Rysslands cyberberedskap på hemmaplan

Carolina Vendil Pallin

FOI-R--5611--SE

Augusti 2024

FOI

Carolina Vendil Pallin

Rysslands cyberberedskap på hemmaplan

Första året av ryska anfallskriget mot Ukraina

Titel	Rysslands cyberberedskap på hemmaplan – Första året av ryska anfallskriget mot Ukraina
Title	Russia's cyber preparedness at home – The first year of Russia's invasion of Ukraine
Rapportnr	FOI-R--5611--SE
Månad	Augusti
Utgivningsår	2024
Antal sidor	57
ISSN	1650-1942
Uppdragsgivare	Försvarsmakten
Forskningsområde	Säkerhetspolitik
FoT-område	Operationer i cyberdomänen
Projektnr	E12435
Godkänd av	Emil Hjalmarson
Ansvarig avdelning	Cyberförsvar och ledningsteknik

Bild/Cover: Vladimir Putin på Sankt Petersburgs internationella ekonomiska forum den 17 juni 2022 – efter att forumet försenats av en cyberattack, foto: Maxim Shemetov, Reuters.

Sammanfattning

Samma dag som Ryssland inledde sitt storskaliga anfallskrig mot Ukraina drabbades ryska it-nätverk av cyberattacker. Trots att Ryssland rankats högt som cybermakt, tycks landets cyberförsvar ha stått relativt oförberett. Inledningsvis rörde det sig främst om överbelastningsattacker, men attackerna blev med tiden mer avancerade. Hacktivister och kriminella grupper låg bakom de flesta attackerna och främst drabbades ryska myndigheter, statstrogna medier och it-företag.

Att försvara it-resurser i krig och gråzonsläge innebär större utmaningar än i fred. Ryssland var krigförande part trots en retorik om att det rörde sig om en begränsad militäroperation. Denna retorik kan ha bidragit till att för få försvarsåtgärder vidtogs. Ryssland överskattade troligen sin cyberförsvarsförmåga samtidigt som Ukrainas förmåga underskattades. Ryssland stod också illa rustat troligen eftersom rysk informationssäkerhetsdoktrin har betonat kognitiv säkerhet framför teknisk. Retoriken om ett suveränt internet kan snarast ha invaggat landet i falsk säkerhet. Att kontrollera landets befolkning prioriterades alltid högre än att skydda samhällets it-system.

Ryssland kan inte längre importera västlig teknik utan är beroende främst av Kina. Ryska myndigheter vill dessutom ersätta västlig programvara och förbjuder it-säkerhetslösningar från Väst samt blockerar alltmer tillgången på oberoende information liksom flera västliga sociala medier. Det ryska anfallskriget mot Ukraina kommer därmed att driva på en fragmentering av internet

Nyckelord: Säkerhetspolitik, krig, cyberattacker, hacktivism, cyberförsvar, Ryssland, Ukraina

Summary

Almost immediately after the full-scale invasion began, Russia was hit by a wave of cyberattacks. In spite of its high ranking as a cyber power, Russia's cyber defence was found lacking. To start with, distributed denial-of-service (DDoS) attacks dominated, but their sophistication increased with time. Hacktivists and criminal groups were behind most of the attacks, which targeted mainly Russian official authorities, state-loyal media, and IT companies.

In war or a grey-zone situation, IT defence is more challenging than in peace. In spite of the official labelling of the invasion as "a special military operation," Russia was a country at war. This rhetoric may have been part of the reason for Russia's slow cyber-defence response. Russia probably overestimated its cyber-defence capability and underestimated Ukraine. In addition, Russian official information-security doctrine emphasised cognitive over technical security. Another rhetorical device, about "a sovereign internet," risked creating a false sense of security, but this policy was always more about controlling the Russian population than about protecting society's IT networks.

Russia is no longer able or willing to rely on the import of Western technology. Instead, it has become more dependent on China. Russian official policy seeks to replace Western software and IT security solutions. On top of this, Russia is increasingly blocking independent information and Western social media platforms on the Russian internet. As a result, the Russian invasion of Ukraine will contribute to the global fragmentation of the internet.

Keywords: Security policy, war, cyberattacks, hacktivism, cyber defence, Russia, Ukraine

Förord

FOI är ett Eldorado för den som vill studera en aktuell fråga empiriskt och dessutom en fråga som spänner över flera ämneskompetenser. Att studera det som vi brukar sätta prefixet ”cyber” framför kräver kompetenser som inte ryms i en forskare. För att förstå vilka hot vi ser på it-området, hur vi bäst skyddar oss mot dem liksom varför det är svårt behöver vi experter på tekniken, på länders säkerhetspolitiska mål och agerande, på den ekonomi som föder utbyggnaden av it nationellt och globalt liksom på juridiken, för att nämna några av de viktigaste områdena.

Denna rapport har kommit till på uppdrag av Försvarsmakten inom ramen för FoT-projektet Strategier i cyberdomänen genom ett samarbete mellan Enheten för cyberförsvar (avdelningen Cyberförsvar och ledningsteknik) och Enheten för säkerhetspolitik (avdelningen Försvarsanalys). Det har varit en förmån att komma med en säkerhetspolitisk fråga till forskarna och analytikerna i Linköping och återvända till skrivbordet i Kista med en ny bättre fråga (eller inte sällan flera frågor). Rapporten är därmed också en produkt av den miljö och den kunskap som finns på FOI och den generositet som mina kollegor visar i att dela med sig av sin expertis. På deras inrådan har jag även försett rapporten med en ordlista sist i rapporten där it-termer och ryska myndigheter och termer finns samlade.

Rapporten granskades vid ett seminarium i maj 2024 av David Lindahl, som expert på it-säkerhet, och Maria Engqvist, som expert på rysk politik. Jag vill tacka dem för en gedigen insats som förbättrade rapporten avsevärt, liksom även mina kollegor i Rysslandsprojektet, Pär Gustafsson Kurki, Jonas Kjellén, Kristina Melin, som deltog i seminariet och lämnade värdefulla synpunkter. Stort tack också till RUFS-projektets praktikant, Jana Paegle. Emil Wannheden lämnade synpunkter skriftligen, som resulterade i att jag vässade min forskningsfråga (och dessutom såg till att jag undvek att ta fel på vinst och omsättning). Teodor Sommestad kommenterade mitt utkast skriftligen och hans kommentarer fick mig att leta vidare och förbättra min argumentation på flera centrala punkter. Mattias Wallén lämnade kommentarer på ett tidigare utkast, liksom min kollega Per-Erik Nilsson. Av samtliga fick jag utmärkta förslag till förbättringar och är er alla tack skyldig.

Carolina Vendil Pallin

Stockholm, den 19 juli 2024

Innehållsförteckning

Tabeller och figurer

1 Inledning

> *Året 2022 visade hur mottaglig cybervärlden är för förändringar som sker i den verkliga världen. Inledningen av den särskilda militära operationen inverkade kraftigt på cyberhotslandskapet.*
>
> It-säkerhetsföretaget Rostelekom Solar, 2023b.

Citatet ovan från det ryska företaget Rostelekom Solars understryker hur it-säkerhet kan försämras på grund av den säkerhetspolitiska utvecklingen likväl som av kriminalitet, mänskliga misstag, olyckor och dåligt it-skydd. Lika tydligt är att it-attacker kan påverka ett lands nationella säkerhet. Det gäller i fredstid men än mer i så kallat gråzonsläge och i krig.

Så sent som 2022 rankades Ryssland bland de främsta länderna vad gäller offensiv cyberförmåga (se t.ex. Voo, Hemani & Cassidy 2022) och på andra plats i Asien vad gäller militär cyberförmåga 2021–2022 (Lowy Institute 2023). En rankning från 2021 pekade ut Ryssland, tillsammans med Kina, Iran och Nordkorea, som de främsta hoten mot cybersäkerheten för bland andra Storbritannien (IISS 2021: 4). Samma rapport delar in världens länders förmåga på cyberområdet i tre grupper utifrån vilka styrkor de har inom olika områden, där cybersäkerhet är ett område. I den första gruppen finns USA som är det enda landet som är starkt på samtliga områden. Ryssland hamnar i nästa grupp inte minst på grund av svagheter vad gäller cybersäkerhet (IISS 2021: 9–11). De svagheter som existerade inom Rysslands it-skydd visade sig också vara betydande efter att Moskva inlett ett anfallskrig på Ukraina i februari 2022.

Utvecklingen under krigets första år visar på behovet att studera Ryssland inte bara som en offensiv aktör. Med få undantag (t.ex. Giles 2023 och Willett 2022) har analyser av krigets cyberaspekter koncentrerat sig på ryska cyberoperationer, trots att Ryssland troligen var det mest attackerade landet i cyberrymden redan i mars 2022 (Willett 2022: 17). För att förstå Ryssland som cyberaktör finns all anledning att även studera hur väl rustat landet var när det drabbades av cyberattacker. Dessutom finns en rad mer generella lärdomar att dra om hur krig förändrar spelplanen även i cyberrymden.

1.1 Forskningsfråga

Rysslands krig mot Ukraina erbjuder ett tillfälle att analysera hur pass väl rustat Ryssland var för att motstå it-attacker, då antalet attacker mot ryska mål ökade markant under 2022. Den övergripande forskningsfrågan är: *Varför kunde inte*

Ryssland försvara sig bättre när landet drabbades av it-attacker efter den 24 februari 2022, trots att landet rankades högt i termer av cybermakt? Denna övergripande fråga besvaras genom att bryta ned den i delfrågor som:

- Vilka typer av attacker rörde det sig om?
- Hur drabbades olika sektorer, t.ex. statliga myndigheter, it- och finanssektorn?
- Vilka grupper låg bakom och kan de kopplas till tidigare kända hotaktörer (APT:er)[1] och konkreta länder?
- Vilka svagheter existerade och vilka åtgärder har Ryssland vidtagit?
- Vilka slutsatser kan dras om ryskt it-försvar utifrån händelserna under det första året av Rysslands krig mot Ukraina och vilka erfarenheter kan vara aktuella att studera även för andra länder?

Tyngdpunkten i undersökningen ligger på perioden från dagen för Rysslands fullskaliga invasion av Ukraina, den 24 februari 2022, och ett år framåt. Även tiden strax före och efter denna period förekommer i materialet, men då främst för att jämföra läget före februari 2022 och för att följa upp ryska svarsåtgärder som har tagit tid att verkställa.

1.2 Källmaterial

Generellt har det blivit svårare att studera Ryssland sedan invasionen. Dels har vi som forskare inte möjlighet att åka till landet och genomföra intervjuer, dels har repression och statlig censur minskat tillgången till öppen information. Nya lagar och förordningar har gjort att ryska myndigheter, företag, forskare och analytiker är mer försiktiga med vad de publicerar samtidigt som propagandan som genomsyrar rysk information gör att t.ex. statistiska underlag och opinionsundersökningar bör tolkas med mer försiktighet än tidigare. Ryssland har ett auktoritärt politiskt system med allt vad det innebär i termer av censur och propagandadiktat (Engqvist 2024).

Jag försöker att löpande diskutera tillförlitlighet i källor och bakgrundsmaterialet i denna rapport. Jag använder mig av ryska artiklar i ämnet, men det kan vara på sin plats att redan här notera att det inte längre finns någon helt oberoende press i Ryssland. För att uppväga detta och för att följa utvecklingen har jag även använt mig av olika ryska it-experter, personer som ofta idag befinner sig utanför Ryssland, och deras analyser i bloggar eller på YouTube. Dessutom har jag följt utvecklingen genom att läsa artiklar i tidningar som har erfarna skribenter på

[1] Förkortningen APT, *advanced persistent threat*, används för grupper som genomför attacker som är avancerade och som regel besitter resurser och ihärdighet som snarast förknippas med ett land.

området teknisk informationssäkerhet som ofta är mindre politiskt känsligt som ämne, främst i *Kommersant* och *RBK* samt i viss mån även *Vedomosti.*

Jag använder även ryska it-säkerhetsföretags analyser som källmaterial. Som företag vill de attrahera kunder och intäkter och ibland är intervjuer med företrädare för ryska it-säkerhetsföretag en blandning mellan nyhetsartikel och ren reklam precis som är fallet i de flesta länder. Företagen kan därför vilja överdriva t.ex. förekomsten av it-attacker, eller en viss typ av attacker som de råkar sälja en säkerhetslösning för. Deras rapportering kan också färgas av att de samarbetar nära med ryska myndigheter. Det ryska it-säkerhetsföretaget Positive Technologies finns dessutom på USA:s sanktionslista eftersom det enligt amerikanska myndigheter samarbetar nära med den ryska Federala säkerhetstjänsten (FSB) (Sherman 2023; Soldatov & Borogan 2023). Även Kaspersky Lab brukar kopplas till FSB, eftersom dess grundare och ägare har en bakgrund inom sovjetiska KGB, FSB:s föregångare. Både Kaspersky Lab och Positive Technologies deltar också i de övningar som äger rum inom ramen för de årliga it-säkerhetsövningar som genomförs sedan 2019 (se avsnitt 2.2 Cyberövningar, s.18). För att välja vilka företags översiktliga rapporter som är mest relevanta för studien använde jag mig huvudsakligen av en lista i publikationen *CNews* över de största it-säkerhetsföretagen 2022 baserat på omsättning 2021 (se Tabell 1).

Endast vissa av dessa företag publicerar öppna rapporter om it-säkerhetsutvecklingen i Ryssland. Jag valde att leta bland de tio största, men inkluderade även Group-IB, som kommer först på 21:a plats i *CNews* lista. Företaget är specialiserat på att upptäcka och förebygga cyberkriminalitet. Group-IB:s direktör, Ilja Satjkov, kritiserade 2020 öppet FSB:s kontakter med cyberkriminella, något som gjorde att företaget fick allt svårare att verka i Ryssland. I september 2021 genomförde FSB en räd mot Group-IB och grep Satjkov. Företaget har flyttat sitt huvudkontor till Singapore och döpt om företaget till F.A.C.C.T., men är fortfarande verksamt i Ryssland och deras analytiker brukar intervjuas av ryska journalister, som regel med hänvisning till företagets tidigare namn, Group-IB. Att företaget fallit till plats 21 på *CNews* lista återspeglar troligen företagets konflikt med statliga myndigheter snarare än brist på expertis (Eckel 2023).

Tabell 1. Största ryska företag inom it-säkerhet 2022 baserat på omsättning 2021

Placering	Företag	Publicering av öppna analyser
1	Kaspersky Lab	En mer begränsad rapport samt en statistisk översikt över alla incidenter som deras egna system har noterat från samtliga länder de är verksamma i.
2	Softline	Publicerar ingen öppen översikt
3	Tsytadel	Publicerar ingen öppen översikt
4	Rostelekom-Solar	Publicerar flera översikter.
5	Bi.Zone	Publicerar inte någon öppen översikt; publicerade en analys av kriminella hackergrupper som under 2022 genomförde attacker på ryska organisationer.
6	Infosistemy Dzjet	Publicerar ingen öppen översikt
7	InfoTeKS	Publicerar ingen öppen översikt
8	Positive Technologies	Publicerar flera översikter.
9	Innostage	Publicerar ingen öppen stor översikt; publicerade en kort analys om de sju typer av attacker som var ”populära” 2022.
10	Norsi-Trans	Publicerar ingen öppen översikt
21	Group-IB	Specialiserar sig på cyberkriminalitet. Bytt namn till F.A.C.C.T.

Källa: CNews Analytics, 2022.

Ryska it-säkerhetsföretag har, liksom it-säkerhetsföretag i andra länder (Karlzén 2020b), ett ekonomiskt intresse av att framhålla dels en ökad hotnivå, dels egna säkerhetslösningar som de kan sälja in till företag som riskerar att drabbas på en marknad där de inte längre behöver konkurrera med västliga it-företag. Nästan 40 internationella it-säkerhetsföretag lämnade den ryska marknaden under 2022 (Dubov 2022: 3).

Slutligen använder jag mig av två databaser för att kartlägga cyberattacker mot Ryssland:

- *CFR Cyber Operations Tracker*, som amerikanska *Council of Foreign Relations* står bakom och som är en databas som ofta refereras i media.
- *Cyber Peace Institute*, som är en organisation (NGO) baserad i Geneve har en separat databas för cyberoperationer och –attacker relaterade till Rysslands krig mot Ukraina som startades i februari 2022, tillgänglig under fliken *Attack Details* (https://cyberconflicts.cyberpeaceinstitute.org/threats/attack-details).

För båda dessa databaser gäller att nästan inga it-attacker utförda av västländer förekommer i materialet. I fallet Council of Foreign Relations speglar detta troligen en tendens att fokusera på de länder som attackerar resurser i egna landet eller länder med vilka man samarbetar (se även Karlzén 2020a: 9; Lindahl 2020: 6). Underlaget till samtliga poster i databaserna kommer främst från västliga källor. Cyber Peace Institute hänvisar även till ryska eller ukrainska källor, men det blev vanligare först en bit in i perioden. Båda dessa institut loggar endast attacker som de bedömt har utförts av en ”hotaktör” där en stat antingen ligger direkt eller indirekt bakom. Därmed förekommer inte kriminella attacker i materialet. Båda förlitar sig på öppna källor.

