och ständigt nya regleringar gjorde det allt svårare att bedriva

verksamhet. I APKIT ingår såväl ledande internationella som några av de största ryska IT-bolagen, alltifrån *Cisco* och Google till Kaspersky Lab och Yandex (dock ej bredbandsbolagen MTS, Vympelkom eller Megafon som ofta benämns de ”tre stora”, se nedan s.68). Brevet varnar för att företag kommer att flytta sin verksamhet utomlands:

> Det är välkänt att en konkurrenskraften inom en viss jurisdiktion inte bara beror på nivån på skattetrycket och omfattningen av statliga bidrag. Inte mindre utan snarare mer viktig är affärsverksamhetens säkerhet, investeringssäkerheten och företagarnas personliga säkerhet. … Det som nyligen har hänt uppfattas som ett hot, som gör att företagare inom den högteknologiska branschen ser rysk jurisdiktion som mindre vänlig och att det får dem att flytta sin verksamhet till andra länder. Därmed kan IT-företagare inte lugnt koncentrera sig på den digitala transformationen av landet; de känner sig inte övertygade om att deras verksamhet har någon framtid i Ryssland eller att ett gynnsamt företagsklimat kan skapas i landet. (APKIT 2020)

Förutom ekonomiska konsekvenser upplevde Ryssland en ökning av cyberkriminaliteten under pandemin. Den nye vice ordföranden i Säkerhetsrådet, Dmitrij Medvedev, uppgav i juli att cyberbrottsligheten hade ökat med 85 procent och pekade på detta som en av lärdomarna från pandemin (Krivjakina 2020; *Izvestija*, 9 juli 2020). Generellt stärkte pandemin de tendenser som redan kunnat iakttas (Persson 2020: 66). Risken för smitta blev en anledning att öka övervakningen i form av applikationer för mobiltelefoner och kameraövervakning. Det fanns inget datum för när denna skärpta kontroll av medborgarna skulle mattas av eller avslutas (Kovatjitj 2020a).

Även under pandemin pekades Ryssland också ut som liggande bakom cyberattacker t.ex. mot Ukraina (Lindahl et al. 2020: 8). USA, Storbritannien och Kanada anklagade också Ryssland – och då troligen FSB – för att ligga bakom cyberattacker i syfte att komma över forskningsunderlag mot institutioner som utvecklade virusvaccin. Ryssland nekade liksom tidigare till anklagelserna (Fox & Kelion 2020).

Sammanfattning av en begynnande fjärde period

Exakt startdatum för en fjärde kommer att vara lättast att sätta i efterhand. Perioden kommer att präglas av dels pandemin och dess efterverkningar, dels det teknikskifte som äger rum på cyberområdet. Båda dessa externa krafter kan påskynda trender och intensifiera tendenser som redan varit tydliga. Till exempel fanns under 2020 flera tecken på att övervakning och möjligheter för att kontrollera trafikflöden och innehåll skulle öka snarare än minska. Alltmer tydde också på att en ökande tendens till att ett ”splinternet” etableras globalt, med olika regionala internetsfärer som domineras av länder som Kina respektive USA. I denna dragkamp tydde allt 2020 på att Ryssland skulle fortsätta att göra val som placerar landet främst i Kinas cyberinflytelsesfär (trenden är dock inte entydig, se t.ex. Kovatjitj 2020b; Kluge 2020).

Ryssland har en fortsatt uttalad ambition att i ökad utsträckning bli självförsörjande vad gäller hård- och mjukvara. Till det ska läggas en strävan att etablera sig som en viktig spelare på framväxande teknologiområden med cyberapplikationer – inte minst inom AI-området. Liksom tidigare är de hinder som Ryssland behöver övervinna för att nå dit betydande – det rör sig om alltifrån svårigheter med att behålla viktig kompetens inom landet och ett bristande företagarklimat till att landet släpar efter jättarna på området – USA och Kina – vad gäller tillgång till stora mängder data.

Såväl pandemin som nya teknologier innebar nya möjligheter att övervaka landets medborgare. Möjligen kan det innebära att myndigheterna i mindre utsträckning än tidigare förlitar sig på att slå ned demonstrationer med våld. Snarare skulle framtidsambitionen då troligen vara att stävja missnöjesyttringar tidigt – innan de har nått gatan – genom en kombination av övervakning, trafikstyrning och skräddarsydda budskap.

4 Nyckelaktörer

4.1 Ledningen

Presidenten har en dominerande roll i Rysslands politiska system och hans roll blir än starkare när landet utvecklas i auktoritär riktning. Samtidigt finns det en diskussion om huruvida all makt är koncentrerad i Vladimir Putins händer eller om han är ett verktyg som måste förhålla sig till olika maktcentra inom rysk politik. Utan att fördjupa sig i denna debatt så är det möjligt att slå fast att Putin inte bestämmer allt, men att han ofta är den slutliga skiljedomaren när olika aktörer konkurrerar om inflytande. Ministerier och myndigheter kan bestämma rutiner och t.o.m. policy inom ett avgränsat politikområde, men när en intressekonflikt uppstår i systemet mellan olika aktörer – t.ex. som ett resultat av externa krafters inverkan – avgör presidenten konflikten och slår fast den framtida strategiska inriktningen för maskineriet som helhet. Alla inom systemet förväntas då stödja denna inriktning eller åtminstone synas göra det. Presidenten fördjupar sig troligen inte i alla detaljerna i varje strategi, men kan sätta ned foten när olika intressen står emot varandra.

Presidenten och de permanenta medlemmarna i Säkerhetsrådet har sista ordet vad gäller formulerandet av landets cybersäkerhetsstrategi, men deras analys baseras troligen på information som kommer från Säkerhetsrådets kansli, från viktiga enheter och personer inom Presidentadministrationen, FSB och Ministeriet för digital utveckling. Rysslands ledning spelar således en roll framför allt då en officiell strategi ska formuleras, men också när olika delar av det organisatoriska systemet förespråkar olika linjer eller den externa miljön gör det nödvändigt att anpassa strategin.

4.2 Organisatoriska krafter

Ett intrikat nät av enskilda tjänstemän, ministerier, myndigheter, statliga och privata bolag samt GONGO:er deltar i utarbetandet av cyberpolitik, bereder ny lagstiftning samt planerar och implementerar det som sammantaget är landets cyberstrategi. Den ryska regeringsbyråkratin och dess förgreningar ut i samhället, det som Mintzberg (1978: 94) benämner som ett organisatoriskt, operativt system består således av allt ifrån de institutioner som formulerar policy och myndigheter som lägger upp konkreta planer för hur policyn ska förverkligas till halvofficiella organisationer som driver på konkret lagstiftning och stöder regeringens politik.

Det organisatoriska krafterna, dvs. byråkratin i vidare mening, är långt ifrån monolitiska utan rymmer interna maktkamper och intressekonflikter. Det finns avsevärda nyansskillnader mellan olika ministerier och myndigheter vad gäller hur de söker påverka, uttolka och förverkliga cyberstrategin (Nocetti 2015: 118). Till

dessa ska läggas den kamp om inflytande som ständigt pågår mellan olika ministerier och myndigheter, inte minst säkerhetstjänsterna som GRU, FSB och FSO (se även Giles 2011: 51ff; Soldatov & Rochlitz 2018: 84).

Det är lätt att lockas att dra slutsatsen att ett på det stora hela hierarkiskt system arbetar som en effektiv organism. Så är inte alltid fallet och det som i förstone kan synas som ett mindre beslut i en del av organisationen kan få stora återverkningar i systemet som helhet – i synnerhet när det finns en brist på transparens och en oberoende granskning av myndigheter är nästan helt satt ur spel (för en diskussion om detta angående, se Bartles 2016: 5). När en myndighet driver igenom en lagändring om t.ex. ökad övervakning av internet kan detta bidra till att underminera det arbete som andra delar av systemet bedriver inom ramen för cyberstrategin, t.ex. i form av flaskhalsar när all digital trafik tvingas passera visa noder för övervakning och eventuell blockering. När ryska cyberoperationer attribueras får det också negativa konsekvenser för rysk IT-industris möjligheter att vinna marknadsandelar internationellt. Sammantaget kan det leda till att cyberstrategin som helhet inte realiseras.

Central byråkrati

Vissa delar av den ryska regeringsbyråkratin framstår som viktigare än andra. Det ryska Säkerhetsrådet har en viktig roll när beslut ska fattas, men det är dess kansli som utför det praktiska arbetet med att formulera och koordinera landets cyberstrategi. En del av detta arbete har gjorts genom landets två informationssäkerhetsdoktriner, där en av Säkerhetsrådets vice sekreterare med ansvar för informationssäkerhet, har koordinerat processen. Indelningen i avdelningar i Säkerhetsrådets kansli framgår inte längre av dess förordning och sådan information presenteras heller inte på dess hemsida. Det har dock länge funnits en avdelning för informationssäkerhet (Vendil 2001) och 2018 listades medlemmarna i en organisatorisk kommitté för den årliga konferensen Infoforum där Sergej Bojko ingår som chef för Avdelningen för säkerhet inom informations- och informationsteknologiområdet (se Appendix Tabell 3; se även *Nezavisimaja gazeta*, 18 juli 2018 och Thomas 1998: 158). Här bereds sannolikt många av de policyförslag och strategiska dokumenten som inbegriper temat cybersäkerhet. Det var också Säkerhetsrådets kansli som tog initiativet till Infoforum som samlar de viktigaste företrädarna för det organisatoriska systemet som ansvarar för informationssäkerhet.

Säkerhetsrådets Interdepartementala kommission för informationssäkerhet träffas minst en gång var tredje månad och har som uppgift att ta fram rekommendationer och analyser som underlag för politiska beslut som berör informationssäkerhet (Förordning Säkerhetsrådets Interdepartementala kommission för informationssäkerhet, nr.560, 6 maj 2011). Vilka som ingår i kommissionen ger en god bild av vilka som är nyckelinstitutioner när rysk politik på cybersäkerhetsområdet utarbetas. De två vice ordföranden för kommissionen är en vice minister för digital

utveckling respektive en chef för ett FSB-direktorat. Kommissionens sekreterare anges som ”avdelningsschef” inom Säkerhetsrådets kansli och det rör sig då sannolikt om chefen för säkerhet inom informations- och informationsteknologiområdet, Sergej Bojko (Presidentdekret nr 1711, 26 maj 2015).

Tabell 2. Vice sekreterare med ansvar informationssäkerhet i Säkerhetsrådet 2000–2020

Namn	Period	Bakgrund
Vladislav Sjerstiuk	maj 1999 – maj 2004 (1:e vice sekreterare) sep 2004 – dec 2010 (ass. sekreterare)	KGB, FAPSI
Nikolaj Klimasjin	okt 2010 – juni 2011 (ass. sekreterare) juni 2011 – dec 2013 (vice sekreterare)	FSB, chef vetenskapliga-tekniska tjänsten (tf chef FAPSI kort 2003)
Sergej Burgalev	Dec 2013 – 2017 (vice sekreterare)	FSB
Oleg Chramov	Jan 2017 – (vice sekreterare)	FSB

Källor: Engqvist 2020: 8; Informationssäkerhetsinstitutets hemsida (http://www.iisi.msu.ru/ISforum/committees/, http://www.iisi.msu.ru/Main(eng)/bayern2013/); Säkerhetsrådets hemsida (http://www.scrf.gov.ru/news/allnews/863/, http://www.scrf.gov.ru/news/allnews/1068/, http://www.scrf.gov.ru/news/allnews/663/); Vendil 2001.

Sjerstiuk var också drivande bakom att Informationssäkerhetsinstitutet vid Moskvauniversitetet kom till 2003 och det blev tidigt en kanal för att föra fram rysk syn på informationssäkerhet internationellt, t.ex. vid de årliga konferenserna som institutet anordnar i Garmisch-Partenkirchen i Tyskland och i bilaterala möten med europeiska tjänstemän och experter (Nocetti 2015: 119).