Council of Foreign Relations (inget datum) anger i sin metodbeskrivning att de i sin tur har förlitat sig på tre databaser, på uppgifter i media samt från it-säkerhetsföretag.[2] Dessutom uppmanar hemsidan läsare till att rapportera in incidenter, vilket gör att CFR anser sig förlita sig på *crowdsourcing*. Inget står om urval eller vad som kvalificerar som ”cyber operation”. Underlaget för attacker mot Ryssland är tunt och det är svårt att avgöra hur urvalet skett.

Cyber Peace Institute (inget datum) är mer transparanta och har en mer stringent metod för urval och klassificering. Underlaget är väsentligt större (mer än 20 gånger så många poster ingår i materialet), vilket förklaras av att de också fokuserar på Rysslands krig mot Ukraina och startade loggningen i januari 2022. Endast attacker mot civila mål ingår. Vidare definierar Cyber Peace Institute (CPI) vad som är en cyberattack samt använder sig av FN:s definition av olika kategorier som drabbas och för samtliga poster anges om attacken är möjlig, trolig eller bekräftad (Cyber Peace Institute, inget datum). Däremot är det tydligt att loggningen inte varit så konsekvent som metodbeskrivningen anger. Till exempel loggas skadan för de första posterna ofta som ”Not Yet Known”, en formulering som försvinner i maj 2022. Vidare använder CPI, som nämnts ovan, även ryska och ukrainska källor som underlag senare i materialet, men inte de första månaderna. Mycket tyder på att tillgången till språkkunskaper eller annan kompetens har påverkat hur loggning i databasen har skett. CPI anger uppgifter i media, från CERT:ar,[3] it-säkerhetsföretag samt sociala medier och bloggar som underlag, men även om CPI:s underlag är rikare än CFR:s är det oklart hur urvalet skett, t.ex. om

[2] Florian Roth’s APT Groups and Operations (https://docs.google.com/spreadsheets/d/1H9_xaxQHpWaa4O_Son4Gx0YOIzlcBWMsdvePFX68EKU/pubhtml#); Center for Strategic and International Studies (CSIS) (länkeb på CFE:s hemsida är inte längre aktiv); och KasperskyLabs ”Targeted Cyberatattacks Logbook” (https://apt.securelist.com/).

[3] CERT – computer emergency response team, men betecknas numera som en ”pseudoförkortning” i Computer Swedens IT-ordlista. Beteckningen används för att beteckna centrum på olika nivåer och inom olika sektorer för att upptäcka it-attacker och sabotage. Till exempel är CERT-SE beteckningen för Sveriges nationella CSIRT (*Computer Security Incident Response Team*) och Rysslands riksbanks avdelning för informationssäkerhet har ett centrum för it-incidenter *FinTsert* (FinCert).

det har funnits sökkriterier eller på vilka grunder man har följt olika Twitter- eller Telegramkanaler.

Samtliga källor har således svagheter och styrkor. Det går heller inte att jämföra mängd av attacker mellan de olika källorna eftersom alla har sin egen definition och sätt att mäta. Inte heller har det varit möjligt att dela upp attackerna efter typ (överbelastnings-, spionage- respektive sabotageattacker t.ex.). Medan CFR och CPI förlitar sig på rapporterade cyberattacker och -operationer i öppna källor tenderar it-säkerhetsföretag att nämna antal incidenter, och utgår i regel från det material de själva har tillgång till i form av kundunderlag om attacker. Vissa av dessa företag har god insyn i t.ex. finansbranschen, andra i kritisk infrastruktur eller försvarsmyndigheter, men inget företag täcker alla mål som drabbats. Till detta kommer problemen med att de flesta attacker har undersökts i detalj först efter en betydande tid och att många attacker aldrig kommer till offentlighetens kännedom (Giles 2023: 5). De mest avancerade attackerna som syftar till underrättelseinhämtning upptäcks kanske inte ens av den som drabbas. Det finns således ett betydande mörkertal.

Den ryska politiska ledningen har i sin tur ett intresse både av att förminska betydelsen av cyberkrigföringen mot Ryssland, och av att utmåla landet som hotat för att motivera sin krigföring mot Ukraina liksom olika repressiva åtgärder gentemot den egna befolkningen (se även Giles 2023: 29). Ingen av källorna kan således ge något svar på ”antal attacker” eller andel överbelastningsattacker jämfört med exempelvis cyberspionage. Däremot ger de sammantaget en god bild av hur Ryssland angreps, vilka branscher som drabbades och hur beslutsfattare och myndigheter i Moskva såg sig tvungna att agera för att skydda sina nätverk. De ger också en indikation om vilka svagheter som fanns i det ryska it-försvaret.

1.3 Terminologi

Som framgår i avsnittet ovan om källor är det svårt, för att inte säga omöjligt, att definiera vad som utgör en cyberattack för olika aktörer, då de olika källor som jag har använt har utgått från olika terminologi och underlag för sina bedömningar. Jag har valt att löpande redovisa dessa skillnader när jag diskuterar materialet. Jag använder också prefixet ”cyber” omväxlande med ”it” då det stämmer relativt väl överens med hur ryska källor använder prefixen. Ryska källor använder mer sällan ”cyber” (*kiber*), utan oftast ordet digital (*tsifrovoj*).”Cyber” eller ”it” som prefix motsvarar också relativt väl den uppdelning som Ryssland gör mellan teknisk respektive psykologisk informationssäkerhet (se även mer om rysk doktrin s. 16).

När ryska termer är svåra att översätta exakt har jag valt att skriva även det ryska ordet inom parentes. För att i möjligaste mån undvika engelska termer och anglicismer har jag använt mig av Computer Swedens hemsida för it-ord. Jag har även inkluderat en ordlista sist i denna rapport (s. 55)

1.4 Struktur för denna studie

Jag inleder med att redogöra för huvuddragen i rysk doktrin och cyberförsvar på området. Lagstiftning från 2019 föreskriver att Ryssland ska genomföra cybersäkerhetsövningar varje år och ett avsnitt ägnas särskilt åt att försöka kartlägga vad det är som ryska myndigheter faktiskt har övat och vilka organisationer som övas. Jag undersöker om vi kan säga något om mängden och vilken typ av attacker det rör sig om efter 2022; om det faktiskt rör sig om en väsentlig ökning. Därefter analyseras vilka sektorer som framför allt drabbades. Att attribuera cyberattacker är notoriskt svårt. Jag gör dock ett försök analysera vilka som låg bakom de flesta av attackerna dels utifrån ryska uttalanden, dels utifrån attackdatabaserna och it-säkerhetsrapporterna. Därefter undersöker jag vilka de viktigaste ryska motåtgärderna var och vad de säger om luckor och brist på konsistens i ryskt cyberförsvar. Slutligen försöker jag svara på frågan varför Ryssland drabbades så pass hårt trots sin höga rankning som global cybermakt. Jag föreslår även ryska erfarenheter som kan vara intressanta att studera då de antingen är allmängiltiga för cyberförsvar när ett land befinner sig i krig eller pekar mot en mer generell utveckling av strategi inom cyberdomänen.

2 Ryskt cyberförsvar före 2022

Vilken är då rysk doktrin på cyberförsvarsområdet? Det korta svaret är Ryssland inte har någon enskild sådan utan en informationssäkerhetsdoktrin från 2016. Som så ofta är dock det korta svaret otillräckligt.

2.1 Rysk doktrin och cyberförsvar

Ryssland har ett väl utvecklat tänkande kring informationssäkerhet. och informationskrigföring. Cybersäkerhet och cyberkrigföring är komponenter i detta, det vill säga den del av informationskrigföring som omfattar informationstekniska system och digitala nätverk, där den andra delmängden är psykologisk krigföring och säkerhet. Cybersäkerhet utgör således i ryskt tänkande en delmängd i det mer omfattande begreppet ”informationssäkerhet” och det är det senare som framför allt förekommer i officiella strategiska dokument (Vendil Pallin 2020: 18). Federationsrådet, första kammaren i ryska parlamentet, försökte 2014 utarbeta en cybersäkerhetsstrategi 2014. Det hela stupade dock på att FSB förhindrade att dokumentet tog sig förbi utkaststadiet främst därför att det inte beaktade informationssäkerhet i den bredare bemärkelsen (Vendil Pallin 2020: 42–43). Sammantaget skvallrar detta om hur intimt förknippade it-säkerhetsaspekter ofta blir i rysk doktrin till det som snarast sorterar under psykologiskt försvar.

Bland de nationella intressen som Informationssäkerhetsdoktrinen (2016) anger ingår att skydda ryska medborgares privatliv när de använder informationsteknik (§8:a) och att säkerställa att kritisk informationsinfrastruktur fungerar robust och utan avbrott ”i fred, under en period där omedelbar aggression hotar och i krigstid” (§8:b). Doktrinen betonar också behovet av att utveckla en inhemsk it-industri, alltifrån elektronik till it-säkerhetsprodukter, för att stärka rysk informationssäkerhet (§8:c). Vidare går doktrinen in på vad som hotar it-säkerheten, t.ex. att andra länder använder it för att påverka Rysslands informationsinfrastruktur i militärt syfte (§11) och cyberkriminalitet (§14) samt vilka åtgärder som krävs för att motverka detta (§§20–29).

Även i den Nationella säkerhetsstrategin från 2021 finns ett avsnitt om informationssäkerhet där liknande hot och åtgärder räknas upp (§§48–57). Således fanns skrivningar i dessa liksom andra policydokument om vikten av att skydda landets it-system, men i samtliga dessa återfinns också skrivningar om vikten av psykologisk eller kognitiv informationssäkerhet, formuleringar om vikten av att skydda traditionella ryska andliga och patriotiska värderingar, något som närmast liknar en ideologisk säkerhet. Jämfört med den tidigare nationella säkerhetsstrategin ägnade 2021 års version mer utrymme åt samhällelig och inrikes säkerhet och då inte minst åt andlig och patriotisk säkerhet. I den ryska debatten tenderar de senare aspekterna, den kognitiva säkerheten, att ta det mesta av utrymmet medan teknisk

informationssäkerhet får mindre uppmärksamhet – något som inte är unikt för Ryssland.

I västlig analys tenderar dessutom fokus att hamna på ryska offensiva cyberoperationer. Så har varit fallet även när det gäller kriget mot Ukraina, vilket kanske är naturligt med tanke på att Ryssland är angripande part. Intresset för att studera rysk offensiv förmåga har dock överskuggat studier av landets cyberförsvar. Det stämmer troligen att Rysslands strateger på cyberområdet har varit snabbare än väst att utveckla en offensiv doktrin och ett agerande som snabbt drog nytta av ny teknik och västliga svagheter (Adamsky 2023; Kello 2022: 16ff.). Ryska doktrindokument behandlar främst försvar (eller avskräckning) genom att göra det svårt att penetrera Rysslands informationssfär, *deterrence by denial*, Adamsky 2023: 48), men tycks inte ha varit lika aktivt i att vidta praktiska åtgärder kring landets cyberförsvar.[4]

Det lagpaket som antogs 2019, i ryska medier ofta refererat till som ”lagen om ett suveränt internet”, innehöll komponenter som skulle ha kunnat stärka landets cyberförsvar. Lagändringarna syftade till något mer komplicerat än att ”klippa av” ett ryskt segment av internet från omvärlden. Målet var att öka möjligheterna för ryska myndigheter att kontrollera vilken information som var tillgänglig för ryska internetanvändare på ryskt territorium, men lagpaketet introducerade även möjligheten för Roskomnadzor att ta över och dirigera trafikflödet på ett ryskt segment av internet. Ryssland vidtog också åtgärder för att man skulle kunna använda en så kallad *kill switch*, att skapa ett regionalt nätverk, som var isolerat ett ryskt segment från omvärlden utan att det innebar att internet förändrades alltför mycket för användarna. Ryska medier benämnde det som ”ett ryskt segment av internet” (Vendil Pallin 2022). Det som den ryska politiska ledningen beskrev som ett ”suveränt internet” var alltid mer inriktat på att kontrollera och övervaka den egna befolkningen, mindre på att stärka it-säkerheten. Ryssland var berett att betala priset i termer av minskad funktionalitet (Meduza 2024).

Federala skyddstjänsten (FSO) ansvarar för ryska federala organs säkra kommunikationer och stommen i detta, RSNet, kan beskrivas som ett ”regeringsintranät” med en *gateway* (anslutning) mot internet (Kukkola 2020: 344–345). Enligt ett presidentdekret från 2013 tilldelades dessutom FSB huvudansvaret för att upptäcka, förhindra och eliminera konsekvenserna av it-attacker mot statliga informationssystem inom ramen för GosSOPKA (*Gosudarstvennaja Sistema obnaruzjenija, predotvrasjtjenija i likvidatsii posledstvij kompjuternych atak*) – en process för

[4] ITU (International Telecommunication Union) rankade dock Ryssland på delad femteplats i sin översikt *Global Cybersecurity Index* 2020. Ukraina kom först på 78:e plats i denna rankning (av totalt 182) och Sverige på 26:e plats, efter Finland, men även efter länder som Oman, Egypten, Indonesien och Vietnam (ITU 2021: 25–26). Rakningen väcker en rad frågor om metodiken, som riskerar att bli beroende av ländernas självrapportering snarare än en objektiv bedömning. I sin höga rankning av Ryssland som cybermakt påpekar också Voo, Hemani och Cassidy (2022: 15–16, 24) att rysk cybersäkerhet är svagare, inte minst eftersom det var tydligt att Ryssland var attackerat när rapporten publicerades.

cyberförsvar för myndigheter och statliga företag samt för regional federala organ. Det dröjde dock ytterligare fyra år innan en lag fanns på plats om skydd av kritisk informationsinfrastruktur. Myndigheter och företag som ansvarar för det som klassas som kritisk informationsinfrastruktur ålades därmed att koppla upp sig mot GosSOPKA (Kukkola 2020: 350). Statliga informationssystem och främst statliga företag med ansvar för kritisk informationsinfrastruktur hamnade därmed i centrum för lagen, medan det privata näringslivet var mindre berört (Vendil Pallin 2020: 41, 50).

2.2 Cyberövningar

Lagpaketet om ett suveränt internet ålägger utöver detta en rad ryska myndigheter att regelbundet genomföra övningar på federal nivå, men redan innan lagpaketet antogs hade åtminstone två större övningar på liknande tema genomförts. I juli 2014 testade ryska myndigheter om internet på ryskt territorium skulle fortsätta att fungera om ett ryskt segment inte längre hade tillgång till DNS-katalogen[5] globalt. I december 2017 var målet för övningen att testa om en angripare kunde följa abonnenter genom att snappa upp samtal, SMS och positionsdata eller genom att använda sårbarheter i mobilnätet (Skrynnikova 2019). Den genomfördes i Moskva och i Rostov-regionen och förutom myndigheter som Ministeriet för digital utveckling, FSB, Försvars- och Energiministeriet, deltog företag som Rostelekom, Megafon, Kaspersky Lab och Positive Technologies (Kolomytjenko 2017). Ryssland har dessutom en nationell övningsplattform, *Natsionalnyj kiberpoligon*, som en rad universitet kan koppla upp sig mot för att träna it säkerhet. Den tycks främst användas i utbildningssyfte och har byggts för att simulera nätverk inom specifika branscher inom näringslivet (*RBK* 2023).

I oktober 2023 angav en av de vice cheferna för Roskomnadzor, Oleg Terljakov, att Ryssland hade genomfört totalt sex övningar på fyra år, dvs. sedan lagpaketet antogs 2019 (Chabudilina 2023). Några av dessa går relativt lätt att identifiera.

Redan i december 2019 genomfördes en större övning. Ett direktorat inom Presidentadministrationen, [6] ryska Säkerhetsrådets kansli, Ministeriet för digital utveckling, Inrikesministeriet, Försvarsministeriet, Energiministeriet, FSB, FSO, Federala tjänsten för teknisk och exportkontroll (FSTEK), Ryska nationalgardet (*Rosgvardija*), Roskomnadzor och Federala sambandsagenturen (*Rossvjaz*) deltog i övningen. Det gjorde även företagen Rostelekom (det statliga telekombolaget och dess dotterbolag Rostelekom-Solar); Transtelekom, Tele2, Moderna radioteknologier, Positive Technologies, Group IB, MegaFon, Vympelkom, MTS och Kaspersky Lab. En av vice ministrarna för digital utveckling, Aleksej Sokolov, var

[5] DNS – *domain name system*, domännamnssystem, toppdomänerna som .se, .net eller .ru på internet.

[6] Direktoratet för användande av IT och utveckla elektronisk valdemokrati.

övningsledare och menade efter övningen att den hade visat att statliga organ tillsammans med nätoperatörerna kunde säkerställa att internet och elnätet fungerade. Varje deltagare i övningen hade sin del i scenarierna.[7] Till exempel ansvarade Positive Technologies för att testa faror som kan uppstå i sociala medier. Internetanvändare skulle enligt Ministeriet för digital utveckling inte märka av att övningen pågick och den genomfördes bara i Moskvaområdet och på ön Russkij belägen utanför Vladivostok i Fjärran östern (Kretjetova och Kinjakina 2019).

Ministeriet för digital utveckling utfärdade samma månad ett dokument (order nr. 839) om planen för övningar under 2020. Enligt ordern skulle fyra övningar äga rum 2020. I mars för att testa om det var möjligt att blockera trafik som använder kryptering i form av DNS över HTTPS eller DNS över TLS;[8] i juni för att motverka hot mot internets stabilitet på ryskt territorium i en övning där en del av sambandsnätet slutar att fungera på grund av extern destabiliserande påverkan av naturlig eller teknisk karaktär; i september för att öva att stå emot attacker som använder sig av sårbarheter inom smalbandsnätet för Internet of Things; och i december för att öva att motstå attacker som använder sårbarheter i BGP-protokollet.[9] I oktober 2020 hade dock inga av dessa övningar ägt rum (se Tabell 2). Samtliga hade ställts in med hänvisning till pandemin, men experter pekade också på problem som hade att göra med att nödvändig utrustning inte fanns på plats (Demurina 2020). Troligen har de dock genomförts senare.

Enligt Roskomsvoboda (2023), en rysk organisation som bevakar inskränkningarna av friheten på ryska internet sedan 2012, genomförde Ryssland två övningar under 2021 medan det saknas uppgifter för 2022. Under 2023 genomfördes tre övningar. Det är dock bara 2019 som Roskomnadzor publicerade ordern med beskrivning av övningarna på förhand. Eventuellt skedde det av misstag. Ryska aktivister och analytiker tog skärmdump av ordern och sparade den (Roskomsvoboda 2023), eller att reglerna och graden av sekretess har skärpts sedan dess. Order 839 från 2019 beskriver dessutom mer specifika övningar (se föregående stycke), medan åtminstone två av de övningar som rapporterades om i ryska media istället rörde sig om att dels testa hur ett ryskt segment klarade sig då

[7] Totalt ingick arton scenarier om cirka tjugo minuter vardera (tolv i signalprotokollet SS7 för telefoni och sex i nätverksprotokollet Diameter). Angriparen lyckades enligt rapporter från övningen att genomföra 62,5 procent av attackerna i SS7 och 50 procent i Diameter och attackerna upptäcktes inom cirka två–tre minuter (Skrynnikova 2019).

[8] DNS över HTTPS liksom DNS över TLS innebär kryptering av anrop till DNS-tjänsten, att användaren kan hitta en webbplats utan att teleoperatören kan se, eller ändra vilken adress det är. . I Rysslands fall innebär det att t.ex. FSB eller Roskomnadzor inte kan se vilken webbsida en internetanvändare letar efter om det sker genom DNS över HTTPS eller DNS över TLS. Det försvårar också dessa ryska myndigheters arbete med att blockera oönskade webbsidor eftersom de inte kan veta vilka sökresultat de ska ändra eller blockera. Om användaren använder en så kallad VPN-tjänst är det inte längre möjligt att genom trafikavlyssning se vare sig vilka webbplatser som besöks eller vilket innehåll som skickas.

[9] BGP, border gateway protocol, ett internetprotokoll som tillhandahåller information om tillgänglighet och rutter för trafik mellan autonoma system.

det inte kunde koppla sig mot den globala internetinfrastrukturen 15 juni–15 juli 2021, dels i juli 2023 hur ett regionalt internet segment klarade att ett ”nätobjekt” upphörde att fungera. Mer omfattande övningar som dessa är troligen svåra att dölja och därmed kommenterar Roskomnadzor dem. Huvuddelen av övningarna som ingick i ordern från 2019 var mindre i omfattning och kan ha genomförts utan att det orsakade alltför stora störningar medan de två större 2021 respektive 2023 ledde till kommentarer och artiklar i media (se Tabell 2).

Tabell 2. Sammanställning av ryska övningar på federal nivå

	Roskom-svoboda	**Rapporterat i media**	**Anmärkning**
2014		Test av vad som hände om Ryssland inte kunde koppla upp sig mot DNS-katalogen (juli).	
2017		Test av sårbarheter i mobilnätet (december).	
Lagpaketet om ett suveränt internet 2019			
2019	1	Övning med två scenarier, dels testades mobilnätet, dels testades nät för energi-, transport- och finanssektorn (23 december).	
2020	0		Fyra planerade som inte genomfördes 2020
2021	2	En större för att testa rysk bortkoppling från det globala internet (15 juni–15 juli).	
2022	Saknas uppgift	Sökningar i media på relevanta ord genererar inga resultat.	Fullskaliga invasionen i februari 2022
2023	3	Regionalt test av ej fungerande ”nätobjekt” (juni).	Oklart om flera övningar ägde rum parallellt med den i juli 2023 eller separat.
Totalt	6	Enligt Roskomnadzor totalt 6 genomförda övningar	

Källor: Chabidulina 2023; Kolomytjenko 2017; Roskomnadzor 2019; Roskomsvoboda 2023; Tjebakova 2021.

Det är värt att notera att övningen 2021 som syftade till att testa bortkoppling från det globala internet genomfördes inför Rysslands storskaliga invasion av Ukraina året därpå. Ryssland har fruktat att framtida sanktioner skulle kunna innebära att

landet inte längre kan koppla upp sig mot internets globala infrastruktur allt sedan sanktionerna i kölvattnet av den första ryska invasionen av Ukraina och olagliga annekteringen av Krim 2014 (Vendil Pallin 2020: 44 –45). Det kan också ses som en övning för att testa en defensiv förmåga för att skydda det ryska samhällets it-system i händelse av krig.

De fyra största ryska internetoperatörerna deltog i övningen liksom även Rostelekom, Transtelekom och ER-Telekom-Holding. Målet var att kontrollera om ”Runet”, dvs. det ryska segmentet av internet,[10] fungerade under yttre påverkan, blockeringar och andra hot. En källa till en rysk dagstidning uppgav att man hade testat ”möjligheten att fysiskt koppla bort den ryska delen av internet” (Tjebakova & Balasjova 2021). Chefen för Roskomnadzor, Andrej Lipov, var i oktober 2021 mycket nöjd med resultatet av övningen tidigare under året och menade att ”övningarna demonstrerar att vi är redo, att allt fungerar robust och säkert vid all form av påverkan utifrån” (*Kommersant* 2019).

Åtminstone på högsta ansvariga myndighetsnivå tycks en officiell bild om ett robust ryskt cyberförsvar ha dominerat i retoriken och i praktiken övades försvar inför ett helt annat hot än det som faktiskt blev Rysslands största problem efter den fullskaliga invasionen. Ukraina bad visserligen ICANN (Internet Corporation for Assigned Names and Numbers) att stänga av Ryssland från den globala DNS-strukturen, men fick nej med motiveringen att ICANNs uppdrag var att neutralt stödja globala internets funktionalitet (ICANN 2022).

Det finns även anledning att diskutera övningen 2023 här trots att den ägde rum efter den undersökta perioden. Den tycks ha syftat till att testa ett liknande scenario som den 2021. Natten mellan 4 och 5 juli genomfördes övningen för att testa robustheten för Runet, i klartext att koppla ur ett ryskt segment från det globala internet. Enligt ett första uttalande från en representant för Roskomnadzor hade övningen varit framgångsrik (Balasjova & Jasakova 2023). Samtidigt tydde en hel del på att övningen hade avbrutits i förtid. Trots att den ägde rum på natten – troligen för att ryska användare skulle påverkas så lite som möjligt – så kunde analytiker konstatera att funktionaliteten i telekomföretagen Beelines och Megafons nät gick ned under en timme då övningen pågick. Enligt en analytiker på ett internetforum för it-säkerhet ska det ha ägt rum framför allt i Centrala federala distriktet och Moskvaområdet drabbades. Ryska telekombolag fick information om att övningen skulle pågå i två timmar, men den avbröts efter bara 40 minuter (@denis-19 2023; Madory 2023). Andrej Lipov uttalade sig också om

[10] Runet används på flera olika sätt. I och med att Roskomnadzor 2019 definierade ”ett nationellt domännamnsystem” som domäner som slutar på .ru, .su och .рф kan man säga att det är något av en officiell rysk definition (Roskomnadzor, order nr. 216). Men termen Runet används också mer slarvigt om t.ex. alla ryskspråkiga sajter. Det finns också en ideologisk dimension i själva termen eftersom den bygger på tanken om ett internet som kan indelas geografiskt i nationella zoner (Franke & Vendil Pallin 2012: 35).

övningen senare och uttryckte att Roskomnadzor hade upptäckt ”problem med nätets robusthet (*zjivutjest*)” som ett resultat av övningen (Chabidulina 2023).

Ryssland hade således 2022 åtminstone på pappret en relativt väl utvecklad doktrin och utvecklade system för cyberförsvar. En regelbunden övningsverksamhet borde dessutom ha hjälpt ryska myndigheter att arbeta förebyggande. Att genomföra övningar och sedan inte ta till vara erfarenheterna är inte unikt för Ryssland. En rapport som genomförde en *net assessment* av ett antal länders cyberförmåga 2021 konstaterade dock att Ryssland låg efter främst vad gäller cyberförsvar (IISS 2021).

3 Mängd och typ av attacker på ryska mål under perioden

Utifrån rapporter från ryska it-säkerhetsföretag är det tydligt att ökningen av antal attacker på ryska nätverk började samma dag som Ryssland inledde sin fullskaliga invasion av Ukraina. Enligt Positive Technologies (2023d: 12) var antalet attacker som flest i april 2022 och sett över året angav de att majoriteten av attackerna var politiskt motiverade. Även Group-IB (2023: 3) anger att attackerna ökade markant, med 37 procent, under 2022 jämfört med föregående år. Rostelekom Solar (2023c) ger en liknande bild. Attackerna ökade således överlag i mars-maj 2022, med en topp i samband med 9 maj, den dag då Ryssland högtidlighåller segern i Andra världskriget. Det rörde sig främst om överbelastningsattacker under denna period. Sedan minskade antalet attacker, men de blev mer riktade och avancerade. Positive Technologies (2023b: 3) anger att antalet incidenter, som de definierar som framgångsrika attacker, ökade med drygt 20 procent under 2022 som helhet. Även under första kvartalet 2023 ökade antalet incidenter jämfört med föregående första kvartalet (Positive Technologies 2023c: 3). År 2022 var dessutom enligt Positive Technologies 2023d: 26) ett år som präglades av att stora mängder data läckte eller stals, inklusive persondata.

Enligt Rostelekom Solars (2023a) data, baserat på antal informationssäkerhets-incidenter som drabbat större företag hade hotnivån fördubblats 2022 jämfört med föregående år. I deras rapport som även täckte första kvartalet 2023 konstaterade Rostelekom Solar (2023a) att antalet incidenter fortfarande ökade men att ökningstakten hade mattats av. Vidare hade mängden läckta data under 2022 gjort att angripare hade kommit över information som kunde komma att användas för framtida mer avancerade attacker, t.ex. genom att använda sig av sårbarheter hos underleverantörer.

Tabell 3. IT-attacker mot Ryssland januari 2022–juni 2023 enligt CFR Cyber Operations Tracker

Datum/ månad	**Attackerat mål**	**Aktör (APT/ bekräftad av aktör)**	**Beskrivning**
Juni 2023*	Appletelefoner tillhörande ryska regeringstjänstemän och anställda på Kaspersky Lab	USA (NSA/okänt)	Spionage
Augusti 2022	Industrier/forskningsinstitut/ regeringsmål	Kina (APT18/okänt)	Spionage
Juni 2022	St. Petersburg Economic Forum	Ukrainas IT-armé (IT Army of Ukraine/ bekräftad)	Sabotage
Maj 2022	Två forskningsinstitut (radar och telekrigsforskning)inom industrikoncernen RosTech	Kina (Okänt vilken APT/okänt)	Spionage
Maj 2022	Ryska och belarusiska militära, statliga, industriella, transport- och mediamål; politiska partier	Ukrainas IT-armé (IT Army of Ukraine/okänt)	Överbelastnings-attacker
April 2022	Ryska militära tjänstemän	Kina (Mustang Panda/okänt)	Spionage
Februari 2022	Moskvabörsen och ryska Sberbank	Ukrainas IT-armé (IT Army of Ukraine/ bekräftad)	Överbelastnings-attacker
Januari 2022	Ryska diplomater i Indonesien	Nordkorea (Konni Group/ okänt)	Spionage

Källa: *CFR Cyber Operations Tracker*, sorterad på ”Russian Federation”, perioden 2022–2023, https://www.cfr.org/cyber-operations/ (2023-10-02).
* Utanför den undersökta perioden, men inkluderades här eftersom det var enda exemplet på att Väst pekas ut som källa för en attack och då troligen främst p.g.a. att Kaspersky Lab är en av källorna för CFR:s underlag.

Sett till vilka attacker som loggats av CFR:s Cyber Operations Tracker, förekom såväl attacker utförda av ukrainska aktörer som kinesiska och nordkoreanska gentemot ryska mål. Generellt loggar CFR relativt få attacker eller klumpar ihop ett stort antal mindre. De kinesiska attackerna bestod främst av riktat spionage med hjälp av skadlig programvara (*malware*), medan grupper som samlades under IT

Army of Ukraine inledningsvis använde sig av överbelastningsattacker med målet att åstadkomma avbrott i funktionalitet.[11] CFR:s insamling av data om it-attacker är viktat mot att hitta sådana som emanerar från kända hotaktörer mot västliga mål (t.ex. attacker från Kina, Ryssland och Nordkorea). I materialet för 2022–2022 listas Ukrainas IT-armé tre gånger, men bakom denna listning ligger troligen många incidenter som redovisas i månaden maj 2022 tillsammans (se Tabell 3). Överlag är antalet loggade poster alltför få för att dra några slutsatser enbart utifrån CFR:s underlag. (Se även nedan avsnittet om vilka som låg bakom.)

Som nämnts ovan är underlaget från CPI betydligt större och dessutom mer metodiskt loggat. Totalt ingår 208 poster i underlaget för perioden 25 februari 2022–24 februari 2023 då en sökning gjordes på ”Russian Federation” (endast attackerat land ingår i databasen, inte angriparland). Olika Anonymous-grupper låg bakom cirka 70 av de loggade attackerna medan IT Army of Ukraine stod för cirka 50. Den övervägande andelen av attackerna var överbelastningsattacker (nästan 90 stycken) eller ”hack and leak” (också nästan 90 stycken). Även CPI loggade ett par kinesiska attacker som syftar till spionage, men de försvinner nästan i mängden av överbelastnings- och *hack and leak*-attacker under perioden.

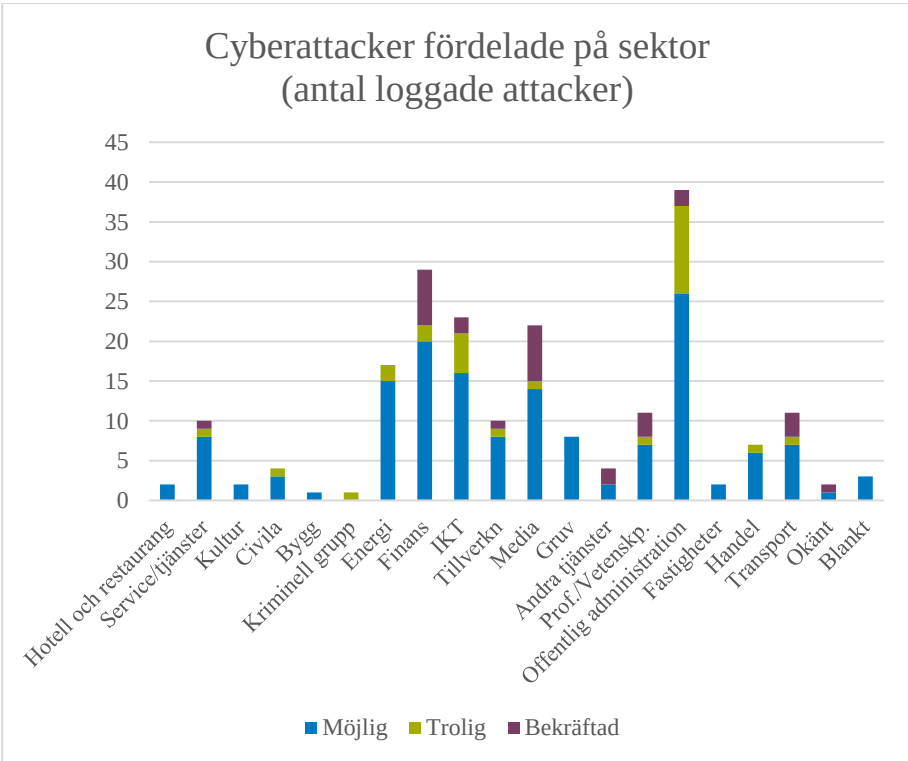
[11] IT Army of Ukraine var Ukrainas sätt att samla frivilliga för att genomföra it-attacker mot Ryssland. Enligt en forskningsrapport från 2022 bestod den av två delar. Dels en som internationellt uppmanar och mobiliserar den som vill delat i koordinerade överbelastningsattacker mot utpekade ryska mål. Dels existerade även en mer dold del kopplad till Ukrainas militära och underrättelsestrukturer, som arbetade för att utveckla mer avancerade attacker mot specifika ryska mål (Soesanto 2022: 4). På en ukrainsk hemsida för IT Army of Ukraine finns instruktioner om hur frivilliga kan ladda ner programvara, vilka mål som är prioriterade och möjligheten att föreslå mål (https://itarmy.com.ua/?lang=en). Se även IT Army of Ukraines telegramkanal: https://t.me/itarmyofukraine2022.