Federala säkerhetstjänsten är också en viktig organisatorisk kraft vad gäller att forma rysk cyberstrategi. Att internet framför allt är ett hot tycks vara ett djupt rotat synsätt inom FSB liksom det tidigare tycks ha varit inom FAPSI (Giles 2012: 73). FSB tog över det direktorat som ansvarat för signalspaning inom FAPSI 2003. Direktoratet ombildades till att bli FSB:s 16:e Centrum för radioelektronisk spaning mot kommunikationsnätverk (Giles 2011: 53; Grebennikov 2019). Förutom signalspaning är detta centrum ansvarigt för att driva det system för övervakning av internet som benämns SORM (System för operativa förundersökningsåtgärder) (Estonian Foreign Intelligence Service 2019: 55). Som en del i den lagstiftning som reglerar SORM är alla internetleverantörer skyldiga att installera FSBs utrustning för internetövervakning på varje server och det är bara FSBs personal som har behörighet att befatta sig med utrustningen. Det innebär att FSB:s 16:e Centrum samlar in information om den ryska befolkningens kommunikation och alla som använder en server som fysiskt befinner sig på ryskt territorium. Möjligen är detta centrum ansvarigt också för FSBs operationer på internet utanför landets gränser (Grebennikov 2019; se även Giles 2011: 55). FSB har aktivt sökt

rekrytera unga personer som är duktiga på cyberområdet t.ex. vid tävlingar för unga programmeringar och hackare (Turovskii 2017).

FSB har också fått successivt ökade befogenheter vad gäller att bekämpa cyberhot. Centrum för informationssäkerhet (*Tsentr informatsionnoj bezopasnosti*, TsIB) lyder under Kontraspionaget inom FSB och tidigare hette Direktoratet för data- och informationssäkerhet (Soldatov & Borogan 2018: 17). TsIB undersöker cyberbrott och ansvarar för skydd av datornätverk och detta inkluderar den hantering som sker vid e-handel och olaglig hantering av persondata. Det innebär även troligen att FSB:s TsIB är något av en samordnare, en ”kurator”, för ryska IT-säkerhetsföretag som Kaspersky Lab och Group-IB (Kolomytjenko 2017). TsIB blev dock inte ansvarig enhet för att skydda Ryssland mot cyberattacker när GosSOPKA (se även s. 41) blev den huvudsakliga processen för att skydda landets informationsinfrastruktur. Det kan ha varit kopplat till att åtminstone två officerare från TsIB greps och anklagades för landsförräderi året innan. Detta ansvar har istället ett särskilt centrum inom FSB, Nationellt koordineringscentrum för datorincidenter (NKTsKI) som bygger på enheter ur FSB:s Vetenskapligt-tekniska tjänst (Rubnikovitj, Zjukova & Barinov 2018). Det är också representanter från den Vetenskapliga-tekniska tjänsten inom FSB som ingår i Regeringskommissionen för digital utveckling (Regeringsinstruktion nr. 1187-r, 30 april 2020).

FSB är således en av de mest inflytelserika myndigheterna vad gäller utformandet av landets cyberstrategi, men också hur den förverkligas i termer av säkerhetsåtgärder och offensiva operationer. Att FSB har denna roll är delvis historiskt betingat. KGB hade en nyckelroll på sin tid inom såväl kryptering som avlyssning av kommunikationer, inklusive telefontrafik inom landet. Dessa ansvarsområden togs över och utvecklades i takt med att ny teknologi infördes av KGB:s arvtagare – främst FAPSI och säkerhetstjänsten som med tiden blev FSB (Soldatov & Borogan 2015: 45ff, se även s. 3636).

Den Federala tjänsten för teknisk och exportkontroll är en myndighet som är underordnad Försvarsministeriet, men får sina instruktioner direkt från presidenten. I dess mandat ingår att koordinera, organisera samarbete och utöva särskilda kontrollfunktioner inom teknisk säkerhet, inklusive cybersäkerhet. Att övervaka säkerheten inom ICT-system som är kritiska för nationell säkerhet är en av FSTEK:s huvuduppgifter. Myndigheten ska även förhindra teknisk underrättelseinhämtning samt säkerställa att hemlig information inte läcker ut, förvanskas eller förstörs genom tekniska kanaler (FSTEK ”Polnomotjija”; Thomas 1998: 164). Som framgått ovan, fick FSB och FSTEK huvudansvaret för skydd av kritisk informationsinfrastruktur. FSTEK har närmast en funktion av tillsynsmyndighet, medan FSB ansvarar för operationella tillämpningen av lagstiftningen (Kari 2019: 44ff).

Ytterligare en myndighet, den Federala skyddstjänsten (FSO) spelar en viktig roll inom rysk cybersäkerhet. En av FSOs största enheter är Tjänsten för specialkommunikation och information (*Sluzjba spetsialnoj svjazi i informatsii*, SSSI), som

FSO tog över från FAPSI 2003. Denna tjänst förser regeringen och dess myndigheter med säkra kommunikationer. Dess officerare rekryteras framför allt från FSB, MVD och de Väpnade styrkorna. FSO har dessutom två institutioner för högre utbildning som utbildar specialister på områdena IT och IT-säkerhet. Förutom att förse regeringen med säkra kommunikationer, har FSO även centra för att övervaka media och den allmänna opinionen (Nikolsky 2013: 35–8, Pertsev & Solopov 2020) och FSO:s upphandling 2014 av program för att automatiskt övervaka blogginlägg tyder på att FSO även kartlägger aktivitet på internet.

Inrikesministeriet spelar en mindre framträdande roll på cyberområdet. Inom MVD är Huvuddirektoratet för att bekämpa extremism som är aktivt även vad gäller att bekämpa extremism på internet (MVD, ”Glavnoje upravlenije po…”). Vidare är Direktorat K är ansvarigt för att bekämpa cyberbrottslighet i form av cyberattacker, nätbedrägerier, distribution av barnpornografi och andra brott på internet (MVD, ”Upravlenije ’K’ MVD Rossii”). Den exakta uppdelningen av ansvaret på detta område mellan FSB och MVD är oklar, men MVD har väsentligt mindre att säga till om än FSB på cyberområdet. MVD har dessutom ett Allryskt centrum för vidareutbildning av MVD-anställda (VIPK). Att detta institut spelar en roll inom cybersäkerhet indikeras av att den före detta chefen för VIPK är en av ordförandena för Infoforums organisationskommitté (se Appendix Tabell 3).

Vissa inflytelserika organisationer lyser snarare med sin frånvaro i cybersammanhang. Till exempel tycks Nationalgardet ha mycket lite inflytande över hur rysk cyberstrategi formas och implementeras. Chefen för Nationalgardet är visserligen ständig medlem av Säkerhetsrådet, men det finns ingen från myndigheten representerad i Säkerhetsrådets interdepartementala kommission för informationssäkerhet. Bristen på cyberinflytande kan eventuellt förklaras med att Nationalgardet bildades som självständig myndighet först 2016, men det är ändå notabelt att det är bara MVD och FSB som deltar i arbetet med att samla in data från t.ex. sociala medier inför stora demonstrationer (Rozjdestvenskij & Pintjuk 2019). Hittills har således Nationalgardet inte spelat någon framträdande roll när cyberfrågor debatteras och politik utformas.

Inom regeringen hade vice premiärminister Maksim Akimov från maj 2018 ett koordinerande ansvar för IT-frågor. Han var även tillsammans med ministern för digital utveckling ansvarig för det nationella programmet ”Digital ekonomi” fram till regeringsombildningen i januari 2020. Inom regeringens kansli finns en Avdelning för Informationsteknologi och kommunikationer, som leddes av Vladislav Fedulov 2012–2020. Han var även medlem av organisationskommittén för Infoforum (se Appendix Tabell 3). Fedulov blev vice minister för ekonomisk utveckling efter regeringsombildningen i februari 2020. Programmet ”Digital ekonomi” är främst en övergripande strategi för att befrämja digital utveckling och därmed även rysk ekonomisk tillväxt och troligen tog Fedulov med sig en del av den portfölj han haft som chef för Avdelning för Informationsteknologi och kommunikationer till sin nya post.

Ministeriet för digital utveckling (Minkomsvjaz) har en viktig roll. Det ansvarar för utformning av policy och implementering inom informationsteknologi, elektronisk kommunikation, masskommunikation, massmedia och hantering av persondata (Minkomsvjaz Rossii, ”Obsjtjaja informatsija”). Som nämns ovan tilldelades ministern för detta ministerium tillsammans med en vice premiärminister huvudansvaret för nationella programmet Digital ekonomi (Minkomsvjaz 2017) när det sjösattes.

Myndigheten Roskomnadzor (Federala tjänsten för övervakning av kommunikationer, informationsteknologi och massmedia) lyder under Minkomsvjaz. I Roskomnadzors uppdrag ingår att övervaka internet. Till exempel administrerar denna myndighet de så kallade svarta listorna över blockerade internetadresser. Representanter från Roskomnadzor ingår både i Säkerhetsrådets interdepartementala kommission för informationssäkerhet och i organisationskommittén för Infoforum (se Appendix Tabell 3 och Tabell 4). Roskomnadzor har dessutom vuxit som myndighet och fått mer vittgående befogenheter inte minst från och med period två i genomgången ovan. I och med lagen om ett suveränt internet kommer dess befogenheter att utökas ytterligare.

Utrikesministeriet har en relativt väl avgränsad roll i arbetet med informationssäkerhet. Det arbetar framför allt för att Rysslands förslag till ett internationellt avtal om informationssäkerhet ska få gehör utomlands. Sedan 2014 är Andrej Krutskich särskilt presidentsändebud för frågor inom internationellt samarbete inom informationssäkerhetssfären. Först i februari 2020 skapades en enskild avdelning med ansvar för internationell informationssäkerhet. Samtidigt torde frågor som berör informationssäkerhet även hanteras av avdelningar som stöder Ryssland inom t.ex. FN, *Collective Security Treaty Organization* (CSTO) och Osse liksom av regionala avdelningar då bilaterala relationer berör cyberfrågor. Utrikesministeriet tycks ha en begränsad roll i formulerandet av rysk cyberstrategi. Snarare stöder ministeriet genomförandet inom en bestämd del av rysk cyberstrategi: att skapa bättre internationella förutsättningar för rysk cybersäkerhetsstrategi.

Försvarsministeriet ansvarar för informationssäkerhet på försvarsområdet. En vice försvarsminister leder arbetet med att formulera en enhetlig militär-teknisk policy för att utveckla informations-, digitala och kommunikationsteknologier inom Försvarsministeriet och samordnar verksamheten inom innovationspolitik, vetenskaplig forskning, utveckling av nya teknologier, informations- och kommunikationsteknologier samt robotik (Potechina 2015). Försvarsministeriets har vetenskapliga forskningsinstitut (*nautjno-issledovatelskije instituty*, NII) som utvecklar förmågor och teknologier för de Väpnade styrkorna inom området informations- och kommunikationsteknologi. Centrumet för särskilda utvecklingsprojekt (*Tsentr spetsialnych razrabotok*) är troligen en av de viktigaste institutionerna under

Försvarsministeriet som specialiserar sig på informationssäkerhet och informationskrigföring (Försvarsministeriet, ”Tsentr spetsialnych razrabotok”; *Meduza – podcast* 2018).

Inom Försvarsministeriet finns vidare olika direktorat som ansvarar för telekrig, signalskydd, propaganda och skydd mot propaganda. Samtliga har en roll inom Rysslands informationssäkerhet och offensiva planering på informationsområdet. Till exempel har Generalstabens 8:e direktorat, Tjänsten för sekretesskydd, en viktig roll i att certifiera IT-utrustning som får användas inom Väpnade styrkorna (Zykov & Ramm 2016). Dokumentet från 2011, Konceptuell syn på Ryska federationens Väpnade styrkors verksamhet i informationsrymden, understryker under rubriken ”Laglighet” med hänvisning till dåvarande militärdoktrinen att Väpnade styrkorna kan användas utomlands endast enligt presidentbeslut och fortsätter: ”Denna paragraf bör utsträckas till att gälla även användningen av Väpnade styrkorna i informationsrymden.” Det indikerar att det åtminstone 2011 fanns en gräns mellan vilka cybermedel som Väpnade styrkorna kunde använda i fred respektive i krig.

GRU:s uppgift är att samla in utrikes underrättelser om militära, militärpolitiska, militärekonomiska och militärvetenskapligt-tekniska frågor. GRU utbildar och övar specialförband samt genomför underrättelseoperationer och annan aktivitet för att ”främja en framgångsrik implementering av Ryska Federationens försvars- och säkerhetspolitik” (Försvarsministeriet, ”Glavnoje upravlenije Generalnogo Sjtaba”; Turovskij 2018). Som framgår ovan, finns det goda grunder för att anta att GRU har bedrivit cyberoperationer gentemot utlandet. Troligen är GRU:s förmåga till cyberoperationer dock en strategisk resurs. Avancerade cyberoperationer är av en rad skäl som regel inte en förmåga som militära förband på taktisk eller ens operativ nivå förfogar över (Schulze 2020).