4 Drabbade sektorer

En sammanställning visar att de sektorer som drabbades värst enligt CPI:s databas var offentlig administration, finans-, informations- och kommunikationsteknik-(IKT), media- och energibranschen (se Figur 1). För media- och finansbranschen gäller att en stor andel av attackerna loggades som ”bekräftade”.

Överlag ger CPI:s databas en liknande bild som den som framkommer ur ryska it-säkerhetsföretagens rapportering. De flesta attackerna var inte avancerade, en stor mängd data stals och offentliga eller statliga resurser drabbades liksom branscher som inte sällan förknippas med den politiska ledningen, som energi- och media-branscherna. Attackerna blev dock mer avancerade med tiden. Till exempel drabbades inte IKT-branschen före april 2022, något som ryska it-säkerhetsföretag också noterar (se nedan). Att attackera IKT-företag är dessutom inte sällan ett sätt att komma över verktyg för att utföra ytterligare attacker.

Figur 1. Attacker fördelade på sektorer enligt CPI februari 2022-februari 2023



Varken CFR eller CPI loggar ökad förekomst av cyberkriminella attacker eftersom de fokuserar på så kallade hotaktörer (*threat actors*) som kan antas vara kopplade till en stat. Ryska it-säkerhetsföretag tenderar istället att summera incidenter –

ibland utan att särskilja om det rör sig om cyberkriminalitet eller t.ex. politiskt motiverade attacker. De har också en egen indelning av vilka sektorer som drabbas. Till exempel anger Positive Technologies att ”statliga” mål drabbas, medan CPI inte särskiljer mellan statliga (federala) myndigheter och regionala eller lokala sådana. De flesta it-företagen tenderar också att dela in sektorer efter vilka branscher de främst arbetar mot eller om det är stora eller små- till medelstora företag som drabbas. Jag har valt att dela in sektorerna i: statliga/offentliga myndigheter, industri- och näringsliv, finanssektorn, media samt IKT-sektorn. Att skilja ut media-, IKT- och finanssektorn ligger i linje med vilka sektorer som CPI:s data ger vid handen drabbades värst. Det finns också goda skäl att anta att flera av de attacker som drabbat mindre företag alls inte har noterats i öppna media och därmed inte heller finns i CPI:s databas (och än mindre i CFR:s material).

4.1 Statliga/offentliga myndigheter

Jämfört med föregående kvartal fördubblades antalet attacker på statliga mål första kvartalet 2022 och fortsatte sedan att öka under resten av året enligt Positive Technologies (2023d: 12). Såväl cyberkriminella som APT-grupper låg bakom. Det bör dock understrykas att det är oklart utifrån Postitive Technologies uppgifter om det bara var ryska statliga resurser som var underlag för deras data; företaget kan även ha inkluderat kundunderlag i andra länder. Däremot är det tydligt att det var ryska statliga resurser och medier som drabbades av politiskt motiverade Överbelastningsattacker 2022 enligt Positive Technologies. I en rapport baserad på data om incidenter, definierade som ”framgångsrika attacker”, noterar Positive Technologies (2023b) att hacktivister låg bakom en fördubbling av antalet incidenter 2022 och trenden höll i sig för första kvartalet 2023 (Positive Technologies 2023c: 14). Mest allvarligt var enligt företaget den höga förekomsten av incidenter som resulterade i att data, inklusive persondata, stals från statliga myndigheter. Postitive Technologies (2023d: 19) underströk riskerna för skyddet av medborgares data som digitaliseringen av statliga tjänster innebar givet utvecklingen 2022.

4.2 Industri och näringsliv

Positive Technologies (2023a) hävdade utifrån sitt underlag att industrisektorn under 2022 inte drabbades i högre grad än föregående år i termer av framgångsrika intrång. Snarare fortsatte antalet framgångsrika attacker per år att ligga kvar på den höga nivå som etablerades under pandemin. Då arbetade fler hemifrån, vilket ledde till nya möjligheter för attacker när medarbetare kopplade upp sig på distans. Som ofta i dessa rapporter är det oklart om detta gällde unikt ryska företag eller en större kundsektor där även utländska företag med rysk anknytning ingick. Sett under året 2022 var det tydligt att en topp ägde rum i kvartal två. Framför allt rörde det sig om kriminella nätverk som genomförde attacker, medan hacktivister som Anonymous genomförde överbelastningsattacker liksom datastölder. Positive

Technologies pekade ut kinesiska Space Pirates och ChamelGang som mest aktiva vad gäller avancerade angrepp i sin sammanställning av framgångsrika attacker mot industriföretag. Här var det tydligt att det rörde sig om ryska företag som mål, bland vilka rapporten särskilt nämnde statliga sådana, flyg- och rymdbranschen samt energi- och försvarsföretag. Dessutom noterade Positive Technologies att kinesiska APT31, som innan 2021 inte hade attackerat ryska mål, nu hade inriktat sig på ryska medie- och energiföretag. I samtliga dessa fall rörde det sig om spionage (Positive Technologies 2023a).

Positive Technologies listar dessutom åtta exempel på ”noterbara attacker på industriföretag” under 2022. Av dessa ägde fem rum i utlandet, och tre av attackerna drabbade rysk livsmedelssektor. Avsikten tycks ha varit sabotage snarare än spionage eller ekonomisk vinning. Positive Technologies pekar inte ut vem som ligger bakom de tre attackerna:

1. En attack i slutet av mars mot företaget Tavr, en av de största köttproducenterna i södra Ryssland, som ledde till ekonomiska förluster i termer av tiotals miljoner rubel när företagets servrar och datorer drabbades av skadlig kod.[12]
2. Hacktivister attackerade livsmedelsföretaget Seljatino i mars 2022. De tog sig in i företagets industriella kontrollsystem som styrde kylanläggningarna och försökte öka temperaturen från minus 24 till plus 30 för att förstöra 400 000 ton frusna produkter. Företaget lyckades avvärja attacken.
3. I mitten av mars 2022 attackerades det största holdingbolaget inom ryska jordbruksnäringen, Miratorg. Som ett resultat av attacken kunde företag inom holdingbolaget inte utfärda produktions-, transport- eller veterinärsdokument.

Även om Positive Technologies inte pekar ut Ukraina som ansvarigt för dessa attacker så finns anledning att misstänka att de bör sättas i samband med Rysslands krig mot Ukraina. Det är attacker som syftar till sabotage, inte till ekonomisk vinning eller spionage. Företaget noterar också att förutom statliga sektorn var det framför allt media- och transportsektorn som drabbades av ökat antal attacker 2022 (Positive Technologies 2023b).

Rostelekom Solar baserade sin analys av säkerhetssituationen på IT-området 2022 på 280 företag med fler än 1 000 anställda och från olika sektorer och regioner. Antalet IT-incidenter hade fördubblats jämfört med föregående år, men typen av incidenter hade också förändrats från kvartal till kvartal under 2022. Andelen attacker som Rostelekom Solar betecknade som allvarliga hade minskat andra

[12] Företaget Tavrs information från 24 mars 2022, http://agrocomgroup.ru/ru/news/kompaniya-tavr-podverglas-hakerskoy-atake.

halvåret och då främst därför att företagen hade satsat mer resurser på it-säkerhet. Under första halvåret hade företagen drabbats av sårbarheter till följd av att de inte kunde uppdatera programvara när leverantörer lämnade den ryska marknaden. Med tiden hade de flesta hittat sätt att täppa till sårbarheter samt gått över till rysk programvara, enligt Rostelekom Solar (2023b).

Hacktivister som attackerade ryska företag av ideologiska eller politiska skäl var främst aktiva under första halvåret efter 24 februari 2022. Små och medelstora företag var dubbelt utsatta. De drabbades även av kriminella utpressningsattacker. I takt med att stora företag allt oftare valde att inte betala de summor som kriminella hackare krävde tycks mindre företag ha blivit mer attraktiva mål. Små och medelstora företag hade mindre resurser att lägga på it-säkerhet samtidigt som de var mer sårbara i termer av att de använder frilansare inom it-branschen, hyr lagringservrar externt och använder t.ex. e-postprogram som finns att tillgå gratis. Små och medelstora företag kunde också ha svårt att bedöma hur effektiv den it-säkerhet de köpte in faktiskt var (Isakova 2023e; Chorusjevskij 2023).

4.3 Finanssektorn

Enligt Rostelekom Solar (2023c) drabbades finanssektorn näst värst efter statliga mål av 2022 års cyberattacker. Positive Technologies (2023d: 23–24) å andra sidan noterade en minskning av antalet attacker mot finanssektorn och angav att det troligen var den bäst skyddade sektorn jämfört med företag inom andra branscher. Sedan 2015 fanns inom Ryska centralbanken ett FinCERT (Financial Computer Emergency Response Team), som dessutom reformerades så sent som 2020 för att bättre svara mot branschens behov (Bujlov & Dementeva 2020). Samtidigt framgår det ur CPI:s databas att Anonymous och IT Army of Ukraine riktade in sig på finanssektorn. Denna diskrepans i beskrivningen mellan Rotelekom Solar och CPI å ena sidan och Positive Technologies å den andra kan troligen förklaras med att man mäter olika saker och på olika sätt, t.ex. huruvida kriminellas attacker ingår i underlaget.

4.4 IKT-sektorn

Rostelekom Solar (2023c) angav utifrån sitt material att 7 procent av attackerna 2022 riktades mot it-sektorn. (Den riktigt stora ökningen av attacker mot it-branchen kom först i kvartal två 2023, vilket ligger utanför den undersökta perioden i denna studie.) Dels blev attackerna överlag mer målinriktade och avancerade, dels fanns sårbarheter på grund av bristen på it-experter och uppdateringar av programvara som branschen fortfarande var beroende av (Isakova 2023b). Även Positive Technologies (2023b: 15) anger att antalet attacker gentemot it-företag ökade under 2022, med en topp i fjärde kvartalet, oktober–december 2022. De konstaterade också att läckta data i sin tur ledde till ytterligare attacker gentemot it-företagens kunder. Det stämmer väl överens med data från CPI:s databas.

En av de mer uppmärksammade attackerna var den mot videotjänsten RuTube, en tjänst som ofta beskrivs som ett ryskt alternativ till YouTube.[13] Den illustrerar också hur säkerhetsrisker och svagheter i cyberförsvar som kan vara acceptabla och t.o.m. väl affärsmässigt motiverade i fred blir mer akuta i krig. Attacken var avancerad och det verkade som att de som låg bakom hade tillgång till RuTubes källkod. Liksom andra företag både i Ryssland och internationellt, hade RuTube troligen lagt ut delar av sin programutveckling på entreprenad. Många programutvecklare som arbetade för entreprenadföretag hade ukrainsk bakgrund eller andra grunder till att vara motståndare till Rysslands invasion. Det blev snabbt ett säkerhetsproblem för Ryssland (Vendil Pallin 2020: 4).

[13] Snarare än RuTube torde den videotjänst som erbjuds av företaget VK vara bättre lämpad som eventuellt alternativ till YouTube i Ryssland.

5 Vilka låg bakom?

Enligt Positive Technologies låg alltifrån skolelever till APT:er som agerade för en regerings räkning bakom attackerna 2022. Möjligen minskade andelen ren cyberkriminalitet; något som kunde iakttas genom att skadlig kod som hotade med att radera data minskade. Men ofta var målet att stjäla data, skapa rädsla och förvirring samt att skada målens rykte (Positive Technologies 2023d: 12). Sammantaget låg Rysslands krig mot Ukraina bakom ökningen av i stort sett samtliga typer av attacker. Rostelekom Solar (2023b) var ett av få företag som både tydligt pekade på Rysslands så kallade ”militära specialoperation” som orsak och på hacktivister som skyldiga till en stor mängd attacker.

Förutom antagonistiska hot och hacktivism ökade antalet attacker med rent kriminellt uppsåt. Attackerna var enligt Group-IB (2023) inte mer avancerade än tidigare, men ryska företag var dåligt skyddade. ”Finansiellt motiverade hackare” låg bakom cirka 60 procent av attackerna mot Group-IB:s kunder under 2022 och det totala antalet incidenter hade ökat med strax under 40 procent jämfört med året innan. Dels hade aktiviteten överlag ökat, dels gjorde tillfället troligen tjuven.

Group-IB uppskattade att aktivister låg bakom endast cirka 20 procent av attackerna under 2022, men det är då värt att notera att företagets fokus ligger på cyberkriminalitet och att deras underlag därmed innehöll främst sådana attacker. Underlaget från CPI:s databas indikerar att hacktivism kan ha spelat en större roll än så. En viktig slutsats är att hacktivism kommer att vara ett viktigt inslag i väpnade konflikter framöver. När den är omfattande så skapar den en miljö full av störningar (”layers of noice”) som gör det lättare för stater att dölja sina underrättelse- och cyberoperation (Willett 2022: 17) och för cyberkriminella att agera.

Recorded Future’s Insikt Group (2023) noterade också att det cyberkriminella ekosystemet hade skakats om av Rysslands krig mot Ukraina och då särskilt inom”brödraskapet” av rysktalande aktörer (se även Giles 2023: 24; Nilsson 2023: 43). Till exempel deklarerade en del av det kriminella nätverk som använder sig av Conti-kod för utpressning sitt stöd för Ryssland. Det ledde i sin tur till att en ukrainsk del av samma nätverk lade ut det som kommit att kallas Conti Leaks på Twitter, inklusive interna chattar och källkod för Contis utpressningsprogram.[14] Ganska snart efter detta splittrades nätverket, men nya kriminella nätverk dök också snart upp (Bi.Zone 2023) och Network Battalion 65 använde läckt Conti-kod för att attackera ryska mål (Willett 2022: 17).[15] Ytterligare en anledning till att den ryskspråkiga cyberkriminella världen omstrukturerades var en rad rättsliga

[14] Denna incident loggades även av CPI och är det enda exemplet på en attack mot kriminella sektorn i deras underlag.

[15] Network Battallion 65 loggades av CPI som ”NB 65” som möjligen bakom ett antal attacker från februari till och med juni 2022, samt som associerad till Anonymous-nätverket.

åtgärder som Ryssland vidtog så sent som i januari 2022, bland annat mot nätverket REvil (Recorded Future's Insikt Group 2023).

Enligt Positive Technologies (2023d: 12) ändrades cyberhotlandskapet 2022 eftersom en rad helt nya APT-grupper uppträdde i det. De går dock inte in på vilka länder dessa grupper skulle vara kopplade till. Redan den 28 februari 2022 gick Ukrainas Ministerium för digital transformation ut med information om hur IT Army of Ukraine blockerade ryska webbsidor på några få minuter. Bland de mål som räknades upp fanns statliga resurser (Presidentens, regeringens, FSB:s, Roskomnadzors, Dumans och Federationsrådets hemsidor), finansiella resurser (Moskvabörsen, Sberbank, BestChange) mediaresurser (*Tass*, *Kommersant* och *Fontanka*), men också Belarus riksbank (Ukrainas Ministerium för digital transformation 2022). Olika analytiker uttolkar också vad IT Army of Ukraine är på olika sätt; i CPI:s och CFR:s databaser är det en hotaktör, för andra är det en rubrik för flera olika hacktivistgrupper och för återigen andra är det både Ukrainas it-försvar och offensiva it-komponent (se t.ex. Render-Katolik 2023; Soesanto 2022; Willett 2022: 16).

Kina nämns inte som land i rapporterna om it-säkerhet under perioden, men däremot nämner flera rapporter APT-grupper som har kopplats till Kina, som t.ex. APT31, Mustang Panda och Space Pirates (Positive Technologies 2023d: 12, 19). Group IB identifierade Tonto Team som ansvarigt för attacker mot ryska it-företag. Tonto Team har kopplats till kinesiska staten och riktar sedan 2009 in sig på framför allt regeringar samt organisationer verksamma inom försvar, finans och utbildning. En av Rostelekom Solars experter uppgav vidare att de under 2022 hade undersökt fem större incidenter där, förutom Tonto Team, APT15, APT31 och APT41 pekades ut som ansvariga – samtliga kopplade till kinesiska staten (Rozjkov & Gavriljuk 2023, se även *CFR Cyber Operations Tracker*). I en incidentrapport från augusti pekade Kaspersky ICS CERT (2022) ut Kina som den troliga förövaren bakom en attack mot försvarsindustriföretag i Ryssland samt i Belarus och Ukraina. Kaspersky ICS CERT hade noterat liknande angreppssätt som TA428. Den övergripande statistikrapport som Kaspersky gav ut 2022 över incidenter i samtliga länder som företaget är verksamt i, pekar otvetydigt ut Kina som det land som de flesta attackerna utgår ifrån. Även Nordkorea tycks ha varit aktivt. Åtminstone två grupper som kopplats till Nordkorea angrep ett ryskt försvarsföretag under perioden (Hegel & Milenkoski 2023).