Övervakning av internet kostar pengar och att stimulera innovationer på cyberområdet eller stimulera egen tillverkning av hårdvara får ekonomiska konsekvenser. Det gör även ministerier som Finansministeriet och Ministeriet för ekonomisk utveckling till viktiga instanser när rysk cyberstrategi formas. För varje lagförslag som läggs fram ska konsekvenser i termer av ökade utgifter från federala budgeten specificeras. Som regel anger förslagsställarna att förslaget inte innebär ökade utgifter och i remissgången tenderar Finansministeriet och Ministeriet för ekonomiskt utveckling att påpeka att förslaget faktiskt innebär kostnader – antingen direkt i termer av att budgeten belastas eller indirekt genom att marknaden förväntas absorbera kostnaden. Även om ökad kontroll och säkerhet oftast vinner i termer av att lagförslaget går igenom är de ekonomiska ministerierna och myndigheternas invändningar ändå en del av processen och inte sällan modifieras förslaget eller så måste besvärliga omfördelningar ske inom federala budgeten. Genomgången ovan tyder dock på att de ekonomiska ministeriernas inflytande gradvis minskade från period två. Möjligen kommer de att få en större roll inom utvecklingen av AI som en del av ett generellt försök att öka Rysslands ekonomiska tillväxt.

Parlamentet

Parlamentets roll i systemet är reducerad till att anta nödvändig lagstiftning och att stödja regeringens politik i uttalanden. På cybersäkerhetsområdet har en skara dumaledamöter och senatorer varit aktiva i att föreslå skärpningar av lagar och förordningar. Parlamentet har inte en granskande och balanserande roll i det politiska systemet. När ett lagförslag som berör cybersäkerhet väl har lanserats tenderar det att antas i tre omröstningar med endast smärre ändringar, nästan hur dåligt förberett och koordinerat det än är. Det finns utskott och kommissioner för medie- och informationsfrågor, men de utskott och kommissioner som har generell säkerhet som huvudområde är minst lika aktiva på cyberområdet. Allt fler av lagförslagen på cyberområdet kommer också från Duman; en utveckling som tog fart under den tredje perioden. Flera utskott är verksamma, t.ex. Utskottet för informationspolitik och för säkerhet och korruptionsbekämpning. Det är oklart i hur stor utsträckning det rör sig om egna initiativ till nya och ändrade lagar och hur ofta det rör sig om mer eller mindre beställningar som i själva verket kommer från ministerier och myndigheter som t.ex. FSB eller från Presidentadministrationen.

Även i den första kammaren, Federationsrådet, har senatorer i allt högre grad verkat för ökad statlig kontroll över internet genom ny lagstiftning, men också genom att aktivt stödja förd politik framför allt sedan annekteringen av Krim. Den cyberstrategi som Federationsrådet utarbetade och som landets internetföretagare hade varit positiva till, försvann från agendan under den tredje perioden.

Internetföretag

De stora internetföretagen har föga anledning att öppet kritisera regeringen. Inte ens kontroll- och övervakningsåtgärder som innebär betydande kostnader för näringslivet brukar i slutänden drabba de stora företagen. De har direktkanaler in i regeringen och vet att de sannolikt kommer att kompenseras genom att tilldelas lukrativa statliga kontrakt, genom subsidier eller helt enkelt genom att de tillåts att dominera ICT-marknaden. Det här gör det besvärligt för små och medelstora företag att ta sig in och överleva på marknaden. De har ofta inte de resurser som krävs för att leva med ny kostsam reglering samtidigt som de inte har de kontakter som krävs för att vinna statliga anbud. Det här är ingalunda unikt för internetbranschen utan gäller på de flesta affärsområden. Unikt för internetföretagen är dock dels att sektorn var relativt dynamisk och fri från regleringar fram till period två, dels att mängden nya pålagor och begränsningar vuxit snabbt särskilt från och med period tre.

I Ryssland brukar man hänvisa till de största bredbandsbolagen som ”Big Three” eller ”Big Five” lite beroende på vilka segment av IT-marknaden som beskrivs. Framför allt används benämningen ”de stora tre” för de privata bolagen MTS, Megafon och Vympelkom (Kolomytjenko 2019b).

Megafon ägs av holdingbolaget USM som i sin tur kontrolleras av Alisjer Usmanov. Han har gjort en förmögenhet inom ICT-branchen och står Kreml nära. Hans företag Mail.ru tog över sociala nätverket VKontakte från Pavel Durov 2014 (Vendil Pallin 2017a: 24) och äger även de sociala nätverken Odnoklassniki och *Moj mir* samt har en ägarandel i betalningstjänsten *Qiwi*. Under 2018 valde Usmanov att lämna över kontrollen över Mail.ru ”till en yngre generation”, men media spekulerade i att det var ett schackdrag för att skydda företaget i händelse av ytterligare sanktioner som skulle kunna drabba Usmanov (*BBC News – Russkaja sluzjba*, 22 oktober 2018).

Telecomföretaget Vympelkom ingår i holdingbolaget VEON, som kontrolleras av *Alfa-grupp*, som i sin tur kan kopplas till, bland andra, Michail Fridman. Han är en av få så kallade oligarker som behållit en inflytelserik position i ryskt näringsliv sedan 1990-talet. De som på olika sätt motsatte sig att Putin stärkte kontrollen över såväl politik som näringsliv – t.ex. Boris Berezovskij, Michail Chodorkovskij och Vladimir Gusinskij – tvingades alla lämna landet och ge upp större delen av sina affärsintressen i Ryssland.

MTS (*Mobilnye TeleSistemy*), slutligen, ägs av företaget *Sistema*, ett konglomerat som i sin tur ägs av Vladimir Jevtusjenkov. Han placerades i husarrest på grund av en konflikt med Igor Setjins oljebolag *Rosneft* under en period, men allting tyder på att Sistema tilläts fortsätta sin verksamhet och då inte minst på internetområdet. Det finns också tecken på att MTS samarbetar med säkerhetstjänsten (Turovskij 2016).

Om man studerar de största spelarna på cyberområdet finns dock all anledning att även inkludera även de statliga bolagen Transtelekom och Rostelekom och då talar man om ”de fem stora” (se t.ex. Franke & Vendil Pallin 2012: 35; Kolomytjenko 2019b). I Sovjetunionen hanterade ett ministerium kommunikationer inklusive infrastrukturen, men det ändrades 1990 då Rostelekom bildades och tog över fjärrkommunikation. Sedan dess har Rostelekom fått en nyckelroll inom ICT. Rostelekom blev en central aktör i alltifrån utbyggnaden av fibernät i Ryssland till att bygga de servrar som behövs enligt Jarovaja-lagstiftningen om lagring av trafikdata och trafikinnehåll. Transtelekom förfogar över Rysslands största nät av fiberoptisk kabel och är en av de viktigaste bredbandsleverantörerna. Företaget är ett dotterbolag till det statliga bolaget Ryska järnvägar. En stor andel av Rysslands kabelnätverk löper längsmed med järnvägsspåren. Inom ramen för delprojektet ”Informationsinfrastruktur” inom det nationella projektet ”Digital ekonomi” ska Transtelekom bland annat bygga ut tillgången till bredband i landets regioner. Företaget kontrollerar den fiberoptiska kabel som går under namnet *Eurasia Highway*. Den löper över kontinenten och förbinder Ryssland med i stort sett samtliga grannländers nät (se t.ex. *Kommersant*, 17 oktober 2019).

De stora telekom- och IT-företagen har i mångt och mycket blivit en del av den organisation som formar och implementerar rysk cybersäkerhetstrategi. De föreslår lagstiftning (se t.ex. Kolomytjenko & Balasjova 2018) och deltar aktivt i

att kontrollera internet i Ryssland. De flesta stora företag var vid slutet av period tre antingen statligt ägda eller ägda av personer som står Kreml nära (Vendil Pallin 2017a). Branschen som helhet domineras av stora spelare – ömsom i konkurrens, ömsom i nära samarbete med varandra. *Rostech* är t.ex. en statlig jätte på teknikområdet. Dess officiella namn är ”Statliga företaget för produktion och export av högteknologisk industriell produktion” och det kontrollerar cirka 700 företag, främst inom försvarsindustrin och andra strategiskt viktiga branscher. Dess generaldirektör, Sergej Tjemezov, står Putin nära sedan tiden då de båda arbetade för KGB i Östtyskland på 1980-talet. Rostech samarbetar bland annat med Alisjer Usmanovs holdingbolag USM för att tillhandahålla IT-säkerhetslösningar (Jastrebova 2018a).

Även de företag som bildades som oberoende uppstickare har alltmer tvingats bli mer följsamma. Yandex var tidigt ute med att presentera ryska lösningar för sökningar på internet och mutade snabbt in den ryska marknaden. Sedan dess har Yandex utvecklats till ett internetimperium som ägs av ett moderbolag som är registrerat i Holland och som handlas på den elektroniskt baserade börsen Nasdaq. Grundaren, Arkadij Volozj, hade 2020 fortfarande en aktiepost som gav honom nästan 50 procent av rösterna i företaget (*RBK*, 29 juli 2019). Yandex har dock betalat ett pris för sin framgång i termer av minskad självständighet gentemot ryska staten. Yandex’ aktiekurs har de senaste åren oscillerat i takt med att Putin gjort ett positivt eller negativt uttalande om företaget.

Flera av Rysslands IT-säkerhetsföretag har blivit framgångsrika även internationellt. Det mest kända, Kaspersky Lab, har dock drabbats av att Ryssland pekats ut som liggande bakom cyberattacker och rykten om Kasperskys kontakter med FSB. Det ryska företaget Group-IB var visserligen mindre omgivet av rykten om band till FSB, men är som alla IT-säkerhetsfirmor i Ryssland beroende av att ha goda kontakter med ryska myndigheter för att alls kunna bedriva en framgångsrik verksamhet där (Gershikov 2018).

Att expandera internationellt och samtidigt bibehålla goda kontakter med ryska myndigheter blev från och med period tre en allt besvärligare balansgång för ryska internetföretag generellt. De ökade kraven på statlig kontroll inom Ryssland fick konsekvenser både för hur verksamheten kunde bedrivas och för företagens rykte internationellt. Att länder attribuerade en rad aggressiva cyberattacker som ryska spädde på denna problematik för ryska internetföretag. Det brev som APKIT publicerade i juli 2020 pekade också på hur den del av ryska cybersäkerhetsstrategin som syftar till att göra Ryssland till ett land där IT-branschen bidrar till landets tillväxt och dessutom mindre beroende av import, kom i direkt konflikt med statens ständigt ökade kontroll- och övervakningsbehov.

Företagsorganisationer och GONGO:er

Det finns en rik flora av företagarorganisationer, branschorganisationer inom IT-sektorn i Ryssland. Vissa av dessa samarbetar mycket nära med regeringen eller

har t.o.m. tillkommit på regeringsinitiativ; andra har en något mer fristående roll. Dessutom finns organisationer som försöker ge intryck av att vara en del av civilsamhället, men som regeringen utövar ett betydande direkt eller informellt inflytande över, ofta refererade till som GONGO:er (*government-operated non-governmental organizations*).[19] Vissa av dessa organisationer är så pass intimt sammankopplade med regering och myndigheter att de föreslår ny lagstiftning och policy; deras företrädare deltar i regeringsprogram och de levererar idéer om hur övervakningen av internet kan stärkas. Gränsen mellan vad som är en förlängd arm av regeringen och en genuin lobbyorganisation eller frivilligorganisation är inte alltid klar och kan variera över tid. En rad organisationer har gradvis anpassat sitt arbetssätt till de ändrade politiska förutsättningarna.

I början av andra perioden vidtog regeringen mått och steg för att öka sitt inflytande även över mindre företag och innovationsklimatet inom internet- och telekombranschen. En viktig åtgärd bestod i att etablera den fond för internetinitiativ, FRII, som snabbt blev den viktigaste källan till riskkapital inom rysk IT-industri (se period två, s. 41). Det är en verklighet som samtliga lobbyorganisationer behöver förhålla sig till.

Bland de viktigaste branschorganisationerna återfinns Ryska föreningen för elektronisk kommunikation (*Rossijskaja assotsiatsija elektronnych kommunikatsii*, RAEK) som bl.a. sammanställer rapporter om RuNets utveckling inom olika internetsegment, ordnar konferenser och delar ut priset ”RuNet Premium”. Ett av projekten som har fått det priset är *Aktivnyj grazjdanin*, som tagits fram för Moskva stad. Sergej Plugatarenko utsågs till direktör för RAEK 2006, men även German Klimenko har varit en av dess nyckelpersoner (Turovskij 2016). RAEK är bara en av flera branschorganisationer, men kan räknas bland de mest inflytelserika. Det finns dessutom en företagarförening som företräder hårdvarutillverkare, RATEK, och Media-Kommunikationsförbundet (*Medija-kommunikatsionnyj sojuz*, MKS) som förenar de viktigaste media- och telekomföretagen som MTS, VympelKom, TransTeleKom, Rostelekom, Megafon and Gazprom-Media Holding, för att nämna några ytterligare exempel. En viktig branschorganisation är också APKIT, som räknar några av de mest inflytelserika ryska IT-företagen bland sina medlemmar, men också internationella företag verksamma i Ryssland. Samtliga dessa föreningar företräder branschens intressen – något som inte sällan innebär att de behöver ha goda förbindelser med regeringen, delta i kommissioner och samarbetsorgan.

Flera organisationer som är verksamma inom cyberområdet kan räknas som regeringens förlängda arm snarare än som frivillorganisationer. Bland dessa kan nämnas Klimenkos organisation Institutet för internetutveckling men också Förbundet för ett säkert internet, vars ”Cybermilis” (liksom även Enade Rysslands Mediagarde) var som viktigast under andra och i början av den tredje perioden.

[19] Frivilligorganisationer benämns ofta *non-governmental organisations*, NGO:er.

Regeringen kunde använda dessa GONGO:er för att ge intryck av att olika repressiva åtgärder tillkom spontant genom initiativ från samhället. Samtidigt var förekomsten av en ”milis” på internet en del i en ökad kontroll över internetanvändare och ett försök att mobilisera unga i statligt styrd aktivism på nätet.

5 Nyckelaktörer och rysk cyberstrategi

President Vladimir Putin är central i ryskt beslutsfattande. Genomgången ovan av beslutsfattande om rysk cyberstrategi illustrerar dock att påståendet att han bestämmer allt bör nyanseras väsentligt. Fördelningen av ansvar och befogenheter inom det politiska systemet har konsekvenser – för enskilda personer och organisatoriska enheter i systemet samt för hur politiken utformas och implementeras och resurser fördelas. Genomgången av de olika interna och externa krafterna samt hur den politiska ledningen dömt av under olika perioder visar dessutom på hur viktiga brytpunkter kan identifieras. För varje brytpunkt har den del av systemet som domineras av Säkerhetsrådet, FSB, FSO och FSTEK, vunnit mark. Bland dessa instanser har det länge funnits en uppfattning om cybersfären som ett hot. I deras analys är mer statlig kontroll som regel något att sträva efter. Både trafikinnehåll och vilken väg trafiken färdas bör övervakas och, när så krävs, blockeras. Denna del av det politiska systemet har haft en dominerande roll vad gäller att skriva informationssäkerhetsdokument, men det är först från och med period två som praktiska åtgärder på allvar minskar friheten på internet. Gruppens syn på cyber har också gradvis har vunnit mark både i parlamentet och i samhället i stort.

Företag verksamma inom cybersektorn har blivit alltmer medvetna om att det kan stå dem dyrt att kritisera regeringens politik och tenderar att stödja förslag om mer kontroll. De dominerande internetbolagen är antingen statliga eller kontrolleras av regeringen närstående affärsmän och var redan från 2000 obenägna att kritisera regeringens politik. Under den första perioden fanns dock fler exempel på mindre och innovativa företag som var kritiska mot ökade kontrollåtgärder och övervakning och de bördor det medförde för näringslivet. Detta förändrades dock gradvis och från och med den tredje perioden togs flera av dessa företag över av regeringen närstående bolag samtidigt som det politiska trycket ökade på samtliga. Sektorn har blivit alltmer beroende av statliga kontrakt och majoriteten av internetbolagen antingen stöder eller begränsar sig till att uttrycka en mild kritik mot regeringens politik (Prokopenko 2019; Vendil Pallin 2017a).

Den verkställande grenen av Rysslands politiska system dominerar landets beslutsfattande på bekostnad av parlamentarisk granskning och rättsligt ansvarsutkrävande samtidigt som staten alltmer dominerar landets ekonomi. Därmed blir kontrollåtgärder och åtföljande lagstiftning ett större demokratiskt problem i Ryssland än motsvarande lagstiftning i länder där myndigheters verksamhet ständigt kan granskas. Inget av Rysslands stora internetföretag har öppet motsatt sig den ökade kontrollen över internet trots alla de kostnader, direkta och indirekta, som den medför för branschen.

Många organisationer utgör en länk mellan regeringen och internetföretagen och samhället och finns gränser för hur hård kritik som kan framföras offentligt mot nya kontrollåtgärder. De organisationer som skapats på mer eller mindre direkt regeringsinitiativ (GONGO:er) används också för att skapa en illusion av att olika initiativ att reglera internet är resultat av krav från gräsrotsorganisationer. På det hela tycks det som att säkerhetstjänsternas och militärens, de så kallade *silovikernas*,[20] syn på information och informationsteknologi har kommit att dominera inte bara byråkratin utan också dess förgreningar ut i samhället. Deras analys av världen beskrivs ofta som ”misstänksam och inåtskådande” (Soldatov & Rozhlitz: 94) snarare än fokuserad på de möjligheter till fritt utbyte av information som den nya informationsteknologin kan erbjuda.

Det finns dock konkurrerande krafter även inom regeringssfären som ser cyberutvecklingen som en källa till utveckling av landets ekonomi i stort, till effektiviseringsvinster och innovationer. Något som kan beskrivas som ett ekonomiskt block inom rysk byråkrati, med Ministeriet för ekonomisk utveckling i centrum, utgör kärnan bland dessa krafter. De motsätter sig också de avsevärda direkta och indirekta kostnader som ökad kontroll och övervakning för med sig.

Fram till cirka 2011 fanns också en betydande frihet på internet – både för användare och för företag som t.ex. utvecklade nya applikationer för den ryska marknaden. Från och med 2014 hårdnade klimatet betänkligt. Den politiska ledningen steg in och visade tydligt att det var den hårdare linjen, företrädd av framför allt Säkerhetsrådets kansli och FSB som skulle få dominera hur rysk cyberstrategi formulerades och implementerades. När en målkonflikt uppstod, t.ex. mellan målet att stimulera en rysk internetindustri och målet att öka statens kontroll över industrin vann som regel kontrollivrarna efter 2014.

Vid en rad brytpunkter har den politiska ledningen justerat kursen på rysk cyberstrategi och då kanske mest tydligt 2011 och 2014. Det skedde som ett resultat av externa krafter. I första fallet, 2011, pga. demonstrationer som den ryska politiska ledningen uppfattade som ett hot som förstärktes av internet. Mycket av det som FSB och Säkerhetsrådets kansli länge förespråkat började därmed bli även regeringens politik. När Ryssland befann sig under internationellt tryck 2014 skruvades tumskruvarna åt ytterligare i termer av konkreta åtgärder och långsiktiga program för att stärka cybersäkerheten.

Parallellt har Ryssland byggt upp sin förmåga att genomföra cyberoperationer. Något som gjorde att spänningen mellan väst och Ryssland ökade ytterligare. I lagförslaget om ett suveränt internet angavs att det faktum att USA såg Ryssland som ett hot inom cyberdomänen, var en anledning till att öka landets oberoende av

[20] Av ryskans ”sila” som betyder kraft eller makt. I ryskt tidningsspråk kallas ofta samtliga ministerier och myndigheter som förfogar över trupp och väpnad personal eller någon slags säkerhetstjänst ”siloviker”, dvs. kraftministerierna som en grupp institutioner. Uttrycket kan även referera till personer som representerar dessa ministerier eller har en bakgrund därifrån och därför antas representera liknande intressen, se t.ex. Soldatov & Rochlitz 2018)

internets globala infrastruktur. Lagen om ett suveränt internet blev också ett exempel på hur överväganden om funktionalitet samt ekonomiska invändningar fick stå tillbaka för det som hade blivit den dominerande linjen: att öka statens kontroll över innehåll och trafikflöden.

Även om det är tidigt att säga säkert tycks Presidentadministrationen ha inlett en delvis ny taktik för att vinna över internetanvändare. Enbart kontroll och tvång kan resultera i omvänt beteende – något som protesterna mot blockeringen av meddelandetjänsten Telegram var ett bra exempel på. Antalet användare av Telegram ökade drastiskt och fler ryska internetanvändare lärde sig att använda sig av VPN. Ny teknologi, framför allt i form av AI, utlovade nya möjligheter för att övervaka men också påverka ryska internetanvändares politiska uppfattning och beteende.

Externa krafter i form av teknologiutvecklingen men också pandemin 2020 och Kinas växande roll internationellt kommer att ha konkreta konsekvenser för utformningen av rysk cyberstrategi även framöver. Vilka aktörer inom Rysslands politiska system som framöver får mest inflytande kommer dessutom att bestämma hur Ryssland väljer att möta dessa utmaningar men också dra nytta av de möjligheter som uppstår.

Litteraturlista och källor

Officiella dokument

(huvuddelen av dokumenten är på ryska med titlar i svensk översättning)

Convention on International Information Security, Utrikesministeriet, 22 september 2011 http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666 (10 mars 2017).

Digital ekonomi – Program, Regeringsförordning nr. 1632, 28 juni 2017, http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf (14 september 2017).

Federal lag 126-FZ, ”Om samband”, 7 juli 2003, http://www.consultant.ru/document/cons_doc_LAW_43224/#dst0 (20 maj 2020).

Federal lag 149-FZ, ”Om information, informationsteknologier och om skyddet av information”, http://www.consultant.ru/document/cons_doc_LAW_61798/ (29 maj 2020).

Federal lag 187-FZ, ”Om Ryska federationens kritiska informationsinfrastrukturs säkerhet”, 26 juli 2017, http://kremlin.ru/acts/bank/42128 (19 maj 2020).

Federal lag 188-FZ, ”Om införande av ändringar i Federala lagen ’Om information, informationsteknologier och skydd av information’ och artikel 14 i Federala lagen ’Om kontraktssystemet gällande upphandling av varor och tjänster för att tillgodose statliga och municipala behov’”, 29 juni 2015, http://kremlin.ru/acts/bank/39838 (4 juni 2020).

Federal lag 369-FZ, ”Om införande av ändringar i Federala lagen ’Om operativ förundersökningsverksamhet’ och artikel 13 i Federala lagen ’Om federala säkerhetstjänsten’”, 21 december 2013, http://kremlin.ru/acts/bank/37908 (29 maj 2020).

Federal lag 375-FZ,”Om införande av ändringar i Ryska federationens Straffrättskodex och Straffprocessrättskodex i delar för att infoga ytterligare åtgärder för att bekämpa terrorism och säkerställa samhällets säkerhet”, 6 juli 2016, https://rg.ru/2016/07/11/uk375-dok.html (28 maj 2020).

Federationsrådets förordning, nr. 475-SF, 26 oktober 2016, http://council.gov.ru/activity/documents/72902/ (12 maj 2020).

Förordning Säkerhetsrådets Interdepartementala kommission för informationssäkerhet, Presidentdekret nr. 590, 6 maj 2011, http://www.scrf.gov.ru/about/commission/MVK_info/ (2 juni 2020).

Förslag till federal lag, nr 428884-6, 15 januari 2014, http://asozd2c.duma.gov.ru/addwork/scans.nsf/ID/A1C7BA1998A172DD43257C61003AF389/$FILE/428884-6.PDF?OpenElement (28 maj 2020).

Handlingsplan (*pasport*) för nationella projektet ”Digital ekonomi”, Ryska regeringens hemsida, oklart datum, https://digital.gov.ru/uploaded/files/natsionalnaya-programma-tsifrovaya-ekonomika-rossijskoj-federatsii_NcN2nOO.pdf (11 juni 2020).

Informationssäkerhetsdoktrin, Presidentinstruktion nr. 1895, 9 september 2000, http://www.scrf.gov.ru/Documents/Decree/2000/09-09.html (15 september 2000).

Informationssäkerhetsdoktrin, Presidentdekret nr. 646, 5 december 2016, http://static.kremlin.ru/media/acts/files/0001201612060002.pdf (11 augusti 2017).

Konceptuell syn på Ryska federationens Väpnade styrkors verksamhet i informationsrymden [på engelska], Ryska federationens Försvarsministerium, 2011, http://ens.mil.ru/science/publications/more.htm?id=10845074@cmsArticle (19 januari 2018).

Nationell strategi för utveckling av artificiell intelligens för perioden till 2030, Presidentdekret nr. 490, 10 oktober 2019, http://static.kremlin.ru/media/events/files/ru/AH4x6HgKWANwVtMOfPDhcbRpvd1HCCsv.pdf (13 november 2019).