Vid ett möte i Säkerhetsrådet i maj 2022 hävdade Putin att attackerna flerdubblats och att de var koordinerade av ”statliga strukturer, och vi vet att det helt officiellt ingår cybertrupper i vissa länders försvarsmakter” (Putin 2022). Det var tydligt i sammanhanget att han syftade på västliga länder. Däremot är det svårare att finna konkreta exempel på attacker som attribueras till västländer. Enligt Rostelekom Solar (2023c) emanerade majoriteten av överbelastningsattackerna i mars 2022 från IP-adresser i USA, men ingen ATP-grupp med koppling till USA pekades ut. Snarare finns anledning att anta att det rör sig om hacktivism som antingen utförts

från USA eller genom amerikanska IP-adresser. Det enda exemplet på en avancerad attack som eventuellt kan kopplas till USA var riktad mot ryska Appletelefoner, men dels ligger den eventuellt utanför perioden (den rapporterades åtminstone efter februari 2023), dels är anledningen till att peka ut USA främst att det är ett amerikanskt företag. Det var Kaspersky Lab som larmade om avlyssnade Appletelefoner. Att nyheten fick stor spridning kan vara Rysslands sätt att försöka höja säkerhetsmedvetandet bland egna tjänstemän (Rustamovoj & Tovkajlo 2022). Antagligen har också ryska myndigheter noterat chefen för USA:s Cyberkommando, general Paul Nakasones uttalande om att man genomfört såväl defensiva som offensiva operationer mot Ryssland, men det är fortfarande oklart exakt vad detta innebar i praktiken (Giles 2023: 15; Willett 2022: 18–19).

Endast en av de rapporter från it-säkerhetsföretag som jag har använt som källa nämner det faktum att Ryssland inledde en storskalig invasion mot Ukraina 2022. I stället gömmer de detta i allmänna formuleringar om ”ett instabilt år”, ”rådande geopolitiska situationen” (F.A.C:C.T. 2023: 3). Inte heller nämns Ukraina som ett land som ligger bakom it-attackerna som rapporterna beskriver. Det indikerar att det finns en hel del andra analytiska slutsatser som inte skrivs rakt ut, något som i sin tur också kan försvåra arbetet med att vidta rätt motåtgärder.

6 Ryska motåtgärder

De nya lagar och förordningar som den ryska regeringen raskt antog för att bekämpa it-attackerna utgjorde ytterligare en indikation på att Ryssland drabbades hårt omedelbart efter att den fullskaliga invasionen inleddes. Tvärtemot Andrej Lipovs påstående om att Ryssland var redo att stå emot alla former av attacker från omvärlden i oktober 2021 stod det klart att det fanns en rad luckor i ryskt cyberförsvar.

6.1 Lagar, förordningar och instruktioner om ökad säkerhet

Som redovisats ovan fanns en rad lagar, förordningar och system på plats för cybersäkerhet för statliga och regionala organ, men det fanns också rutiner och system inom näringslivet. Dessutom fanns utmärkta it-säkerhetsföretag i Ryssland, både ryska och utländska. Samtidigt var troligen ingen av dessa förberedda på en fullskalig invasion och de säkerhetspolitiska följder och konsekvenser för rysk it-säkerhet detta skulle få i termer av ökat antal angrepp samtidigt som it-specialister lämnade landet liksom västerländska även företag. Sanktionerna bidrog också till minskad it-säkerhet i och med att västerländsk programvara för alltifrån operativsystem till industriella styrsystem inte längre kunde uppdateras så att sårbarheter eliminerades. Troligen inledde också Ryssland sitt utökade krig mot Ukraina med ett ofta lågt it-säkerhetsmedvetande inom många företag och statliga myndigheter (Dubov 2023: 3).

Trots att det redan tidigare var obligatoriskt för statliga myndigheter och andra organisationer som ansvarade för kritisk informationsinfrastruktur att ansluta sig till GosSOPKA rapporterade FSB hösten 2022 att antalet anslutna till systemet hade ökat under året (Isakova 2023d). Det indikerar att Ryssland antingen definierade ytterligare organisationer som ansvariga för kritisk informationsinfrastruktur eller att vissa helt enkelt hade undvikit att ansluta sig tidigare.

En av de omedelbara åtgärderna som vidtogs för att skydda främst den ryska regeringen webbsidor från överbelastningsattacker var geoblockering. Det innebar att tillgång till dessa webbsidor var möjlig endast för datorer med ip-addresser[16] geografiskt belägna på ryskt territorium samt troligen i länder som ingår i Oberoende staters samvälde (OSS) och Georgien.[17] Redan i mars utfärdade Ministeriet för digital utveckling en instruktion, i vilken ryska bredbandsoperatörer ålades att

[16] En ip-adress (internetprotokolladress) är ett unikt nummer som identifierar en dator som ansluter till internet.

[17] I februari 2022 ingick följande länder i OSS: Armenien, Azerbajdzjan, Belarus, Kazakstan, Kirgizistan, Moldavien, Ryssland, Tadzjikistan, Uzbekistan. Turkmenistan deltar men är inte formellt full medlem.

flytta webbsidor och webbtjänster till ryska servrar, dvs. servrar belägna i Ryssland och i rysk ägo. Åtgärden gav upphov till rykten och farhågor om att detta innebar förberedelser för att den 11 mars aktivera Rysslands *kill switch*. Snarare rörde det sig om förberedelser för att skydda landets internetsegment från pågående cyberattacker. Instruktionen utfärdades med en uppmaning om försiktighet samt att se över lösenord (Vendil Pallin 2022: 3).

När Putin inledde Säkerhetsrådets möte den 20 maj 2022 hävdade han först att Ryssland hade lyckats avvärja en ”cyberaggression” eftersom man hade varit väl förberedd och arbetat systematiskt de senaste åren. Men han övergick snabbt också till att beskriva problemen och de åtgärder som behövde vidtas (Putin 2022). Bland de åtgärder Putin nämnde fanns presidentdekret nr. 250 som hade publicerats den 1 maj 2022. Det pekade ut konkreta svagheter som skulle rättas till inom rysk it-säkerhet. En vice chef på varje statlig organisation, inklusive på så kallade ”strategiska företag” och kritisk infrastruktur, skulle vara ansvarig för organisationens informationssäkerhet och en avdelning för informationssäkerhet skulle skapas (§1:a, b). Alla statliga organ ålades dessutom att värdera och inrapportera säkerhetsnivån för sina respektive informationssystem till regeringen före den 1 juni 2022 (§4). Efter den 1 januari 2025 skulle det heller inte längre vara tillåtet att använda it-säkerhetsprogram som importerades från icke-vänliga länder (§6). Ytterligare en viktig punkt i dekret nr. 250 var instruktionen till FSB att ackreditera centrum för olika branscher inom ramen för GosSOPKA (§5; se även Positive Technologies 2023d: 8).

Ordföranden i Dumans utskott för informationssäkerhet, Aleksandr Chinsjtejn, och ordföranden i Federationsrådets utskott för konstitutionella lagstiftning och statens utveckling, Andrej Klisjas, hade redan i april initierat ett lagförslag enligt vilket samtliga organisationer som hanterar personuppgifter – närmare 400 000 enligt en rysk analytiker – skulle vara tvungna att rapportera in till varje incident till GosSOPKA. Lagförslaget ålade dem att begära tillstånd från Roskomnadzor varje gång de avsåg att föra personuppgifter över landets gränser. Roskomnadzor kunde vägra utifrån ”skydd av konstitutionella systemet; medborgares moral, hälsa, rättigheter och lagliga intressen; landets försvar; samt statens säkerhet” (Gavriljuk 2023). Formuleringen var ur ett juridiskt uttolkningsperspektiv minst sagt ospecifik. Den ligger dock väl i linje med rysk säkerhetspolitik som den formuleras t.ex. i Nationella säkerhetsstrategin och dess emfas på ryska traditionella värderingar, på befolkningens hälsa och reproduktion som en säkerhetsfråga samt på statens primat.

Näringslivets olika intresseorganisationer protesterade dock eftersom det skulle innebära ökade kostnader, men analytiker påpekade också att det skulle kräva investeringar i GosSOPKA för att hantera mängden av inkommande information. Det fanns betydande frågetecken vad gäller hur effektivt lagförslaget skulle förhindra framtida läckor. Det vanligaste skälet till att ryska internetanvändares personliga data läckte var misstag och att illojala medarbetare sålde informationen,

inte hackerattacker (se t.ex. Ustinova 2023). Lagförslaget skulle däremot innebära att FSB fick direkttillgång till ytterligare information om landets befolkning. Det fanns heller inga mekanismer som innebar att FSB genom GosSOPKA återkopplade med information till näringslivet som skulle kunna bidra till en bättre lägesbild för det i arbetet med att förhindra framtida läckor eller andra attacker (Isakova 2023c). Det kan också ha varit en viktig förklaring till varför många företag stod illa rustade.

Tidigare hade bötesbeloppet för dataläckor varit lågt, vilket innebar att det var mindre kostbart för företag att betala böter än att vidta åtgärder för att förhindra dem. Under hösten 2022 låg ytterligare ett lagförslag i Duman om att böterna för dataläckor framöver skulle höjas väsentligt och tas ut i termer 1–3 procent av företagets årsomsättning (*Kommersant* 2022) och hösten 2023 resulterade ändringar av lagen ”Om information” i att *hosting*-leverantörer ålades att rapportera in attacker till GosSOPKA, samt att delta i årliga cyberövningar (Isakova 2023d). Ytterligare ett tecken på att Ryssland oroade sig för att personuppgifter var dåligt skyddade kom under 2023. Då förelåg ett lagförslag om att personuppgifter för anställda inom så kallade kraftministerier, som t.ex. FSB och Nationalgardet (*Rosgvardija*), skulle behandlas i särskilt ordning (Lagförslag 6526-P4-MM, 3 augusti 2023).

Ett behov att övergripande inventera it-säkerheten inom federala organ fanns uppenbarligen också. Den 13 maj 2022 utfärdade regeringen en instruktion (nr. 860) med tillhörande förordning om att genomföra ett experiment för att höja säkerheten för federala myndigheters informationssystem. Ansvarigt ministerium var Ministeriet för digital utveckling. Experimentet skulle pågå fram till 30 mars 2023. Syftet var att konstatera hur väl skyddade statliga informationssystem var, att inventera vilka säkerhetsskydd som existerade, hur en angripare kunde använda existerande sårbarheter samt utarbeta en lista på åtgärder för att minska sårbarheter. Även FSB och FSTEK skulle vara involverade i experimentet.

Andra åtgärder var mer specifika för att täppa till sårbarheter. Ryska myndigheter ville också skapa en högre grad av it-säkerhet genom att knyta ryska myndigheter och regionala samt kommunala organ till informationsinfrastruktur som de kunde utöva mer direkt kontroll över. I slutet av oktober 2022 utfärdade den ryska regeringen en föreskrift som innebar att samtliga statliga och regionala organisationer endast fick använda mejladresser som använde domännamn och nätadresser som ingår i den ryska nationella domänzonen från och med den 1 december samma år (Regeringsföreskrift nr. 1934). Från och med mitten av 2022 fick ryska regeringstjänstemän och ministrar inte längre ta med sig sina iPhones in till sammanträden eftersom ryska säkerhetstjänster ansåg att det innebar en säkerhetsrisk. Kaspersky Lab hade noterat att deras medarbetares iPhones hade hackats, men FSB gick ett steg längre och anklagade Apple för att samarbeta med amerikanska National Security Agency (Plamenev 2023). Kanske var det mer anmärkningsvärda dock att denna säkerhetsåtgärd kom först i juni 2022 (@Faridaily 2022).

Antagligen låg ett mer allmänt behov av att öka medvetenheten om it-säkerhet bakom initiativet den 9 december 2022 att skapa ett Kompentenscentrum för informationssäkerhet, som skulle inleda sin verksamhet från och med 2023. Ett forskningsinstitut, FGBU NII Integral, som lyder under Ministeriet för digital utveckling och redan övervakar och reagerar på it-incidenter, skulle utveckla detta centrum liksom även olika centrum för it-säkerhet för olika näringslivsbranscher. Ett kompetenscentrum för informationssäkerhet existerade i själva verket redan inom ramen för nationella programmet ”Digital ekonomi”, väl förankrat inom näringslivet. Det var oklart hur samarbetet eller gränsdragningen mellan det redan existerande kompetenscentrumet och det som nu skulle skapas skulle struktureras (TASS 2022).

6.2 Rysk mjuk- och hårdvara

De sanktioner som följde för Ryssland på den fullskaliga invasionen innebar, som nämnts ovan, bland annat att ryska företag inte längre fick tillgång till uppdateringar av programvara eller kunde använda sig av säkerhetsverktyg från västliga producenter. Även i direkt frånvaro av sanktioner valde många västliga företag, som Cisco, att avsluta sin verksamhet i Ryssland. Det innebar också att ryska företag som använt västlig programvara, hårdvara och it-säkerhetslösningar stod utan nödvändiga uppdateringar samtidigt som ryska lösningar saknades eller krävde omfattande utveckling för att utgöra en fullgod ersättning (se t.ex. Isakova 2023a).

Målsättningen att öka andelen rysk program- och hårdvara fanns sedan länge. Informationssäkerhetsdoktrinen från 2016 understryker att det är ett geopolitiskt hot att vissa länder är tekniskt överlägsna (se främst §§17, 19 och 25). Enligt ett omfattande regeringsprogram för använda digital teknik för att övervaka och effektivisera statlig styrning till 2030, var ökad produktion av rysk mjuk- och hårdvara ett av målen för att öka informationssäkerheten (Regeringsförordning nr 2998-r, 22 oktober 2021). Sanktionerna, den djupgående konfrontationen med Väst och it-attackerna fick regeringen att vilja skynda på denna process, men i praktiken var det svårare efter februari 2022 än det hade varit tidigare. Regeringens krav på ”rysk” programvara innebar snarare ett beroende av kinesiska produkter (Dubov 2023: 3).

Det är också tydligt att det inte saknades ivriga kandidater som ville ta del av statliga subventioner för att producera ryska alternativ. Hösten 2022 presenterade Rostelekom en ”högnivåstrategi för att utveckla det nationella mobila ekosystemet på basis av operativsystemet ”Aurora” 2022–2030. Rostelekom föreslog tre produktionslinjer för ryska smarta mobiler och läsplattor – för statliga tjänstemän, för näringslivet och för vanliga användare. Enligt ett försiktigt scenario skulle endast produktion ske endast på basis av statliga beställningar; då skulle 1,5 miljoner enheter tillverkas till 2030. Ett mer expansivt maxscenario förutsåg en produktion på 65,9 miljoner enheter till 2030, men det förutsatte massivt statligt stöd, förbud

mot att använda ryska operativsystem på importerade enheter och kvoter för import. Ett förslag var även att ”socialt utsatta” skulle få telefoner inom ramen för ett federalt projekt ”Social telefon”. Enligt flera analytiker lät strategin som en utmaning i praktiken, både givet vilka kostnader den skulle innebära för staten och den produktionsvolym som rysk industri hade 2022 – mindre än en miljon enheter per år (Kornev, Korolev & Tisjina 2022). Kostnaden för att sjösätta ett mobilt ekosystem, där Rostelekom skulle ta ansvaret för att utveckla operativsystemet, uppskattades till strax under 500 miljarder RUR. Det skulle rymmas inom tidigare program som nationella projektet ”Digital ekonomi”. Enligt Rostelekom var strategin nödvändig på grund av att ryska användare och företag hotades att stängas av från Google och Apple. I det utkast till handlingsplan som åtföljde strategin antyddes också att tillverkningen av mobila enheter i själva verket skulle ske i Kina – eller möjligen i Ryssland men då i form av montering av kinesiska komponenter (Kornev & Korolev 2022).

Det fanns således tecken på att Ryssland ville röra sig mot ett ryskt cyberekosystem (Sherman 2023), men svårigheterna och kostnaderna det skulle innebära var betydande. Mer specifikt ville den ryska regeringen accelerera övergången till ryska it-säkerhetsverktyg som man redan tidigare uppmuntrat till. Enligt presidentdekret nr 250 skulle det som nämnts ovan vara helt förbjudet att använda it-säkerhetsprodukter från ”ovänliga länder” från och med 1 januari 2025.[18] Tillsammans ledde detta till en ökad efterfrågan på ”rysk” programvara, på ryska it-säkerhetsföretags lösningar. Positive Technologies (2023d: 4) konstaterade i sin rapport att inget av de företag som stått bakom avancerade brandväggslösningar på tillräcklig nivå var ryska. ”För att överbrygga denna klyfta till Väst måste man hitta en unik väg”, konstaterades i rapporten. Det hade tagit västliga företag decennier att nå dit samtidigt som den tiden inte fanns för Ryssland nu.