Presidentdekret nr. 31s (utdrag), 15 januari 2013, http://kremlin.ru/acts/bank/36691 (19 maj 2019).

Presidentdekret nr. 204, 7 maj 2018, http://kremlin.ru/acts/bank/43027 (9 juni 2020).

Presidentdekret nr. 620, 22 december 2017, http://kremlin.ru/acts/bank/42623 (19 maj 2019).

Presidentdekret nr. 334, 14 juni 2018, http://kremlin.ru/acts/bank/43183 (13 augusti 2019).

Presidentdekret nr. 474, 21 juli 2020, http://publication.pravo.gov.ru/Document/Text/0001202007210012 (10 augusti 2020).

Presidentdekret nr. 1711, 29 december 2012 (med ändringar från 5 mars 2014 (nr. 119) och 26 maj 2015 (nr. 267), http://www.scrf.gov.ru/about/commission/MVK_info_members/ (18 augusti 2017).

Regeringsinstruktion nr. 1187-r, 30 april 2020, http://government.ru/info/39633/.

Strategi för utvecklingen av informationssamhället i Ryska Federationen, Presidentdekret nr. Pr-212, 7 februari 2008, https://rg.ru/2008/02/16/informacia-strategia-dok.html (hämtat 14 augusti 2020).

Strategi för utvecklingen av informationssamhället i Ryska Federationen 2017–2030, Presidentdekret nr. 203, 9 maj 2017, http://static.kremlin.ru/media/acts/files/0001201705100002.pdf (hämtat 21 september 2017).

Övrig litteratur och källor

Agora (2017) *Rossija. Svoboda interneta 2016: na vojennom polozjenii*, februari, https://meduza.io/static/0001/Agora_Report_2017_Internet.pdf (4 oktober 2017).

Agora (2018) *Svoboda interneta 2017: polsutjaja kriminilizatsija*, 5 februari, https://meduza.io/static/0001/Agora_Internet_Freedom_2017_RU.pdf (13 januari 2020).

Agora (2019a) *Svoboda interneta 2018: delegirovanije repressij*, 5 februari, https://guides.files.bbci.co.uk/bbc-russian/AGORA_Freedom-of-the-Internet-2018.pdf (13 januari 2020).

Agora (2019b) *Votum neuvazjenija prezidentu: pervoje polugodije ”Zakona Klisjasa”*, september, https://meduza.io/static/0001/Agora_Report_Disrespect_For_The_President.pdf (1 oktober 2019).

Agora och Radio Svoboda (2020) *Svoboda interneta 2019: plan ”Krepost”*, 4 februari, https://2019.runet.report/assets/files/Internet_Freedom%202019_The_Fortress.pdf (5 februari 2020).

Allison, Graham (1971) *Essence of Decision: Explaining the Cuban Missile Crisis*, New York, Harper Collins Publishers.

Allison, Graham och Zelikow, Philip (1999) *Essence of Decision: Explaining the Cuban Missile Crisis*, 2:a uppl., New York, Longman.

Allison, Graham T. och Halperin, Morton H. (1972) ”Bureaucratic Politics: A Paradigm and Some Policy Implications”, *World Politics*, vol. 24, Supplement: Theory and Policy in International Relations, s. 40–79.

APKIT (2020) “Pozitsija APKIT po ugalovnomu presledovaniju IT-predprinimatelej”, 22 juli, https://apkit.ru/files/2020%20APKIT_position_06.pdf (11 augusti 2020).

Balasjova, Anna, Parfenteva, Irina och Kozlov, Vjatjeslav (2019) ”Glava Roskomnadzora nazval petjalnoj situatsija s Facebook v Rossii”, *RBK*, 10 juni, https://www.rbc.ru/technology_and_media/10/06/2019/5cfcdd9f9a794783fad0d1e8 (10 juni 2019).

Bartles, Charles K. (2016) ”Russia’s Indirect and Asymmetric Methods as a Response to the New Western Way of War”, *Special Operations Journal*, nr. 1, s. 1–11.

Baletskaja, Ksenija (2019) ”’Jandeks’ vmeste s tjinovnikami pridumal novuju strukturu upravlenija kompaniej”, *Vedomosti*, 18 november, https://www.vedomosti.ru/technology/articles/2019/11/18/816461-yandeks-s-chinovnikami (18 november 2019).

Basjlykova, Natalja (2013) ”Spetssluzjby natjnut operativno-rozysknuju dejatelnost v internete”, *Izvestija*, 16 november, http://izvestia.ru/news/560754 (3 oktober 2014).

BBC News – Russkaja sluzjba, ”MVD Rossii: sotsseti ugrozjajut ustojam obsjtjestva”, 8 december 2011, https://www.bbc.com/russian/russia/2011/12/111208_osce_declaration_russia_block (4 juni 2020).

BBC News – Russkaja sluzjba, ”Usmanov uchodit iz Mail.ru. Tjto stoit za etim resjenijem?”, 22 oktober 2018, https://www.bbc.com/russian/news-45938144 (6 november 2019).

Council on Foreign Relations (inget årtal) ”Cyber Operations Tracker”, https://www.cfr.org/interactive/cyber-operations (senast besökt 9 mars 2020).

Demidov, Oleg (2016) ”Gosobezopasnost: kak ustrojena novaja strategija borby s kiberugrozami”, *RBK*, 7 december, http://www.rbc.ru/opinions/politics/07/12/2016/5848251b9a79473c64458637 (12 december 2016).

”Dmitrij Medvedev provel sovesjtjanije po voprosu utjastija Rossijskoj Federatsii v razrabotke kompleksa mezjdunarodnych mer po sozdaniju rezjima ravnych prav v upravlenii seti internet”, Säkerhetsrådet, 12 augusti 2020, http://www.scrf.gov.ru/news/allnews/2821/ (17 augusti 2020)-

Engqvist, Maria (2020) *Ryska federationens Säkerhetsråd – överblick och bedömning*, FOI Memo 7090, 27 april.

Estonian Foreign Intelligence Service (2018) *International Security and Estonia 2018*, https://www.valisluureamet.ee/pdf/raport-2018-ENG-web.pdf (7 mars 2018).

Euronews (2020) ”Merkel Says Germany Has ‘Hard Evidence’ of Russian Hacking”, 13 maj, https://www.euronews.com/2020/05/13/merkel-says-germany-has-hard-evidence-of-russian-hacking (9 juni 2020).

Facebook, ”Dmitrij Medvedev – Sovesjtjanije po voprosam sozdanija rezjima ravnych prav v upravlenii internetom”, 12 augusti 2020, https://www.facebook.com/Dmitry.Medvedev/videos/vb.175517041850/617263725858982/?type=3&theater (17 augusti 2020)

Federationsrådet (2014) ”Utkast till cybersäkerhetsstrategi för Ryska Federationen”, http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf (31 januari 2018).

Federationsrådet (2018) ”Ezjegodnyj doklad”, Tillfälliga kommissionen för att skydda statlig suveränitet och hindra inblandning i Ryska Federationens inrikespolitik, februari 2018, http://council.gov.ru/media/files/G6hNGZ3VbQNiMdZki1BKbrsrvuRxPwim.pdf (10 juni 2019).

Federationsrådet (2019) ”Ezjegodnyj doklad”, Tillfälliga kommissionen för att skydda statlig suveränitet och hindra inblandning i Ryska Federationens inrikespolitik, mars 2019, http://council.gov.ru/media/files/LIkgU7Df0m31nfswAg80N5d4TKFhy8UG.pdf (23 oktober 2019).

FireEye (2017) *APT28: At the Center of the Storm – Russia Strategically Evolves Its Cyber Operations*, FireEye Special Report, https://www2.fireeye.com/rs/848-DID-242/images/APT28-Center-of-Storm-2017.pdf (18 december 2018).

FOM (2016) ”Internet v Rossii: dinamika proniknjvenija. Vesna 2016”, *Fond obsjtjestvennaja mnenija*, 11 oktober, https://fom.ru/SMI-i-internet/13012 (8 mars 2020).

Fox, Chris & Kelion, Leo (2020) ” Coronavirus: Russian spies target Covid-19 vaccine research”, *BBC News*, 16 juli, https://www.bbc.com/news/technology-53429506 (13 augusti 2020).

Franke, Ulrik (2015) *War by Non-Military Means: Understanding Russian Information Warfare*, FOI-R--4065--SE, mars, Stockholm FOI.

Franke, Ulrik and Vendil Pallin, Carolina (2012) *Russian Politics and the Internet in 2012*, FOI-R--3590--SE, december, Stockholm, FOI.

Freedman, Lawrence (2013) *Strategy: A History*, New York, Oxford University Press.

Freedom on the Net, https://freedomhouse.org/report/freedom-net, rapporter finns för åren 2009, 2011, 2012, 2013, 2014, 2015, 2016, 2017, 2018, 2019.

F-Secure (2015) *The Dukes: 7 Years of Russian Cyberespionage*, F-Secure Whitepaper, September 2015, https://blog-assets.f-secure.com/wp-content/uploads/2020/03/18122307/F-Secure_Dukes_Whitepaper.pdf (28 maj 2020).

FSTEK, ”Polnomotjija”, https://fstec.ru/obshchaya-informatsiya/polnomochiya (31 januari 2019).

Förbundet för ett säkert internet (2017) “Godovoj ottjet 2016”, http://www.ligainternet.ru/upload/docs/liga-2016-v-17.pdf (20 februari 2020).

Förbundet för ett säkert internet (datum saknas) ”Kiberdruzjina”, http://www.ligainternet.ru/liga/activity-cyber.php (2 oktober 2014).

Förbundet för ett säkert internet (datum saknas) ”O Lige”, http://www.ligainternet.ru/liga/about.php (2 oktober 2014).

Försvarsministeriet, ”Glavnoje upravlenije Generalnogo Sjtaba Vooruzjennych Sil Rossijskoj Federatsii”, https://structure.mil.ru/structure/ministry_of_defence/details.htm?id=9711@egOrganization (15 oktober 2018).

Försvarsministeriet, ”Tsentr spetsialnych razrabotok Ministerstva oborony Rossijskoi Federatsii”, http://ens.mil.ru/science/SRI/infrmation.htm?id=11739@morfOrgScience (15 oktober 2018).

Gaaze, Konstantin (2019) ”Kremlin Analytica: zatjem administratsii prezidenta iskusstvennyj intellect”, Carnegie Moscow Center, *Commentary*, 14 augusti, https://carnegie.ru/commentary/79665 (19 August 2019).

Gershikov, Evan (2018) ”The Spector of Kaspersky Looms over Russian Cybersecurity Firms”, *The Moscow Times*, 11 januari, https://www.themoscowtimes.com/2018/01/11/are-russian-cybersecurity-companies-still-welcome-in-the-west-a60164 (4 mars 2019).

Giles, Keir (2011) ”’Information Troops’ – A Russian Cyber Command” i Czosseck, C., Tyugu, E. och Wingfield, T. (red) *3rd International Conference on Cyber Conflict*, NATO CCD COE Publications, Tallinn, s. 45–60.

Giles, Keir (2012) ”Russia and Cyber Security”, *Nação e Defesa*, nr. 133–5, s. 69–88.

Giles, Keir (2016) ”Handbook of Russian Information Warfare”, *Fellowship Monograph, Research Division – NATO Defense College*, nr. 9 (november), http://www.ndc.nato.int/news/news.php?icode=995 (9 mars 2020).

Goldberg, Anna och Romanova, Svetlana (2015) ”Nasj runet Tjemberlenu”, *Kommersant*, 20 april, https://www.kommersant.ru/doc/2703720 (19 september 2017).

Golitsyna, Anastasija (2017) ”Institut razvitija interneta uvolnjajet sotrudnikov”, *Vedomosti*, 18 januari, https://www.vedomosti.ru/technology/articles/2017/01/18/673512-institut (20 september 2017).

Granik, Irina och Nagornych, Irina (2012) ”Elektronnaja demokratija vzjata pod upravlenije”, *Kommersant*, 2 juli, https://www.kommersant.ru/doc/1971860 (11 september 2019).

Grebennikov, Vadim (2019) *Radiorazvedka Rossii: Perechvat informatsii*, Paratajp, Kindle edition.

Greenberg, Andy (2019) *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*, New York, Doubleday.

Habersetzer, Nicola (2020) "Interview with Andrei Soldatov on Digital Rights in Russia", *Human Rights Watch*, 19 juni, https://www.hrw.org/news/2020/06/19/interview-andrei-soldatov-digital-rights-russia (30 juni 2020).

Halperin, Morton H. och Clapp, Priscilla med Kanter, Arnold (2006) *Bureaucratic Politics and Foreign Policy*, (2:a uppl.). Washington D.C., Brookings Institution Press.

Hammarkrantz, Sara (2017) "Richard H. Thaler – och nudge på svenska", *Modern Psykologi* (återpublicerad artikel, ursprungligen publicerad i *Modern psykologi*, nr. 5, 2016), https://modernpsykologi.se/2017/01/11/psykologi-med-knuff/ (3 juni 2020.

Infoforum, "Ob Infoforume", https://infoforum.ru/about-infoforum (3 juni 2020).

Infoforum, "Orgkomitet", https://infoforum.ru/conference/orgcommitteeCategories/index (26 mars 2019).

Infoforum-2017, https://infoforum.ru/conference/conference/view/id/32 (14 maj 2020).

IRI, "Ob Institute razvitija interneta", https://xn--h1aax.xn--p1ai/ (20 februari).

Izvestija, "Tjislo kiberprestuplenij v Rossii vyroslo bolsje tjem na 85%", 9 juli 2020, https://iz.ru/1021686/2020-06-09/chislo-kiberprestuplenii-v-rossii-vyroslo-bolshe-chem-na-85 (13 augusti 2020).

Japparova, Lilija (2020) "'Osjtjusjtjenije, tjto ty okazalsia v bojevike iz 1990-ch'", *Meduza*, 26 februari, https://meduza.io/feature/2020/02/26/oschuschenie-chto-ty-okazalsya-v-boevike-iz-90-h (3 mars 2020).

Jastrebova, Svetlana (2018a) "Partner Usmanova prodolzjajet skupat proizvoditelej sistem dlja zakona Jarovoj", *Vedomosti*, 27 september, https://www.vedomosti.ru/technology/articles/2018/09/27/782237-partner-usmanova-prodolzhaet-skupat-zakona-yarovoi (3 oktober 2018).

Jastrebova, Svetlana (2018b) ”Siluanov trebujet ot goskompanii tjetkich planov perechoda na rossijskij soft”, *Vedomosti*, 16 december, https://www.vedomosti.ru/technology/articles/2018/12/16/789399-siluanov-trebuet-ot-goskompanii (18 december 2018).

Jastrebova, Svetlana (2018c) ”’Tsifrovaja ekonomika’ obojdetsia bjudzjetu uzje v 2 trln rublej”, *Vedomosti*, 18 september, https://www.vedomosti.ru/economics/articles/2018/09/18/781144-tsifrovaya-ekonomika-oboidetsya-byudzhetu-2-trln (19 september 2018).

Jastrebova, Svetlana (2019) ”Jevgenij Kasperskij: ’Risk-menedzjment v kiberbezopasnosti bolsje ne rabotajet’”, *Vedomosti*, 8 juni, https://www.vedomosti.ru/technology/characters/2019/06/08/803772-kasperskii (13 november 2019).

Jensen, Benjamin, Valeriano, Brandon och Maness Ryan (2019) ”Fancy Bears and Digital Trolls: Cyber Strategy with a Russian Twist”, *Journal of Strategic Studies*, Volv. 42, nr. 2, s. 212–34.

Johnson, James (2019) ”Artificial Intelligence & Future Warfare: Implications for International Security”, *Defense & Security Analysis*, vol. 35, nr. 2, s. 147–69.

Jonsson, Oscar (2019) *The Russian Understanding of War: Blurring the Lines Between War and Peace*, Washington D.C., Georgetown University Press.

Kahneman, Daniel (2012) *Thinking, Fast and Slow*, London, Penguin.

Kari, Martti J. (2019) *Russian Strategic Culture in Cyberspace*, JYU Dissertations 122, Jyväskylä, University of Jyväskylä – Faculty of Information Technology.

Karlzén, Henrik (2019) *Cyberoperationers attribution, tillvägagångssätt och sofistikation*, FOI-R--4834--SE (december), Stockholm, FOI.

Kasjevarova, Anastasija (2014) ”FSO budet sledit za ekstremistami tjerez blogi i sotsseti”, *Izvestija*, 10 januari, http://izvestia.ru/news/563116 (3 oktober 2014).

Kluge, Janis (2020) *Russia’s Transition to 5G: Stuck in a Regulatory Tug of War*, Foreign Policy Research Institute, Philapelphia, augusti, https://www.fpri.org/wp-content/uploads/2020/08/rpe-kluge-.pdf (31 augusti 2020).

Kodatjigov, Valerij (2019) ”Tjinovniki ne spesjat perechodit na rossijskij soft”, *Vedomosti*, 1 februari, https://www.vedomosti.ru/politics/articles/2019/02/01/792990-chinovniki-rossiiskii-soft (4 februari 2019).

Kolesnikov, Andrej (2019) ”Technokraty, vpered!”, *gazeta.ru*, 19 mars, https://www.gazeta.ru/comments/column/kolesnikov/12249110.shtml (20 mars 2019).

Kolomytjenko, Marija (2017) ”U kiberbezopasnosti menjajetsia kurator”, *Kommersant*, 13 januari, http://www.kommersant.ru/doc/3189312 (30 januari 2017).

Kolomytjenko, Marija (2019a) ”FSB potrebovala kljutji sjifrovanija polzovatelej u ’Jandeksa’”, *RBK*, 4 juni, https://www.rbc.ru/technology_and_media/04/06/2019/5cf50e139a79474f8ab5494b (13 november 2019).

Kolomytjenko, Marija (2019b) ”Operatory svjazi i FSB vystupili protiv ispolzujemoj v iPhone technologii”, *RBK*, 8 april, https://www.rbc.ru/technology_and_media/08/04/2019/5ca8e3319a79470abf10b8ac (23 april 2019).

Kolomytjenko, Marija och Balasjova, Anna (2018) ”MTS, ’VympelKom’ i drugije kompanii perepisjut zakony v sfere IT i svjazi”, *RBK*, 15 januari, https://www.rbc.ru/technology_and_media/15/01/2018/5a58ccd99a79475bf73470c1 (15 januari 2018).

Kommersant, ”Tjeresjnja polutjila ’sjirokopolosnyj’ dostup’”, 17 oktober 2019, https://www.kommersant.ru/doc/4127646 (8 augusti 2020).

Kovatjitj, Leonid (2020a) ”Ot Moskvy do Pekina”, Carnegie Moscow Center, *Commentary*, 8 maj, https://carnegie.ru/commentary/81656 (26 maj 2020).

Kovatjitj, Leonid (2020b) ”Sdelano ne v Kitaje”, Carnegie Moscow Center, *Commentary*, 5 augusti, https://carnegie.ru/2020/08/05/ru-pub-82419 (17 augusti 2020).

Krasnusjkina, Nadezjda (2019) ”Iskusstvennomu intellektu podyskvajut zanjatije”, *Kommersant*, 4 oktober, https://www.kommersant.ru/doc/4112456 (19 november 2019).

Krivjakina, Jelena (2020) ”Dmitrij Medvedev: Mne pisjut: ’v ekonomike pri vas byla stabilnost’, no pensionnuju reformu pripominajut do sich por”,

Komsomolskaja pravda, 9 juli, https://www.kp.ru/daily/27153/4250026/ (13 augusti 2020).

Kushner, David (2013) ”The Real Story of Stuxnet”, *IEEE Spectrum*, 26 februari, https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet (27 maj 2020).

Lehtisaari, Katja (2019) ”Formation of Media Policy: The Case of the Iarovaia Law” i Wijermars, Mariëlle och Lehtisaari, Katja (red.) *Freedom of Expression in Russia's New Mediasphere*, Abingdon, Routledge, s. 57–73.

Lilly, Bilyana och Cheravitch, Joe (2020) ”The Past, Present, and Future of Russia’s Cyber Strategy and Forces”, i Jančárková, T., Lindström, L., Signoretti, M., Tolga, I. och Visky, G. (red.) *12th International Conference on Cyber Conflict*, NATO CCD COE Publications, Tallinn, s. 129–55.

Lindahl, David, Liljedahl, Birgitta och Waleij, Annica (2020) *Cyberattacks in the Healthcare Sector During the First Three Months of the Covid-19 Pandemic*, FOI Memo 7062, 9 april, Stockholm, FOI,

Lonkila, Markku, Shpakovskaya, Larisa och Torchinsky, Philip (2019) ”The Occupation of Runet? The Tightening State Regulation of the Russian-Language Section of the Internet” i Wijermars, Mariëlle och Lehtisaari, Katja (red.) *Freedom of Expression in Russia's New Mediasphere*, Abingdon, Routledge, s. 17–38.

Marczak, Bill, Guarnieri, Claudio, Marquis-Boire, Morgan och Scott-Railton, John (2014) ”Mapping Hacking Team’s ’Untraceable’ Spyware”, *Citizen Lab*. Munk School of Global Affairs & Public Policy, University of Toronto, 17 februari, https://citizenlab.ca/2014/02/mapping-hacking-teams-untraceable-spyware/ (27 maj 2020).

Markotkin, Nikolaj och Tjernenko, Jelena (2020) ”Razvitije technologij iskusstvennogo intellekta v Rossii: tseli i realnost”, Carnegie Moscow Center, *Nautjnaja statia*, 7 juli, https://carnegie.ru/2020/07/07/ru-pub-82173 (14 augusti 2020).

Maurer, Tim (2018) *Cyber Mercenaries: The State, Hackers, and Power*, Cambridge, Cambridge University Press.

Meduza (2019) ”’Tjtoby nas ne trjaslo’. ’Jandeks’ pridumal novuju strukturu upravlenija, kotoraja ustroit gosudarstvo”, 18 november, https://meduza.io/feature/2019/11/18/chtoby-nas-ne-tryaslo-yandeks-pridumal-novuyu-strukturu-upravleniya-kotoraya-ustroit-gosudarstvo (18 november 2019).

Meduza – podcast (2018) ”Taksi do Solsberi! Tjto stoit za gromkimi provalami GRU”, *Meduza v kurse*, 5 oktober, https://meduza.io/episodes/2018/10/05/taksi-do-solsberi-chto-stoit-za-gromkimi-provalami-gru (15 oktober 2018).

Medvedev, Dmitrij (2011) ”Dmitrij Medvedev provel vo Vladikavkaze zasedanije Natsionalnogo antiterroristitjeskogo komiteta”, *Prezident Rossii*, 22 februari, http://kremlin.ru/events/president/news/10408 (20 november 2018).

Minkomsvjaz Rossii, ”Obsjtjaja informatsija”, http://minsvyaz.ru/ru/ministry/common/ (2 oktober 2017).

Minkomsvjaz (2017) ”V Minkomsvjaze Rossii obsudili trechletnij plan meroprijatij programmy ’Tsifrovaja ekonomika’”, 29 september, http://minsvyaz.ru/ru/events/37435/ (2 oktober 2017).

Mintzberg, Henry (1978) ”Patterns in Strategy Formation”, *Management Studies*, vol. 24, nr. 9, s. 934–48.

Mintzberg, Henry (1994) *The Rise and Fall of Strategic Planning: Reconceiving Roles for Planning, Plans, Planners*, New York, The Free Press.

Mintzberg, Henry och Waters, James A. (1985) ”Of Strategies, Deliberate and Emergent”, *Strategic Management Journal*, vol. 6, nr. 3, s. 257–72.

MVD, ”Glavnoje upravlenije po protivodejstviju ekstremizmu”, http://mvd.ru/mvd/structure1/Glavnie_upravlenija/Glavnoe_upravlenie_po_protivodejstviju_j (2 oktober 2014).

MVD, ”Upravlenije ‘K’ MVD Rossii”, http://mvd.ru/mvd/structure1/Upravlenija/Upravlenie_K_MVD_Rossii (7 oktober 2014).

Nakashima, Ellen (2017) ”Israel Hacked Kaspersky, Then Tipped the NSA That Its Tools Had Been Breached”, *The Washington Post*, 10 oktober, https://www.washingtonpost.com/world/national-security/israel-hacked-kaspersky-then-tipped-the-nsa-that-its-tools-had-been-breached/2017/10/10/d48ce774-aa95-11e7-850e-2bdd1236be5d_story.html (19 november 2019).

Nezavisimaja gazeta, ”Poteri ot kiberatak v mire v blizjajsjije dva goda uvelitjatsia v dva-tri raza”, 18 juli 2018, http://www.ng.ru/politics/2018-07-18/3_7269_internet.html (14 mars 2019).