Onekligen fanns en ökad efterfrågan på ryska it-säkerhetslösningar när västliga sådana inte längre var tillgängliga. Samtidigt var det dock en besvärlig uppgift eftersom it-säkerhetslösningar ska fungera med operativsystem och annan programvara. För att nå den ”teknologisuveränitet” som varit ett slagord för den ryska regeringen borde även hårdvaran vara rysk, enligt ryska företrädare för it-industrin och regeringstjänstemän med ansvar för området (Morozova 2023; se även Sherman 2023). Förutom efterfrågan på ryska it-säkerhetslösningar ökade även antalet företag som vände sig till kinesiska leverantörer som tidigare hade haft en liten del av marknaden (5% enligt en undersökning 2022, se Isakova & Kornev

[18] Ryssland kallade redan 2018 USA för ett ”ovänligt land” som en svarsåtgärd. Listan utökades 2021 med Tjeckien som ett svar på att Prag hade anklagat ryska specialförband för att ha sprängt ett ammunitionslager i Vrbětice och därefter utvisat 18 ryska diplomater. Listan över ovänliga länder fylldes snabbt på under 2022 med samtliga länder som anslöt sig till sanktionerna mot Ryssland och omfattade alltifrån EU-länderna, Taiwan Singapore, Japan och Sydkorea till San Marino, Mikronesien och alla länder som ingår i Brittiska samväldet. Se t.ex. https://www.rbc.ru/politics/03/08/2023/62e3b3f59a79472ed9cfd9ee.

2023). Kinesiska företag kunde dock inte komma ifråga för leveranser av säkerhetslösningar till statliga myndigheter, företag och institutioner, ej heller för objekt som klassats som kritisk informationsinfrastruktur. För det krävs en licens från FSTEK, vilket inte är omöjligt att få för utländska företag, men ryska företag hade fortsatt en fördel på den marknaden (Isakova & Kornev 2023). Samtidigt torde det också stå klart att det fanns hinder på vägen. Inte ens statliga organisationer ålades att ersätta sina it-säkerhetslösningar från icke-vänliga länder tidigare än 1 januari 2025 (Presidentdekret nr. 250, 1 maj 2022: §6). Det tyder på att övergången innebar en utmaning.

En stor utmaning för Ryssland kommer att vara att ta fram rysk programvara som inte innehåller nya sårbarheter. Microsoft har under decennier arbetat med att jaga så kallade *zero-day-exploits*[19] efter att först ha försökt att negligera problemet. Allt talar för att även rysk programvara när den används brett kommer att stimulera hackare att leta sårbarheter. Positive Technologies (2023d: 13) förutsåg att 2023 skulle kännetecknas av att attackerande grupper sökte efter *zero-days* i ryska operativsystem baserade på Linux som Astra Linux, ALT Linux och RED OS (se även Positive Technologies 2023b: 4). En god indikation på hur pass väl Ryssland lyckas täppa igen *zero-days* kommer att vara priset för sådana på Dark Net, ju lägre pris desto större fler sårbarheter finns troligen.

6.3 Personal inom it-området

En av de största utmaningarna för Ryssland kommer dock att bestå i att utbilda, attrahera och behålla kompetent it-personal. Redan innan februari 2022 fanns uppskattningar om att det fattades specialister inom it-branschen (Engvall, Gustafsson & Vendil Pallin 2021: 47ff). En analys av problemet fanns t.ex. i regeringens prognos teknologisk utveckling mot perioden 2030 (Regeringsbeslut, nr. DM-P8-5, 3 januari 2014). I december 2021 uppgav Sberbank, som är en tongivande aktör på det digitala området i Ryssland, att bristen på personal inom it-säkerhetsområdet var katastrofal och uppgick till 20 000. Än mer oroande enligt Sberbank var bristen på lärare för att utbilda ny personal (RIA Novosti 2021). Något som komplicerar bilden är också att ”it-specialister” knappast är en homogen grupp utan består i specialister på olika system och olika områden. Enligt en rapport från april 2023 som regeringen hade beställt hade efterfrågan på it-personal ökat med över 60 procent på ett år. Det var framför allt personal med erfarenhet snarare än nyutbildade som företagen letade efter. Inte sällan var det en specifik expertis som efterfrågades, exempelvis erfarenhet av Python eller av att administrera databaser (Isakova et al. 2023).

[19] Dagnollattack, dvs. ett dataintrång som utnyttjar en sårbarhet som inte varit publikt känd innan angreppet och därmed saknar färdiga lösningar från säkerhetsföretagen. (Försvararen har noll dagar att uppdatera sina program.)

Trots en rad åtgärder tycks det ha varit besvärligt att attrahera it-personal. Att till exempel undanta it-personal från mobilisering och erbjuda ökad ersättning tycks inte ha lockat många att återvända. Problemet förvärrades av att den ryska regeringen och landets företag av säkerhetsskäl var mindre benägna att acceptera att anställda arbetade på distans, särskilt från utlandet. Vid en nationell konferens med cybersäkerhet som tema sommaren 2023 konstaterade talarna att ett av de stora problemen fortfarande var bristen på it-specialister och då särskilt på säkerhetsområdet (Morozova 2023).[20]

Kanske var det därmed inte förvånade att när morötter fungerade sämre kom också förslag på piskor som skulle lösa problemet. Till exempel började anställda inom företaget VK få krav på att återvända hem för att få behålla jobbet under 2023 (Pljusjtjev 2023). Wagnerledaren Jevgenij Prigozjin ville göra det svårare för it-personal att lämna landet (Dubov 2023: 3) och ett förslag från Dumaledatmoten Aleksandr Chinstejn som visserligen var ett skämt fick många att frukta det värsta. Han skämtade om att skapa ”it-sjarasjkor”, dvs. arbetsläger för dömda it-arbetare enligt hur sovjetiska myndigheter hade tvingat forskare att arbeta i läger (Dubov 2023: 3). Samme Chinsjtejn föreslog i september 2023 att hackare som agerar ”i Rysslands intresse” på ryskt territorium eller utomlands skulle bli straffbefriade. Det skedde efter att utskottet för informationssäkerhet hade haft ett möte för att diskutera Rysslands cybersäkerhet (Tass 2023).

[20] Konferensen IT IS conf var den fjärde i ordningen och ägde rum i Jekaterinenburg (https://itisconf.ru/livebroadcast2023). Kaspersky Lab var strategisk partner och företagen Positive Technologies och Kod bezopasnosti var generella partners.

7 Slutsatser – kriget som utvärdering av cyberförberedelser

Internationella rankningar, analytiker samt ryska tjänstemän och politiker var relativt eniga i att ranka Rysslands cyberförmåga högt. Att Ryssland skulle drabbas så pass hårt av it-attacker från och med 24 februari 2022 kom dock som en överraskning för många – kanske inte minst för ryska myndigheter. Att ha en god offensiv cyberförmåga tycks inte per automatik resultera i en god försvarsförmåga på it-området.

7.1 Attackernas karaktär

Attackerna var till en början relativt enkla överbelastningsattacker utförda av hacktivister som visade sitt stöd med Ukraina. De blev mer avancerade allteftersom Ryssland fortsatte sitt krig mot Ukraina. Samtidigt fortsatte tidigare attacker, t.ex. de som Kina sedan länge bedrivit mot ryska industrier och forskningsinstitut för att inhämta underrättelser. Även kriminella it-attacker blev mer av ett problem än tidigare för ryska företag. Det skedde troligen som ett resultat av att sårbarheterna blev fler när västerländska företag lämnade Ryssland, men också som ett resultat av att kriminella grupperingar med ursprung i före detta sovjetiska republiker inte längre var lika försiktiga i att angripa ryska intressen.

Om framför allt ryskt näringsliv tidigare drabbades av it-attacker, var det främst ryska myndigheter och samhällsfunktioner med en viktig roll i Rysslands invasion av Ukraina som drabbades från och med februari 2022. Allteftersom attackerna blev mer avancerade drabbades även ryska it-bolag, inklusive it-säkerhetsföretag. Till det ska läggas att alltifrån stora banker till småföretag drabbades av kriminella attacker liksom av ett allmänt sämre cybersäkerhetsklimat och brist på personal som skulle kunna åtgärda problemen.

Att attribuera it-attacker är aldrig enkelt och sker ofta med betydande grad av osäkerhet. Som framgår av diskussionen om källor inledningsvis finns också starka skäl för såväl attackerande part som den som utsätts att antingen överdriva eller spela ned attackens betydelse eller förneka att den alls ägt rum. Utifrån CFR:s och CPI:s databaser, ryska it-säkerhetsrapporter och medierapportering samt de motåtgärder som vidtogs går det dock att fastställa att antalet attacker ökade samt att det inledningsvis rörde sig om internationella hacktivistnätverk som inte sällan agerade på uppmaning av Ukrainas initiativ, IT Army of Ukraine. Ryska uttalanden om att Väst låg bakom går inte att belägga i materialet. Det är också tydligt att de APT:er som var verksamma snarare var hackergrupper i länder som redan tidigare var aktiva i att t.ex. bedriva underrättelseverksamhet gentemot Ryssland.

Denna studie visar på värdet av att arbeta med flera olika sorters källor för att kunna analysera om en bred våg av angrepp och hur de påverkar ett lands säkerhetspolitiska läge, att det är vanskligt att förlita sig på t.ex. bara en databas (se även Lucas Kello 2018).

7.2 Krig, felbedömning av egen förmåga och en strategisk fälla

Att Ryssland drabbades mer än vad landets ledning hade förutsett är också tydligt utifrån de åtgärder som ryska myndigheter vidtog – alltifrån geoblockeringar, förbud mot västlig programvara i känsliga sammanhang. Presidentdekretet som ålade alla ryska myndigheter att skapa en it-säkerhetsavdelning är talande liksom det faktum att problemen med stulna persondata fortsätter att plåga Ryssland. Det tycks också som att det fortsatt finns ett betydande glapp mellan de cybersäkerhetssystem som FSB har ansvar för, främst inom ramen för GosSOPKA, och det som bedrivs inom resten av samhället. Till och med efter februari 2022 tycks de åtgärder som vidtogs främst ha syftat till att samla information och fungera som kontrollinstrument under FSB:s egid.

Vilken är då förklaringen till att Ryssland som rankades så pass högt vad gäller förmåga inte kunde försvara sig bättre i cyberdomänen? Svaret kan delas upp i tre huvudsakliga förklaringar. För det första, är det en helt annan sak att försvara sig i fred eller t.o.m. i så kallad gråzon jämfört med när ett krig pågår. För det andra överskattade Ryssland sin cyberförsvarsförmåga samtidigt som ryska myndigheter underskattade risken för en motattack. Slutligen bidrog rysk informationssäkerhetsdoktrin och hur den formulerats och i praktiken genomförts troligen till att cybersäkerhet inte togs på tillräckligt stort allvar av den ryska politiska ledningen.

Krig förändrar med ens reglerna för vad som är tillåtet och vad som är en acceptabel risk. I Rysslands fall, ville den politiska ledningen inte heller vidgå att det var ett krig utan hänvisade till den ryska invasionen som ”en militär specialoperation”, trots att Ryssland redan under första året hade förlorat fler soldater än t.ex. Sovjetunionen under tio års krig i Afghanistan. I ryska it-säkerhetsföretags rapporter, ryska analytikers och regeringstjänstemäns uttalanden och journalisters rapportering nämns som regel inte anledningen till att Ryssland blev ett mål för en våg av attacker från februari 2022.[21] Den politiska ledningen i Moskva var mån om att kriget inte skulle bli impopulärt bland befolkningen. Ryssland var dock krigförande part och mer känsligt för avbrott i samhällstjänster och näringsliv – den part som har flest funktioner igång är också mest sårbar för it-attacker. Ukraina

[21] Som konstaterats ovan, nämns den ”militära specialoperationen” alls bara av it-säkerhetsföretaget Rostelekom Solar (2023a, b, c).

slogs för sin existens som stat och befolkningen hade därmed troligen högre tolerans för t.ex. avbrott i betalningssystem.

Rysslands invasion resulterade dessutom i att Väst enades kring sanktioner i en omfattning som Moskva inte hade förutsett. Samtidigt lämnade västliga it-företag den ryska marknaden. Det resulterade bland annat i att ryska system blev sårbara då de inte längre uppdaterades, då västliga it-säkerhetslösningar inte längre var ett alternativ för ryska företag och it-personal lämnade landet.

Inte heller tycks det ha föresvävat den ryska sidan att den kunde drabbas av en våg av attacker från hacktivister och att Ukraina skulle uppmana till sådan hacktivism. Världen var van vid att se exempel på hackare som agerade samfällt i ryskt intresse, men att en liknande attack skulle vändas mot Ryssland kom som en överraskning. Rysslands invasion ledde också till att den borgfred som länge rått mellan kriminella cybernätverk och den ryska staten bröts. Cyberkriminella hade tidigare kunnat agera från ryskt territorium så länge som ryska intressen inte drabbades, men kriget ledde till att även kriminella nätverk splittrades utmed konfliktens skiljelinjer mellan Ukraina och Ryssland. Kriget resulterade dessutom i att ytterligare skadlig kod som använts i attacker inledningsvis kom ut på den kriminella marknaden och blev tillgängliga även för dussinhackare (se t.ex. Isakova 2023a). Sammantaget drabbades ryska företag och andra resurser av ökad cyberkriminalitet samtidigt som de inte längre hade tillgång till säkerhetsuppdateringar för västliga it-lösningar som de tidigare byggt sin säkerhet på.

Förutom kriget var Rysslands överskattning av sin egen förmåga en viktig förklaring till varför landet var sämre rustat än väntat. Förutom de internationella rankningarna av Rysslands cyberförmåga, som kan ha bidragit till rysk överskattning, rapporterade företrädare för ryska myndigheter att it-beredskapen var god så sent som 2021. Här kan även rysk politisk kultur ha spelat in. Att rapportera in problem är sällan karriärfrämjande för ryska tjänstemän och ingen oberoende granskning sker i ett allt mer repressivt och korrupt system där alltmer information dessutom inte längre är öppet tillgänglig. När attackerna väl hade börjat eliminerade ryska myndigheter en rad sårbarheter, men det tycks även ha funnits ett element av inaktivitet (Giles 2023: 29).

Samtidigt underskattade Moskva också Ukrainas förmåga att svara på cyberområdet precis som man hade underskattat landet militärt. Konflikten i cyberdomänen mellan Ryssland och Ukraina var troligen den första större mellan relativt jämbördiga parter (Willett 2022: 22). Ukraina lyckades motivera ”civila hackare” internationellt samtidigt som IT Army of Ukraine blev en samlande symbol för motstånd mot Rysslands invasion. Med tiden mobiliserade också grupper och individer som agerade i Ukrainas intresse förmåga till att genomföra mer avancerade attacker.

Slutligen är det värt att reflektera över hur rysk informationssäkerhetsdoktrin kan ha bidragit till att Ryssland var sårbart för cyberoperationer. Det faktum att

Ryssland sällan eller aldrig skiljer ut teknisk informationssäkerhet bidrog troligen till att kognitiv informationssäkerhet ofta stod i fokus för tongivande personer i det ryska politiska systemet. Det var troligen inte brist på kunnande om cybersäkerhet i Ryssland som helhet som var problemet utan bristen på politisk uppmärksamhet, systematik och samordning av it-säkerhet i samhället som helhet. Att skydda samhällets it-system och deras funktionalitet är komplext och kräver it-expertis, men också samordning, inventering av t.ex. ekonomiska sårbarheter som är förknippade med beroende av it-tjänster. Det är en formidabel uppgift för alla länder och kommer att kräva tuffa prioriteringar, men mycket tyder på att de ansvariga i främst det ryska Säkerhetsrådet prioriterade att kontrollera vilken information Rysslands befolkning kunde få tillgång till framför ett systematiskt cybersäkerhetsarbete.

Retoriken kring ett suveränt internet betonade visserligen behovet säkerhet från attacker utifrån, men det var aldrig tydligt om det var främst tekniska eller kognitiva sådana som stod i centrum. Ryssland använde aldrig sin *kill switch* för att skydda ryska nät mot it-attacker 2022–2023, men har använt tekniken som åtföljde ”ett suveränt internet” för att tysta protester i Dagestan, Basjkortostan och Sacha (Jakutien). Det stärker slutsatsen att det huvudsakliga målet var att kontrollera vilken information ryska medborgare kunde få tillgång till snarare än skydd mot cyberoperationer.

Den ryska omedelbara instinkten tycks också ha varit att införa mer central kontroll och då främst i termer av ytterligare mandat för FSB att centralt skapa en lägesbild inom ramen för GosSOPKA. Likaså införde den ryska regeringen åtgärder som syftade till att t.ex. öka kontrollen över vilken programvara som används. Erfarenheterna från Ukraina tyder snarare på att motståndskraft mot cyberoperationer gynnas av en diversifierad marknad (Nilsson 2023: 57–58). Framtiden kommer att utvisa om Rysslands åtgärder på detta område leder till ökad cybersäkerhet.