Nikkarila, Juha-Pekka och Ristolainen, Mari (2017) "'RuNet 2020' – Deploying Traditional Elements of Combat Power in Cyberspace?", *International Conference on Military Communications and Information Systems (ICMCIS)*, maj, https://www.researchgate.net/publication/317919390 (10 januari 2017).

Nikolsky, Aleksey (2013) "Federal Protection Service – FSO", *Moscow Defense Brief*, nr. 4, s. 35–9.

Nocetti, Julien (2015) "Contest and conquest: Russia and Global Internet Governance", *International Affairs*, vol. 91, nr. 1, s. 111–30.

Novyj, Vladislav (2020) "Kurator rubilnika Runeta: tjto izvestno o kandidate na post glavy Roskomnadzora", *Forbes*, 12 februari, https://www.forbes.ru/tehnologii/393021-kurator-rubilnika-runeta-chto-izvestno-o-kandidate-na-post-glavy-roskomnadzora (10 mars 2020).

Odnokolenko, Oleg (2000) "Vse svobodny", *Segodnja*, 24 juni, s. 1.

Parfenteva, Irina och Astafurova, Kristina (2019) "Kirijenko nazval obem finansirovanija dlja molodozjnogo kontenta v internete", *RBK*, 23 december 2019, https://www.rbc.ru/society/23/12/2019/5e00c11c9a79476cb09593e6 (10 mars 2020).

Patterson, Dan (2017) "Ukraine is a Test Bed for Global Cyberattacks That Will Target Major Infrastructure", *TechRepublic*, 27 juni, https://www.techrepublic.com/article/ukraine-is-a-test-bed-for-global-cyberattacks-that-will-target-major-infrastructure/ (4 mars 2020).

Persson, Gudrun (2017) "The War of the Future: A Conceptual Framework and Practical Conclusions Essays on Strategic Thought', *Russian Studies*, NATO Defense College, 03/17 (juli).

Persson, Gudrun (2020) "Kris och pandemi utmanar Ryssland" i Mittermaier, Eva, Granholm, Niklas och Veibäck, Ester (red.) *Perspektiv på pandemin: Inledande analys och diskussion av beredskapsfrågor i ljuset av coronakrisen 2020*, FOI-R--4992--SE, juni, Stockholm, FOI, s. 65–70.

Pertsev, Andrej och Solopov, Maksim (2020) "Tjto tjitajet Putin", *Meduza*, 16 juli, https://meduza.io/feature/2020/07/16/chto-chitaet-putin (8 augusti 2020).

"Polnyj Albats", *Echo Moskvy*, 8 april 2019, https://echo.msk.ru/programs/albac/2403407-echo/ (23 april 2019).

Posen, Barry R. (1984) *The Sources of Military Doctrine: France, Britain, and Germany Between the World Wars*, Ithaca, Cornell University Press.

Potechina, Anna (2015) ”Ot innovatsii – k perspektivnomu vooruzjeniju”, *Krasnaja zvezda*, 27 december, http://www.redstar.ru/index.php/newspaper/item/27165-ot-innovatsij-k-perspektivnomu-vooruzheniyu?tmpl=component&print=1 (2 februari 2018).

Prokopenko, Aleksandra (2019) ”Ot ’Jandeksa’ do imejlov. Tjto stoit za novym nastuplenijem na internet-kompanii”, *Carnegie Moscow Center – Commentary*, 8 augusti, https://carnegie.ru/commentary/79646 (12 augusti 2019).

Putin, Vladimir (2018) ”Presidential Address to the Federal Assembly”, *Prezident Rossii*, 1 mars. http://en.kremlin.ru/events/president/transcripts/messages/56957 (4 april 2019).

Putin, Vladimir (2020) ”Obrasjtjenije k grazjdanam Rossii”, *Prezident Rossii*, 23 juli, http://kremlin.ru/events/president/news/63548 (13 augusti 2020).

Pynnöniemi, Katri och Kari, Martti (2016) ”Russia’s New Information Security Doctrine: Guarding a Besieged Cyber Fortress”, *FIIA Comment*, nr. 26, December, http://www.fiia.fi/en/publication/646/russia_s_new_information_security_doctrine/ (11 augusti 2017).

RBK, 8 december 2011, ”Divizija imeni Dzerzjinskogo v vychodnyje vernetsia v Moskvu”, https://www.rbc.ru/society/08/12/2011/5703f0129a79477633d3ade7 (4 juni 2020).

RBK, 29 juli 2019, ”Aktsii ’Jandeksa’ upali na 3% na fone zakonoprojekta o znatjimych sajtach”, https://www.rbc.ru/rbcfreenews/5d3ea8af9a79476ab5a5c61d (13 november 2019).

RBK, 20 februari 2017, ”V Rossii sozdali konsortsium dlja prodvizjenija otetjestvennogo softa”, https://www.rbc.ru/rbcfreenews/58aad50f9a794753a868d7be (20 februari 2020).

RIA Novosti, ”Sovbez obnarodoval projekt redaktsii dotriny informatsionnoj bezopasnosti RF”, 24 juni 2016, https://ria.ru/politics/20160624/1451054504.html (11 augusti 2017).

Rosjtjina, Marija (2014) ”Sovet federatsii obsudit kiberbezopasnost s obsjtjestvom”, *Kommersant*, 10 januari, https://www.kommersant.ru/doc/2382085 (13 juni 2019).

RosKomSvoboda (2020) ”Raspredelenije blokirovok sajtov po vedomstvam”, https://reestr.rublacklist.net/visual/ (13 januari 2020).

Roskomsvoboda, ”VPN love”, https://vpnlove.me/ (3 mars 2020).

Roskomsvoboda, ”Rejestry”, https://vpnlove.me/ (3 mars 2020).

ROTsIT, ”Sostav upravlenija”, https://rocit.ru/about/board (20 september 2017).

Rozjdestvenskij, Ilja och Pintjuk, Alina (2019) ”Technologija razgona: Kak vlasti gotovjatsia k aktsijam oppozitsii’, *Republic*, 15 oktober, https://republic.ru/posts/94962 (21 oktober 2019).

Rozjkov, Ro och Tisjinja, Yuliia (2017) ”’Paket Jarovoj’ napolnjat psevdoninami”, *Kommersant*, 12 augusti, https://www.kommersant.ru/doc/3383396 (2 oktober 2017).

Rubnikov, Oleg, Zjukova, Kristina och Barinov, Vladimir (2018) ”FSB ustanavlivajet tretiu kiberzasjtjitu”, *Kommersant*, 11 september, https://www.kommersant.ru/doc/3738012 (25 september 2018).

Sarkisian, Lilit och Karliner, Anton (2019) ”’Oni lomajut nasj internet’”, *Novaja gazeta*, 10 mars, https://novayagazeta.ru/articles/2019/03/10/79816-oni-lomayut-nash-internet (5 februari 2020).

Schulze, Matthias (2020) ”Cyber in War: Assessing the Strategic, Tactical, and Operational Utility of Military Cyber Operations”, i Jančárková, T., Lindström, L., Signoretti, M., Tolga, I. och Visky, G. (red.) *12th International Conference on Cyber Conflict*, NATO CCD COE Publications, Tallinn, s. 183–97.

Sergina, Jelizaveta (2016) ”Sovet bezopasnosti opublikoval projekt Strategii razvitija informatsionnogo obsjtjestva”, *Vedomosti*, 14 december, https://www.vedomosti.ru/technology/articles/2016/12/14/669465-sovet-bezopasnosti-strategii-informatsionnogo-obschestva (9 oktober 2017).

Sivetc, Liudmila (2019) ”The Blacklisting Mechanism: New-School Regulation of Online Expression and Its Technological Challenges” i Wijermars, Mariëlle och Lehtisaari, Katja (red.) *Freedom of Expression in Russia's New Mediasphere*, Abingdon, Routledge, s. 39–56.

Sivkova, Alena (2014) ”MGER pomozjet silovikam s blokirovkoj ekstremistskogo kontenta”, *Izvestija*, 1 januari, http://izvestia.ru/news/564857 (3 oktober 2014).

Sjadrina, Tatiana (2014) ”Blogerov prosiat ukazyvat dlja kakogo vozrasta prednaznatjena ich informatsija”, *Rossijskaja gazeta*, 11 augusti, http://www.rg.ru/2014/08/11/blogeri.html (11 augusti 2014).

Soldatov, Andrei och Borogan, Irina (2015) *The Red Web: The Struggle Between Russia’s Digital Dictators and the New Online Revolutionaries*, New York, Public Affairs.

Soldatov, Andrei och Borogan, Irina (2018) ”Russia’s Approach to Cyber: The Best Defence Is a Good Offense”, i Popescu, Nicu och Secrieru, Stanislav (red.) *Hacks, Leaks and Disruptions: Russian cyber strategies*, Chaillot Papers, nr. 148, oktober, Paris, EU ISS, s. 15–23.

Soldatov, Andrei och Rochlitz, Michael (2018) ”The Siloviki in Russian Politics”, i Treisman, Daniel (red.) *The New Autocracy: Information, Politics, and Policy in Putin’s Russia*, Washington D.C, Brookings Institution Press, s. 89–108.

Stepanova, Julija (2020) ”Intellekt minus virus”, *Kommersant*, 6 april, https://www.kommersant.ru/doc/4314920 (18 maj 2020)

Sucharevskaja, Alena (2016) ”Neftegazovyj ventjur: kak rabotajet Fond razvitija internet-initiativ”, *RBK Zjurnal*, nr. 5 (maj), http://www.rbc.ru/magazine/2016/05/570fa16e9a794781cb616fa0 (20 september 2017).

Sucharevskaja, Alena och Juzbekova, Irina (2016) ”Lisjnego ne utetjet: kak immeno tjinovniki namereny obesopasit Runet”, *RBK*, 17 juni, http://www.rbc.ru/technology_and_media/17/06/2016/57613a4b9a794724f3e07644 (17 juni 2016),

The Economist, ”The Kaspersky Equation”, 19 februari 2015, https://www.economist.com/business/2015/02/19/the-kaspersky-equation (14 november 2019).

The Economist – The World in 2020, December 2019.

Tisjina, Julija (2020) ”’Tsifrovaja ekonomika’ stala ekonomnoj”, *Kommersant*, 18 maj, https://www.kommersant.ru/doc/4347753 (18 maj 2020).

Tjeberko, Ivan (2003) ”U Minsvjazi otbirajut tjastoty”, *Kommersant*, 20 mars, https://www.kommersant.ru/doc/372002 (20 maj 2020).

Tjernenko, Jelena (2017) ”Ugrozy informatsionnoj bezopasnosti stanovjatsia vse boleje isosjtjrennymi i massjtabnymi” (intervju med Oleg Chramov), *Kommersant*, 22 maj, https://www.kommersant.ru/doc/3303678 (17 augusti 2017).

Tjernenko, Jelena (2020) ”Bez dogovorennostej globalnogo charaktera etu problemu ne resjit”, *Kommersant*, 25 februari, https://www.kommersant.ru/doc/4267456 (29 maj 2020).

Tjevtajeva, Irina (2019) ”Kto mozet byt priznan inostrannym agentom”, *Vedomosti*, 21 november, https://www.vedomosti.ru/politics/articles/2019/11/21/816846-gosduma-razreshila-priznavat (4 mars 2020).

Tomas, Timothy I. (1998) ”Russia’s Information Warfare Structure: Understanding the Roles of the Security Council, FAPSI, the State Technical Commission and the Military”, *European Security*, vol. 7, nr. 1, s. 156–72.

Tomas, Timothy (2010) ”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*, Carlisle, Strategic Studies Institute, US Army War College, http://ssi.armywarcollege.edu/pdffiles/pub997.pdf (10 januari 2018).

Turovskij, Daniil (2016) ”Internettjik: Kto takoj German Klimenko i tjto budet sovetovat Vladimiru Putinu”, *Meduza*, 4 februari, https://meduza.io/feature/2016/02/04/internetchik (25 augusti 2017),

Turovskij, Daniil (2017) ”V Moskve susjtjestvujet kruzjok sjkolnikov-programmistov pod FSB, gde utjenikam raskazyvajut pro jevrejskij zagovor”, *Meduza*, 25 maj, https://meduza.io/feature/2017/05/25/v-moskve-suschestvuet-kruzhok-shkolnikov-programmistov (29 maj 2017).