7.3 Rysslands it-försvar, erfarenheter för andra länder och vidare konsekvenser

Få i Väst fördömde den hacktivism som riktade sig mot Ryssland efter invasionen, men den väcker en rad frågor på ett principiellt plan om när dataintrång, om alls, är motiverat och om den som väljer att agera som hacktivist i en konflikt också ska betraktas som deltagare i konflikten (Rodenhäuser & Vignati 2023; se även Tidy 2023). Det dröjde t.ex. inte länge innan ryska Killnet tillsammans med Rysslands-affilierade AnonymousSudan uppmanade till attacker mot Israel efter Hamas attack i oktober 2023 (https://t.me/killnet 2023; se även Roussi & Miller 2023). Experter har noterat att dilemman uppkommer när det gäller vilken information som är känslig att ha på t.ex. mobiltelefon i en väpnad konflikt. Som Keir Giles (2023: 31) påpekar är frågan om huruvida ukrainska civila kan betraktas som

kombattanter nästan av akademisk karaktär i Rysslands krig mot Ukraina eftersom ryska styrkor inte har följt internationell humanitär lag i konflikten. Risken är dock att vissa av de fall av krigsbrott som Ukraina nu dokumenterar kan bestridas när det gäller civila som har rapporterat in ryska militära förflyttningar till exempel (Giles 2023: 31–32). Internationell rätt kan idag inte svara på frågor som hur hög grad av hacktivism och skada av den som eventuellt skulle utgöra grund för militära försvarsåtgärder från angripet land. Kan det innebära att tredjeland blir föremål för anfall eller ett företag som tillhandahåller en tjänst? Det här är bara några av de frågor som it-attacker i krig ger upphov till. Sammantaget aktualiserar exemplen på användande av it-attacker och digitala verktyg svårigheterna att skilja mellan vad som är civila eller militära mål i väpnade konflikter (se även Karlzén 2020a: 37; Winther & Nilsson 2023).

Den roll som större internationella it-företag har spelat i cyberförsvaret för Ukraina respektive är också värd att nämna. Ukraina fick omedelbart stöd från en rad internationella it-företag, något som Ryssland saknade (Giles 2023: 16). Det väcker frågan om vad privata företag riskerar när de blir involverade direkt i en väpnad konflikt (Giles 2023: 19–20) och vad som händer när företag lämnar länder som ett resultat av krig eller nära förestående krig. Flera analytiker har uppmärksammat hur Ukrainas militära förmåga påverkades av Elon Musks beslut att först erbjuda Starlink och sedan i ökad grad dra undan det. Färre har noterat de konsekvenser som internationella företags beslut fick för rysk säkerhet. I Rysslands fall lämnade flera västliga it-företag snabbt landet, något som fick direkta konsekvenser för landets cyberförsvar. En översyn av sårbarheter beroende av en viss programvara eller hårdvara resulterade i, skulle troligen ha tjänat Ryssland bättre än tre övningar för att koppla bort det ryska segmentet av internet från omvärlden. De flesta länder har idag beroendekedjor på it-området där det finns all anledning att analysera och komma fram till vilka prioriteringar som måste göras vad gäller att ha förmåga att ersätta produkter eller tjänster i ett skarpt läge.

Rysslands invasion av Ukraina riskerar dessutom att driva på en fragmentering av internet i ett västligt och östligt block. Dels kommer Ryssland att tvingas att välja kinesisk hårdvara och programvara i ökad omfattning som ett resultat av sanktioner och västliga företags ovilja att handla med landet. Dels har ryska myndigheter t.ex. förbjudit användandet av västliga it-säkerhetslösningar och blockerat företag som Meta och Twitter liksom även alltifrån oberoende nyhetssajter till civilsamhällsorganisationer och oppositionell verksamhet inom det Ryssland definierar som sitt nationella segment av internet. Rysslands invasion får således troligen konsekvenser långt bortom Ukraina och i fler domäner än endast den rent militära.

Referenser

@denis-19. 2023. “Eksperty pojasnili, gde imenno i kak dolgo RKN i operatory svjazi v notj s 4 na 5 ijulja ’vykljutjali mezjdunarodnyj internet’”. *Habr*, 7 juli. https://habr.com/ru/news/746688/ (2024-02-01).

Adamsky, Dmitry. 2023. *The Russian Way of Deterrence: Strategic Culture, Coercion, and War*. Standford; California: Standford University Press.

Bi.zone, 2023. *Lost & Found: Issledovanije trech kibergruppirovok, ispolzujusjtjich utetjki program-vymogatelej v atakach na rossijskije organizatsii, september.* https://bi.zone/upload/for_download/BI_ZONE_research_leaked_ransomware_attacks_RU.pdf (2023-09-27).

Bujlov, Maksim and Ksenija Dementeva. 2020. ”FinTsERT okontjen”. *Kommersant*, 12 november. https://www.kommersant.ru/doc/4566802 (2023-11-09).

Balasjova, Anna & Jasakova, Jekaterina. 2023. ”V Rossii proverili ustojtjivost Runeta na slutjaj ego otkljutjenija izvne”. *RBK*, 5 juli. https://www.rbc.ru/technology_and_media/05/07/2023/64a569439a7947106d06262b (2024-01-31).

CFR Cyber Operations Tracker. Inget datum. ”Our Methodology”. Council of Foreign Relations (CFR). https://www.cfr.org/cyber-operations/#OurMethodology (2023-11-16).

Chabudilina, Jekaterina. 2023. ”Roskomnadzor vyjavil problemy s ’zjivutjestiu’ setej posle utjenij po ustojtjivosti Runeta”, *Forbes*, 24 oktober. https://www.forbes.ru/tekhnologii/499096-roskomnadzor-vyavil-problemy-s-zivucest-u-setej-posle-ucenij-po-ustojcivosti-runeta (2024-01-19).

Chorusjevskij, Ivan. 2023. ”Konkurenty strasjneje chakerov”. *Kommersant*, 1 mars. https://www.kommersant.ru/doc/5844222 (2023-03-02).

CNews Analytics, senast uppdaterad 10 november 2022, https://www.cnews.ru/reviews/security2022/review_table/12b4f5538e57db6abd0a5e202c744bc94f1ec876 (hämtad 2023-09-27).

Computer Sweden. Inget datum. “IT-ord: Ord och uttryck i it-branschen”. https://it-ord.idg.se/

Cyber Peace Institute. “FAQ – Data & Methodology”. Cyber Peace Institute (CPI). https://cyberconflicts.cyberpeaceinstitute.org/faq/data-and-methodology (2023-11-14).

Demurina, Gajana. 2020. ”Minkomsvjaz perenesla utjenija po ’suverennomu Runetu’ iz-za koronavirusa”. *RBK*, 20 mars. https://www.rbc.ru/technology_and_media/20/03/2020/5e7456be9a7947247c8bf391 (2024-01-19).

Dubov, Dmytro. 2022. ”The War in Cyberspace”. *ICDS Brief Russia’s War in Ukraine Series*, nr. 2 (maj). https://icds.ee/en//download/47064616/ (2023-03-08).

Duman. Lagförslag 6526-P4-MM, 3 augusti 2023, xxx (2023-11-07).

Eckel, Mike. 2023. ”Sachkov’s Revenge: Jailed on Treason Charges, A Russian Cybersecurity Exec Goes on the Offensive”. *Radio Free Europe – Radio Liberty*, 23 juni. https://www.rferl.org/a/32472306.html (2023-09-27).

Engqvist, Maria. 2024. *Russian Military Capability at War*. FOI-R--5502--SE, FOI, Stockholm, april.

Engvall, Johan, Gustafsson, Pär & Vendil Pallin, Carolina. 2021. *Framtid med förhinder: Rysk teknisk FoU till 2030*. FOI-R--5204--SE, FOI, Stockholm, oktober.

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

Gavriljuk, Anastasija. 2023. “Dannym zakryvajut granitsu”. *Kommersant*, 6 april. https://www.kommersant.ru/doc/5295048 (2023-11-17).

Giles, Keir. 2023. *Russian Cyber and Information Warfare in Practice: Lessons observed f rom the War on Ukraine*. Chatham House. Russia and Eurasia Programme Research Paper, December. https://www.chathamhouse.org/2023/12/russian-cyber-and-information-warfare-practice (2024-01-04).

Group-IB. 2023. *Kak atakovali rossijskij biznes v 2022*. https://www.facct.ru/resources/research-hub/ (2023-09-27).

Hegel, Tom & Milenkoski, Aleksandar. 2023. *Comrades in Arms? North Korea Compromises Sanctioned Russian Missile Engineering Company*. Sentinel Labs, 7 augusti. https://www.sentinelone.com/labs/comrades-in-arms-north-korea-compromises-sanctioned-russian-missile-engineering-company/ (2023-10-19).

ICANN. 2022. https://www.icann.org/en/system/files/correspondence/marby-to-fedorov-02mar22-en.pdf (2024-02-15).

IISS. 2021. *Cyber Capabilities and National Power: A Net Assessment*. IISS, juni. https://www.iiss.org/globalassets/media-library---content--

migration/files/research-papers/cyber-power-report/cyber-capabilities-and-national-power---a-net-assessment___.pdf (2024-01-31).

Informationssäkerhetsdoktrin, presidentdekret nr. 646, 5 december 2016. http://static.kremlin.ru/media/events/files/ru/tGeA1AqAfJ4uy9jAOF4CYCpuLQw1kxdR.pdf (2024-02-15).

Innostage. 2023. *7 tipov kiberatak, kotoryje byli populjarny v 2022 godu*, januari. https://innostage-group.ru/press/media/7-tipov-kiberatak-kotorye-byli-populyarny-v-2022-godu/ (2023-09-27).

Isakova, Tatiana. 2023a. ”Blits-chak”. *Kommersant*, 13 april. https://www.kommersant.ru/doc/5927911 (2023-04-25).

Isakova, Tatiana. 2023b. ”Chakery podbirajutsia k smezhnikam”. *Kommersant*, 29 augusti. https://www.kommersant.ru/doc/6185042 (2023-08-30).

Isakova, Tatiana. 2023c. ”Kiberintisdenty postavjat na platformu”. *Kommersant*, 1 september. https://www.kommersant.ru/doc/5537268 (2023-11-17).

Isakova, Tatiana. 2023d. ”Provajderov gotovjat k otkljutjenijam”. *Kommersant*, 15 september. https://www.kommersant.ru/doc/6212718 (2023-11-22).

Isakova, Tatiana. 2023e. ”S malych po nitkte”. *Kommersant*, 1 mars. https://www.kommersant.ru/doc/5843753 (2023-03-08).

Isakova, Tatiana & Kornev, Timofej. 2023. ”U kitajtsev pozaimstvujut stenu”. *Kommersant*, 6 april. https://www.kommersant.ru/doc/5915014 (2023-04-25).

ITU. 2021. *Global Cybersecurity Index 2020: Measuring commitment to cybersecurity*. ITU, Geneve. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf (2024-01-31).

Karlzén, Henrik. 2020a. *Cyberoperationer: En slutrapport*. FOI-R--5072--SE, december. https://foi.se/rest-api/report/FOI-R--5072--SE (2023-11-23).

Karlzén, Henrik. 2020b. ”Usefulness of Cyber Attribution Indicators”. 19th European Conference on Cyber Warfare and Security, digital Konferens 25–26 juni 2020, FOI-S--6243--SE.

Kaspersky ICS CERT. 2022. *Targeted attack on industrial enterprises and public institutions*, 8 August. https://ics-cert.kaspersky.com/publications/reports/2022/08/08/targeted-attack-on-industrial-enterprises-and-public-institutions/ (2023-10-27).

Kaspersky Lab. 2022. *Statistics 2022*. https://go.kaspersky.com/rs/802-IJN-240/images/KSB_statistics_2022_en_final.pdf (2023-09-27).

Kello, Lucas. 2018. *The Virtual weapon and international order*. New Haven: Yale University Press.

Kello, Lucas. 2022. *Striking Back: The End of Peace in Cyberspace – And How to Restore It*. New Haven: Yale University Press.

Killnet (@killnet_reservs), ”Nasji bratia i glavnyje sojuzniki iz Sudana, podderzjivajut nasju initsiativu, prisojedinjajas k nam i nasjej kompanii protiv Izraelskogo rezjima”, Telegram, 8 oktober 2023, https://t.me/killnet_reservs/7663 (2023-10-16).

Kolomytjenko, Marija. 2017. “Minkomsvjaz zanjalas perechvatom zvonkov i SMS radi ispytanij”. *RBK*, 25 december. https://www.rbc.ru/technology_and_media/25/12/2017/5a3ced9d9a79470b6a5750ad (2024-01-17).

Kommersant. 2021. ”Prisjlo vremja zadymatsia o bezopasnosti personalnych dannych”, 14 september. https://www.kommersant.ru/doc/5559435 (2023-11-17).

Kommersant. 2022. ”Roskomnadzor nazval uspesjnymi utjenija v ramkach zakona ob ustotjivosti runeta”, 19 oktober. https://www.kommersant.ru/doc/5040099 (2022-08-16).

Kornev, Timofej & Korolev, Nikita. 2022. ”’Avrove’ snjatsia dengi”. *Kommersant*, 17 november. https://www.kommersant.ru/doc/5669123 (2023-10-23).

Kornev, Timofej, Korolev, Nikita & Tisjina, Julija. 2022. ”Navstretju severnoj ’Avrove’”. *Kommersant*, 27 oktober. https://www.kommersant.ru/doc/5634227 (2022-11-25).

Korolev, Nikita & Litvinenko, Jurij. 2023. ”Derzji stanok sjire”, *Kommersant*, 12 oktober. https://www.kommersant.ru/doc/6267978 (2023-10-16).

Kretjetova, Angelina och Kinjakina, Jekaterina. 2019. ”Minkomsvjazi nazvalo datu testirovanija ’suverennogo interneta’ po vsej Rossii”. *Vedomosti*, 19 december. https://www.vedomosti.ru/technology/articles/2019/12/19/819154-datu-testirovaniya (2024-01-19)

Kukkola, Juha. 2020. *Digital Soviet Union: The Russian Segment of the Internet as a Closed National Network Shaped by Strategic Cultural Ideas*. Doktorsavhandling. National Defence University, Helsingfors, Series 1: Research Publications, nr. 40. https://www.doria.fi/bitstream/handle/10024/177157/Kukkola_Digital

%20Soviet%20Union_finalnet.pdf?sequence=3&isAllowed=y (2024-01-31).

Lindahl, David. 2020. *Omvärldsbevakning: Statsattribuerade cyberoperationer 2020*. FOI Memo 7422, 18 december. https://foi.se/rest-api/report/FOI%20Memo%207422 (2023-11-23).

Lowy Institute. 2023. Cyber Capabilities". *Asia Power Index: 2023 edition*. Inget datum, täcker åren 2021–2022. https://power.lowyinstitute.org/data/military-capability/signature-capabilities/cyber-capabilities/ (2024-06-18).

Madory, Doug (@DougMadory). 2023. Twitter, 7 juli, 09:58 fm. https://twitter.com/DougMadory/status/1677225659272409088 (2024-02-01).

Meduza. 2024. "Uzje ne raz v 2024 godu v Rossii blokirovali votsap i telegram – i dazje ves mobilnyj internet. Tjto budet dalsje?". *Tjto slutjilos* (podd), 30 januari. https://meduza.io/episodes/2024/01/30/uzhe-ne-raz-v-2024-godu-v-rossii-blokirovali-votsap-i-telegram-i-dazhe-ves-mobilnyy-internet-chto-budet-dalshe (2024-01-31).

Meilnel, Christoph & Hagebölling, David. 2023. *Russia's War Against Ukraine Is Catalyzing Internet Fragmentation*. CFR Net Politics & Digital and Cyberspace Policy Program, 13 mars. https://www.cfr.org/blog/russias-war-against-ukraine-catalyzing-internet-fragmentation (2023-11-24).

Ministeriet för digital utveckling. Order nr. 839, 12 december 2019. https://digital.gov.ru/ru/documents/7002/ (2024-01-19).

Morozova, Aleksandra. 2023. "Eksperty nazvali glavnyje vyzovy kiberbezopasnosti strany". *RBK Jekaterinenburg*, 14 juli. https://www.ekb.rbk.ru/ekb/14/07/2023/64b1478e9a79479172b7e5bc (2023-07-24).

Nilsson, Per-Erik. 2023. *Unravelling the Myth of Cyberwar: Five Hypotheses on Cyberwarfare in the Russo-Ukrainian War (2014–2023)*. FOI-R--5513--SE, december. https://foi.se/rapporter/rapportsammanfattning.html?reportNo=FOI-R--5513--SE (2023-12-18).

Plamenev, Ilja. 2023. "'Kasperskij' vyjavil kiberataku na sotrudnikov s ispolzovanijem iPhone". *RBK*, 1 juni. https://www.rbc.ru/politics/01/06/2023/6478abcf9a79477cf6293546 (2023-07-18).

Pljusjtjev, Aleksandr (https://www.youtube.com/@plushev). 2023. *Totjka*, 5 mars (164s in i programmet). https://www.youtube.com/watch?v=V-

092epW5oc&list=PLZVQqcKxEn_6YaOniJmxATjODSVUbbMkd&index=47&t=164s (2024-01-31).

Positive Technologies. 2023a. *Aktualnyje kiberugrozy dlja promysjlennych organizatsii (itogi 2022 goda)*. 28 februari. https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/industrial-cybersecurity-threatscape-2022_RUS.pdf (2023-03-03).

Positive Technologies. 2023b. *Aktualnyje kiberugrozy: itogi 2022 goda*. 29 March. https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Cybersecurity_threatscape_2022.pdf (2023-11-08).

Positive Technologies. 2023c. *Aktualnyje kiberugrozy: pervyj kvartal 2023 goda*. 16 juni. https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/%D0%90%D0%BA%D1%82%D1%83%D0%B0%D0%BB%D1%8C%D0%BD%D1%8B%D0%B5_%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D1%83%D0%B3%D1%80%D0%BE%D0%B7%D1%8B_Q1-2023_RUS.pdf (2023-11-08).

Positive Technologies. 2023d. *Ogo, kakaja IB! Aktualnyje kiberugrozy: itogi 2022 goda*. 29 mars. https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Ogo-kakaya-IB.pdf (2023-07-21).

Presidentdekret nr. 250, 1 maj 2022, http://publication.pravo.gov.ru/file/pdf?eoNumber=000120220501002 3 (2023-09-27).

Putin, Vladimir. 2022. ”O povysjenii ustojtjivosti i bezopasnosti funktsionirovanija informatitsionnoj ingrastruktury gosudarstva”, 20 maj. http://www.scrf.gov.ru/council/session/3241/ (2023-11-17).

RBK. 2023. ”Kiberutjenija v natsionalnom massjtabe: kak rabotajut kiberpoligony v Rossii”, 1 november. https://www.rbc.ru/technology_and_media/01/11/2022/635bfe3f9a794799a7e0b42e (2022-12-18).

Recorded Future’s Insikt Group. 2023. *Russia’s War Against Ukraine Disrupts the Cybercriminal Ecosystem*, 24 February. https://go.recordedfuture.com/hubfs/reports/cta-2023-0223.pdf (2023-11-01).

Regeringsbeslut, nr. DM-P8-5, 3 januari 2014. ”Prognoz nautjno-technologitjeskogo razvitija Rossijskoj Federatsii na period do 2030 goda”. https://in.minenergo.gov.ru/tek/strategiya-i-prognozy/prognoz-nauchno-tekhnologicheskogo-razvitiya-rossiyskoy-federatsii-na-period-do-2030-goda (3 mars 2021).

Regeringsföreskrift nr. 1934-p, 29 oktober 2022, http://publication.pravo.gov.ru/Document/View/0001202211020018 (2023-10-18).

Regeringsförordning nr. 2998-r, 22 oktober 2021, http://static.government.ru/media/files/d3uclO4ZFGNKmxCPBXbL4OaMPALluGdQ.pdf (2023-11-07).

Regeringsförordning nr. 4088-r, 22 december 2022, http://publication.pravo.gov.ru/file/pdf?eoNumber=000120221223003 5 (2023-09-27).

Regeringsinstruktion nr. 860, 13 maj 2022, http://publication.pravo.gov.ru/Document/View/0001202205160024 (2023-11-01).

Render-Katolik, Aiden. 2023. *The IT Army of Ukraine*. CSIS, 15 augusti. https://www.csis.org/blogs/strategic-technologies-blog/it-army-ukraine (2023-12-04).

RIA Novosti. “Sberbank zajavil o kadrovoj katastrofe v sfere informatsionnoj bezopasnosti”, 7 december 2021. https://ria.ru/20211207/kiberbezopasnost-172519232.html (2024-02-04).

Rodenhäuser, Tilman & Vignati, Mauro. 2023. ”8 Rules for “Civilian Hackers” During War, and 4 Obligations for States to Restrain Them”. *ICRC Blog, Humanitarian Law & Policy*, 4 oktober. https://blogs.icrc.org/law-and-policy/2023/10/04/8-rules-civilian-hackers-war-4-obligations-states-restrain-them/ (2023-10-12).

Roskomnadzor. Order nr. 216, 31 juli 2019. http://docs.cntd.ru/document/561008701 (2020-11-01).

Roskomsvoboda. 2023. ”S 2019 goda bylo provedeno 6 utjenij po ’suverennomu Runetu’”, Novosti, 24 oktober. https://roskomsvoboda.org/en/post/uchenia-runet-6-raz/ (2024-01-19).

Rostelekom Solar. 2023a. *Kiberataki na rossijskije kompanii v I kvartale 2023 godu”*. https://rt-solar.ru/analytics/reports/3445/ (2023-07-21).

Rostelekom Solar. 2023b. *Ottjet. ”Kiberataki na rossijskije kompanii v 2022 godu”*. https://rt-solar.ru/upload/iblock/4a4/ghus61x9rd8cv5vczms5ig1svts4tlep/Otchet-o-kiberatakakh-na-rossiyskie-kompanii-v-2022-godu.pdf (2023-03-08).

Rostelekom Solar. 2023c. *Ottjet ob atakach na onlajn-resursy rossijskich kompanii. Za 2022 god*. https://rt-solar.ru/upload/iblock/34a/5w4h9o57axovdbv3ng7givrz271ykir3/Atak

i-na-onlayn_resursy-rossiyskikh-kompaniy-v-2022-godu.pdf (2023-03-08).

Rozjkov, Roman & Gavriljuk, Anastasija. 2023. “Group-IB rasskazala o napadenii kitajskich chakerov na rossijskij IT-sektor”. *Forbes*, 13 februari. https://www.forbes.ru/technologii/484840-group-ib-rasskazala-o-napadenii-kitajskih-hakerov-na-rossijskij-it-sektor (2023-03-02).

Rustamovoj, Farida & Tovkajlo, Maksim (@faridaily24), ”Posle predosterezjenija FSB tjlenam pravitelstva zapretili pronosit ajfony na zasedanija kabineta ministrov”, Telegram, 7 juni 2022, https://t.me.faridaily24/946 (2023-07-17).

Sherman, Justin. 2023. “Russia’s Largest Hacking Conference Reflects Isolated Cyber Ecosystem”, *Brookings Commentary*, 12 January. Accessed (20 July 2023) at https://www.brookings.edu/articles/russias-largest-hacking-conference-reflects-isolated-cyber-ecosystem/.

Skrynnikova, Anastasija. 2019. “Minkomsvjaz podvela itogi utjenij po ’suverennomu Runetu’”. *RBK*, 23 december 2019. https://www.rbc.ru/technology_and_media/23/12/2019/5e00beb39a79476b254af87c (2024-01-17).

Soesanto, Stefan. 2022. *The IT Army of Ukraine: Structure, Tasking, and Eco-System*. Cyberdefense Report, Center for Security Studies, ETH Zürich, juni. https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/552293/Cyber-Reports-2022-06-IT-Army-of-Ukraine.pdf (2024-07-18).

Soldatov, Andrei & Borogan, Irina. 2023. *Russia’s Cybersecurity Companies Shrug off Sanctions*. CEPA, 18 mars. https://cepa.org/article/russias-cybersecurity-companies-shrug-off-sanctions/ (2023-03-18).

”Strategi för att utveckling av ett informationssamhälle i Ryska federationen 2017–2030”, antagen per presidentdekret nr. 203, 9 maj 2017. http://static.kremlin.ru/media/acts/files/0001201705100002.pdf (2024-01-16).

Tass. 2022. ”Tsentr kompetentsii po informbezopasnosti natjnet rabotu v 2023 godu”, 8 december. https://tass.ru/ekonomika/16543737 (2023-09-27).

Tass. 2023. ”Chinsjtejn zajavil, tjto dejstjujusjtjich v interesach RF chakerov nado osvobodit ot otvetstvennosti”, 10 februari. (2023-09-25).

Tidy, Joe. 2023. “Ukraine Cyber-Conflict: Hacking Gangs Vow to De-Escalate”. *BBC News*, 6 oktober.

https://finance.yahoo.com/news/ukraine-cyber-conflict-hacktivist-gangs-112009075.html (2023-10-12).

Tjebakova, Darja & Balasjova, Anna. 2021. ”V Rossii protestirovali rabotu Runeta pri atkljutjenii ot globalnoj seti”. *RBK*, 21 juli. https://www.rbc.ru/technology_and_media/21/07/2021/60f8134c9a79476f5de1d739 (2024-01-31).

Ukrainas Ministerium för digital transformation. 2022. ”Ministry of Digital Transformation: IT army blocks Russian sites in a few minutes – the main victories of Ukraine on the cyber front”, 28 februari. https://www.kmu.gov.ua/en/news/mincifri-it-armiya-blokuye-rosijski-sajti-za-dekilka-hvilin-golovni-peremogi-ukrayini-na-kiberfronti (2023-10-02).

Ustinova, Anna. 2023. ”Do 30% personalnych dannych utekajet po vine sotrudnikov”, *Vedomosti*, 16 oktober. https://www.vedomosti.ru/technology/articles/2023/10/16/1000720-do-30-personalnih-dannih-utekaet-po-vine-sotrudnikov (2024-07-18).

Vendil Pallin, Carolina. 2020. *Nyckelaktörerna för rysk cybersstrategi: 2000–2020*. FOI-R--5025--SE, oktober. https://www.foi.se/rest-api/report/FOI-R--5025--SE (2023-11-17).

Vendil Pallin, Carolina. 2022. *Rysslands inte så suveräna internet och kriget i Ukraina*. FOI Memo 7925, 12 december. https://foi.se/rapportsammanfattning?reportNo=FOI%20Memo%207925 (2023-11-17).

Willet, Marcus. 2022. “The Cyber Dimension of the Russia-Ukraine War”. *Survival* 54.5: 7–26.

Winther, Pontus & Nilsson, Per-Erik. 2023. *Smart Tactics or Risky Behaviour? The Lawfulness of Encouraging Civilians to Participate in Targeting in an Age of Digital Warfare*. The Hague Centre for Strategic Studies, Paper 2, Paper series: Information-based behavioural influencing and Western practice, maj. https://hcss.nl/wp-content/uploads/2023/05/02-Smart-Tactics-or-Risky-Behaviour.pdf (2024-02-07).

Voo, Julia, Hemani, Irfan & Cassidy, Daniel. 2022. *National Cyber Power Index 2022*. Belfer Center for Science and International Affairs, September. https://www.belfercenter.org/sites/default/files/files/publication/CyberProject_National%20Cyber%20Power%20Index%202022_v3_220922.pdf (2024-06-04).

Ordlista

Ord	Förklaring
APT	*Advanced persistent threat* – från början benämningen på ett it-angrepp som krävde hög kompetens, målinriktat mot ett visst offer och där angriparen hade långvarigt tillträde till offrets nätverk. Numera används begreppet också för de grupper som genomför APT-angrepp och verkar ha förmågor resurser och ihärdighet som förknippas med ett landsförmåga snarare än kriminella grupper eller hacktivister.
BGP	*Border gateway protocol*, ett internetprotokoll för att hitta bästa vägen för att sända trafik till en viss mottagare genom de olika internetleverantörer som gemensamt utgör internet.
CERT	*Computer emergency response team*, numera en ”pseudoförkortning”, a) den grupp av personal inom en organisation som tillsammans ska agera vid en it-kris inom organisationen b) En organisation som ska assistera andra organisationer med information och resurser för att förbereda sig inför en it-kris och som även ger direkt assistans när sådana inträffar. Dessa kan vara privata företag eller myndigheter.
DNS	*Domain name system*, domännamnssystem, en global distribuerad databas som översätter en människoläslig adress som FOI.se till en IP-adress som t ex en webbläsare kan använda för att sända trafik till rätt dator. Toppdomänerna som .se, .net eller .ru är geografiska toppdomäner som håller reda på adresser till organisationer inom områdena. Domänerna .com eller .edu hanterar adresser för vissa typer av organisationer.
DNS over HTTPS	En kryptering av webbläsarens anrop till DNS; innebär att det blir svårt att ”avlyssna” trafiken mellan webbläsaren och servern, och även svårt att ändra meddelandet på vägen. Protokollet kan också kontrollera om DNS-svaret kommer från rätt server så att det blir svårare att lura någon till en falsk webbplats.
DNS over TLS	Nätverksprotokoll för säker kryptering vid anrop till DNS; sker via TLS-protokoll (*transport layer security* – transportskiktet på internet). Fungerar i praktiken likadant som HTTPS utom att trafiken är mer lättdetekterad.
FSB	Federala säkerhetstjänsten (Federalnaja sluzjba bezopasnosti).

FSO	Federala skyddstjänsten (Federalnaja sluzjba ochrany); Rysk myndighet som ansvarar för federala organs säkra kommunikationer.
FSTEK	Federala tjänsten för teknisk och exportkontroll (Federalnaja sluzjba po technitjeskomu i eksportnomu kontrolju).
ICANN	Internet Corporation for Assigned Names and Numbers – internationell icke vinstdrivande organisation som ansvarar för internets adressystem (DNS, ip-adresser, protokoll).
IP-adress	Internetprotokolladress – ett unikt nummer som identifierar en dator som ansluter till internet.
Gateway	Formellt en nätsluss – en dator eller ett program som kopplar ihop nätverk med olika protokoll. Används idag för att beskriva olika anslutningar mer generellt mellan nätverk.
GosSOPKA	Statliga systemet för att upptäcka, förhindra och likvidera följderna av dataattacker (Gosudarstvennaja Sistema obnaruzjenija, predotvrasjtjenija i likvidatsii posledstvij kompjuternych atak) – Rysslands formellt etablerade process för cyberförsvar för åtminstone myndigheter och statliga företag samt för regional federala organ.
Hackergrupp	Används i denna rapport för att beskriva en grupp som begår dataintrång i syfte att spionera, stjäla eller förstöra data (kriminella hackergrupper hotar att förstöra data för att utöva utpressning). En hackergrupp kan även ha som mål att förstöra det it-system den angriper (sabotage). (En hackare kan dock även vara en skicklig programmerare, t.ex. någon som arbetar för att förstärka säkerheten i ett it-system genom att hitta sårbarheter i syfte att eliminera dessa.)
Hacktivist	Någon som genomför it-attacker av politiska eller sociala skäl (en sammanslagning av orden hacker och aktivist, på engelska *hacktivist*, på ryska *chaktivist*).
IKT	Informations- och kommunikationsteknik
Internet of things	Sakernas internet - anslutning av apparater och maskiner som inte är datorer, som t.ex. bilar, kylskåp, mätutrustning, till internet.
ITU	International Telecommunication Union – FN-organ för informations- och kommunikationsteknologier med säte i Geneve.
Kill switch	*Internet kill switch* – en funktion för att centraliserat kunna stänga av kontakten med internet för att skydda användare inom t.ex. en viss geografisk region, ett land eller vissa

	plattformar. Ursprungligen tänkt för att skydda användare från ett angrepp eller annan fara, men flera auktoritära länder har använt denna funktion för att stänga ner internettrafiken och därmed dämpa protester och demonstrationer.
OSS	Oberoende staters samvälde – i februari 2022 ingick Armenien, Azerbajdzjan, Belarus, Kazakstan, Kirgizistan, Moldavien, Ryssland, Tadzjikistan, Uzbekistan (Turkmenistan deltar men är inte formellt full medlem).
Rosgvardija	Federala tjänsten för Ryska federationens nationalgardestrupper (Federalnaja sluzjba vojsk natsionalnoj gvardii).
Roskomnadzor	Rysk myndighet med ansvar för tillsyn av kommunikation, inklusive internet; lyder under Ministeriet för digital utveckling. Formellt namn: Federala tjänsten för tillsyn inom samband, informationsteknologi och masskommunikation (Federalnaja sluzjba po nadzoru v sfere svjazi, informatsionnych teknologij i massovych kommunikatsij).
Roskomsvoboda	Rysk organisation som bevakar inskränkningarna av friheten på ryska internet sedan 2012.
Rossvjaz	Ryska myndigheten för samband. Formellt namn: Federala sambandsagenturen (Federalnoje agenstvo svjazi). Lyder under Ministeriet för digital utveckling.
RSNet	Ett intranät för landets ledning och centrala myndigheter, ett slags ”regeringsintranät” med en *gateway* mot internet.
zero-day-exploits	Dagnollattack, ett dataintrång som utnyttjar en sårbarhet som inte varit känd innan angreppet och därmed saknar färdiga lösningar från säkerhetsföretagen. (Försvararen har noll dagar att uppdatera sina program.) Angrepp av denna typ är ovanliga. Den angripare som utför dem måste ha gjort mycket forskning för att hitta dem, eller betalat mycket pengar för att få tillgång till dem.

ISSN 1650-1942

www.foi.se