Turovskij, Daniil (2018) ”GRU – eto voobsjtje tjto? Kogo berut v sjpiony? I potjemu ich tak tjasto raskryvajut?”, *Meduza*, 15 oktober, https://meduza.io/feature/2018/10/15/gru-eto-voobsche-chto-kogo-berut-v-shpiony-i-pochemu-ih-tak-chasto-raskryvayut (15 oktober 2018).

U.S. Department of Homeland Security (DHS) och Federal Bureau of Investigation (FBI) (2016) ”GRIZZLY STEPPE – Russian Malicious Cyber Activity”, *Joint Analysis Report*, (Reference Number: JAR-16-20296A), 29 december, https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf (21 mars 2018).

U.S. Department of Justice (2018) ”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”, 13 juli, https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-announcing-indictment-twelve (16 juli 2018).

U.S. Department of the Treasury (2018) *Treasury Sanctions Russian Federal Security Service Enablers*, 11 juni, https://home.treasury.gov/news/press-releases/sm0410 (10 mars 2020).

Valeriano, Brandon, Jensen, Benjamin och Maness, Ryan C. (2018) *Cyber Strategy: The Evolving Character of Power and Coercion*, New York, Oxford University Press.

Vedomosti, 23 mars 2011,”Internet pod kontrolem”, https://www.vedomosti.ru/opinion/articles/2011/03/23/schetchik_ekstremizma (20 november 2018).

Vedomosti, 19 september 2014, ”Administrator domenov ’.Ru’ i ’.RF’ gotov k otkljutjeniju Rossii ot interneta”, https://www.vedomosti.ru/politics/news/2014/09/19/administrator-domenov-ru-i-rf-zayavil-o-gotovnosti-k (24 september 2014).

Vedomosti, 4 oktober 2019, ”Putin odobril konkurs na rasprostranenije pozitivnych novostej v seti”, https://www.vedomosti.ru/politics/news/2019/10/04/812905-putin (10 mars 2020).

Vendil, Carolina (2001) ”The Russian Security Council”, *European Security*, vol. 10, nr. 2, s. 67–94.

Vendil Pallin, Carolina (2006) *De ryska kraftministerierna: Maktverktyg och maktförsäkring*, FOI-R--2004--SE, juni, Stockholm, FOI.

Vendil Pallin, Carolina (2017a) ”Internet control through ownership: The Case of Russia”, *Post-Soviet Affairs*, vol. 33, nr. 1, s. 16–33.

Vendil Pallin, Carolina (2017b) ”Russia’s Presidential Domestic Policy Directorate: HQ for Defeat-Proofing Russian Politics”, *Demokratizatsiya*, vol. 25, nr. 3, s. 255–78.

Vendil Pallin, Carolina (2018a) ”Ryssland”, i Thomas Denk och Carsten Anckar (red.) *Komparativ politik: Tio politiska system* (andra upplagan), Lund, Studentlitteratur, s. 249–72,

Vendil Pallin, Carolina (2018b) *Rysslands långsiktiga informationssäkerhetsstrategi*, FOI Memo 6309, 21 december, Stockholm, FOI.

Vendil Pallin, Carolina (2019a) ”Russian information security and warfare”, i Roger Kanet (red.) Routledge Handbook of Russian Security, Abington & New York, Routledge, s. 203–213.

Vendil Pallin, Carolina (2019b) *Ryssland nationaliserar internet – lagförslaget om ett* ”*suveränt internet”*, FOI Memo 6016, 27 februari, Stockholm, FOI.

Vendil Pallin, Carolina (2020) ”Cybersäkerhet och cyberoperationer: Rysk doktrin och praktik”, *Kungl Krigsvetenskapsakademiens Handlingar och Tidskrift*, nr. 1, s. 121–36.

Vendil Pallin, Carolina och Oxenstierna, Susanne (2017) *Russian Think Tanks and Soft Power*, FOI-R--4451--SE (augusti), Stockholm, FOI.

”Zasedanije nabljutadelnogo soveta Agenstva strategitjeskich initiativ”, *Prezident Rossii*, 22 november 2012, http://kremlin.ru/events/president/news/16871 (20 september 2017).

”Zasedanije Soveta Bezopasnosti”, *Prezident Rossii*, 1 oktober 2014, http://kremlin.ru/events/president/news/46709 (18 september 2017).

Zykov, Vladimir (2017) ”V Rossii pojavitsia natsionalnaja sistema filtratsii internet”, *Izvestija*, 2 augusti, https://iz.ru/627080/natcionalnaia-sistema-filtratcii-internet-trafika-poiavitsia-v-rossii (14 september 2017).

Zykov, Vladimir och Ramm, Aleksej (2016) ”V Rossii pojavilsia vojennyj internet”, *Izvestiia*, 19 oktober, https://iz.ru/news/639221 (20 januari 2020).

Appendix

Tabell 3. Organisationskommitté för Rysslands nationella forum för informationssäkerhet – Infoforum

Institution	Position	Namn
Samverkande ordförande för Infoforums organisationskommitté		
Duman	Förste vice ordförande för Utskottet för säkerhet och bekämpande av korruption	Ernest Balejev
Presidentadministrationen	Assistent till Presidentens sändebud i Centrala federala distriktet	Aleksej Mosjkov*
FSB	Chefen för Vetenskapliga-tekniska tjänsten	Andrej Fetisov
FSTEK	Direktör	Vladimir Selin
Utrikesministeriet	Presidentens särskilda sändebud för frågor rörande internationellt samarbete inom informationssäkerhetssfären	Andrej Krutskich
Regeringens kansli	Direktören för Informationsteknologi- och kommunikationsavdelningen	Vladislav Fedulov
Statliga bolaget ”Tsitadel”	Företagets vice direktör	Boris Mirosjnikov
Hedersordförande		
Duman	Före detta förste vice ordförande för Utskottet för säkerhet och bekämpande av korruption	Magomed Bachajev Chozj
Statliga bolaget ”Rostech”	Förste vice generaldirektör	Nikolaj Volobujev
Duman	Före detta förste vice ordförande för Utskottet för säkerhet och bekämpande av korruption; vice generaldirektör för ”Kaspiska rörledningsbolaget”	Michail Grisjankov
Vetenskapliga forskningsinstitutet för datorisering, automatisering och kommunikationer för järnvägstransporter	Förste vice generaldirektör	Vladimir Matiuchin
”RZjDStroj”* **	Assistent till generaldirektören	Aleksandr Spiridonov
Hela organisationskommittén (utom ordförandena)		
Duman	Rådgivare till vice talman	Ilja Kostunov
Säkerhetsrådets kansli	Chef för Avdelningen för säkerhet inom informations- och informationsteknologiområdet	Sergej Bojko
Regeringens kansli	Huvudrådgivare till Avdelningen för informationsteknologi och kommunikation	Oleg Zimenkov
FSB	Förste vice chef för Vetenskapliga-tekniska tjänsten	Eduard Tjernovoltsev
FSB	Vice chef för ett centrum (oklart vilket inom FSB)	Nikolaj Murasjov
FSB	Chef för Moskvas institut för ny informationsteknologi	Andrej Kovalenko

FSTEK	Vice generaldirektör	Vitalij Ljutikov
Inrikesministeriet	Chef för VIPK**	Aleksej Mosjkov*
Federala agenturen för kommunikationer (*Rossvjazi*)	Vice chef	Roman Sjeredin
Generalstaben (Försv.min.)	Chef för direktorat	Jurij Kuznetsov
Generalstaben (Försv.min.)		Sergej Babin
FSO	Vice chef för SSSI	Nikolaj Ilin
MTjS	Vice chef för Vetenskapliga-tekniska direktoratet	Eduard Burunin
Rosinformmonitoring	Assistant till direktören	Igor Volujevitj
Riksbanken	Vice chef för Huvuddirektoratet för säkerhet och informationsskydd	Artem Sytjev
Riksbanken	Chef för Centrum för övervakning och bekämpande av datorattacker	Dmitrij Frolov
Ryska pensionsfonden	Chefen för Avdelningen för informationssäkerhet	Jevgenij Niktitin
CSTO:s sekretariat	Vice generalsekreterare	Ara Badaljan
CSTO:s sekretariat	Rådgivare	Vladislav Sjusjin
Rysslands bankförening	Bankföreningens president	Garegin Tosunjan
Rysslands bankförening	Chefen för Informationssäkerhetskommittén	Aleksandr Veligura
Försvarsföretagens stödförening	Vice president för föreningen	Vladimir Rubanov
ANO för stöd till programmeringsindustrin****	Direktör	Leonid Uchlinov
Ryska unionen för industrialister och entreprenörer	Tillförordnad direktör för Direktoratet för informations- och kommunikationsteknologi	Sergej Mytenkov
Koordineringscentrum för nationella internetdomänen	Vice direktör	Andrej Romanov
Handels- och industrikammaren	Vice ordföranden i Underkommittén för betalningssystem och informationssäkerhet	Timur Aitov

Källa: Infoforum, ”Orgkomitet”.

Anm: Förutom namnen ovan hade organisationskommittén vid den här tidpunkten ytterligare 13 medlemmar som representerar universitet, forskningsinstitut och IT-bolag.

* Aleksej Mosjkov utnämndes till Presidentsändebud för Centrala federala distriktet 2018. Innan dess var han chef för Inrikesministeriets VIPK (se sedan). I listan från Infoforum står han fortfarande som den enda representanten för Inrikesministeriet och då med sin förra tjänst angiven.

** VIPK – Allryska institutet för kvalificering av inrikesministeriets personal.

*** RZjDstroj är ett dotterbolag till Ryska järnvägar och specialiserat på transportbyggnation.

**** ANO (autonom, icke-kommersiell organisation), grundarna bakom denna ANO är bl.a. Rostech och Föreningen för utvecklare av program ”Otetjestvennyj soft”.

Tabell 4. Sammansättningen av Säkerhetsrådets interdepartementala kommission för informationssäkerhet

Position*	**Anmärkning**
Vice sekreterare för Säkerhetsrådet	*Ordförande för kommissionen*, Troligen Oleg Chramov (se nedan)
Presidentens särskilda representant för frågor rörande internationellt samarbete inom informationssäkerhetssfären	Andrej Krutskich (se nedan)
Förste vice ordföranden för Dumautskottet för säkerhet korruptionsbekämpning	
Förste vice ordföranden för Ryska riksbanken (*Bank Rossii*)	
Förste vice kulturminister	
Förste vice utbildnings- och vetenskapsministern	
Statssekreteraren och vice minister för ekonomisk utveckling	
Statssekreteraren och vice energiministern	
Vice inrikesminister	
Vice ministern för industri och handel	
Vice minister för digital utveckling	*Vice ordförande för kommissionen*
Vice transportminister	
Vice justitieminister	
Statlig huvudinspektör för brandsäkerhet	
Vice direktör för finansiell övervakning	
Vice direktör för SVR	
Vice direktör för FSO – chef för direktorat	
Vice direktör för FSTEK	
Förste vice chef för Tulltjänsten	
Statssekreteraren – vice chefen för Teknisk Kontroll	
Vice chef för Migrationstjänsten	
Vice chef för Roskomnadzor	
Vice chef för Patenttjänsten	
Vice chef för Pressagenturen	
Vice chef för Federala agenturen för kommunikation (*Rossviazi*)	
Vice chef för Federala statliga statistiska tjänsten (*Rosstat*)	
Vice chef för Federala skattetjänsten	
Chefen för en av tjänsterna inom FSB	*Vice ordförande för kommissionen*
Chefen för Presidentadministrationens direktorat för användande av informationsteknologi och utveckling av valdemokrati	
Chefen för Generalstabens direktorat för operationer – vice generalstabschef	Sergei Rudskoj
Vice chef för GUSP (Huvuddirektoratet för särskilda program)**	

Vice chef för Presidentadministrationens tjänst för pressen och information	
Referent vid Säkerhetsrådets kansli	
Referent vid Presidentadministrationens direktorat för information och dokumentation	
Chefen för en av avdelningarna inom Säkerhetsrådets kansli	*Kommissionens sekreterare Troligen Sergej Bojko (se nedan)*
Direktören för en av Regeringskansliets avdelningar	
Vice direktören och chef för Rosnefts säkerhetstjänst	
Vice generaldirektör för säkerhet inom Rosatom	
Vice direktör för Gazprom	

Källa: Säkerhetsrådet 2015

Anm: * I Ryssland finns alltid flera vice ministrar och direktörer. Det är därför ofta svårt att identifiera exakt vilken vice som avses utom då det anges att det rör sig om någon som t.ex. även är statssekreterare eller chef för ett direktorat.

** GUSP ansvarar för mobiliseringsberedskap, inklusive kommunikationssystem.

ISSN 1650-1942

www.foi.se