Samhällets motståndskraft mot cyberhot och cyberangrepp

Lärdomar från Estland

ELINA ELVEBORG LINDSKOG OCH
ANNA LIOUFAS

FOI-R--5625--SE
ISSN 1650-1942 December 2024

FOI

Samhällets motståndskraft mot cyberhot och cyberangrepp

Lärdomar från Estland

Elina Elveborg Lindskog och Anna Lioufas

Titel	Samhällets motståndskraft mot cyberhot och cyberangrepp – Lärdomar från Estland
Rapportnummer	FOI-R--5625--SE
Månad	December
År	2024
Antal sidor	78
ISSN	1650-1942
Kund	Försvarsdepartementet
Forskningsområde	Försvarspolitiska Studier
Projektnummer	A12409
Godkänd av	Malek Finn Khan
Ansvarig avdelning	Försvarsanalys

Omslagsbild: City cyber security, Nick Lowndes, TT Nyhetsbyrå.

Sammanfattning

Denna rapport syftar till att identifiera vad som utgör samhällelig motståndskraft gentemot cyberangrepp. I rapporten ges inledningsvis en beskrivning av begreppen försvar och säkerhet inom cyberområdet. Därefter redovisas en fallstudie som syftar till att ge närmare beskrivning av hur Estland arbetar inom cyberområdet för att upprätthålla ett motståndskraftigt samhälle. Avslutningsvis diskuteras hur cyberhotens karaktär och möjligheter till förvarning kan påverka utformningen av cyberförsvaret. Studien utgår från Sternudds cyberförsvarspyramid samt *whole-of-nation*-strategin.

I studien framkommer det att Estland, som är ett land med hög digitaliseringsgrad, har dragit lärdomar från de cyberattacker som landet utsattes för 2007. Estland har sedan dess arbetat för att bygga upp ett robust cyberförsvar med förmåga att hantera upprepade cyberattacker från resursstarka antagonister.

Vissa lärdomar från Estland kan utgöra inspiration för svenska förhållanden, såsom deras nätverk för informationsdelning, organisation av cyberhemvärn, hur de har inkluderat cyberfrågor i deras nationella utbildningskultur samt den estniska informationssäkerhetsmyndigheten RIA:s roll inom cyberförsvaret.

Nyckelord: Cyberhot, cyberangrepp, cyberförsvar, förvarning, indiactions and warning (I&W), informationssäkerhet, motståndskraft, whole-of-nation, Estland.

Summary

This report aims to identify what constitutes societal resilience against cyber attacks. It initially provides a description of the concepts of defense and security within the cyber domain. A case study is then presented, in order to provide a closer look at how Estonia works in the cyber field to maintain a resilient society. The report is then concluded in a discussion on how the nature of cyber threats and the possibilities for early warning can influence the design of cyber defense strategies.

The study is based on Sternudd's cyber defense pyramid and the whole-of-nation strategy. It contends that Estonia, a country with a high level of digitalization, has learned lessons from the cyber attacks it faced in 2007. Since then, Estonia has worked to build a robust cyber defense capable of handling repeated cyber attacks from resourceful adversaries.

Some lessons from Estonia may serve as inspiration for Sweden, such as their information-sharing network, the organization of cyber home guard units, how they have incorporated cyber issues into their national education culture, and the role of the Estonian Information Security Authority (RIA) within cyber defense.

Keywords: Cyber threat, cyber attacks, cyber defence, resilience, information security, indications and warning (I&W), whole-of-nation, Estonia.

Innehållsförteckning

Figurer

Förord

Projektet Försvarspolitiska studier bedrivs av FOI på uppdrag av regeringen (Försvarsdepartementet). Det ska över tid ge stöd med analys och underlag i frågor som rör inriktning, implementering och uppföljning av regeringens beslut om utformning av försvaret i Sverige. Studierna omfattar framförallt militärt försvar men även andra områden av betydelse för totalförsvaret i stort.

Samhällelig motståndskraft mot cyberhot och cyberangrepp är en avgörande förutsättning för att försvaret ska fungera under såväl fred som kris och krig. Utvecklingen av it-relaterade hot går nu snabbare än tidigare, bland annat på grund av ökade internationella motsättningar både globalt och i Sveriges närområde. Möjligheterna att störa, sabotera, spionera och vilseleda genom åtgärder i cyberdomänen har ökat för alla aktörer och det faktum att mycket kan ske dolt innebär höga krav på cybersäkerhet och cyberförsvar i alla konfliktnivåer.

Syftet med föreliggande studie är att höja kunskapsnivån avseende cybersäkerhet och cyberförsvar i allmänhet samt även visa hur motståndskraft kan skapas inom ett samhälle. Estland är ett bra exempel på ett land som har varit tidig med detta.

Vi tackar alla de personer som har bidragit till vårt arbete genom att generöst dela med sig av sin kunskap. Vi vill särskilt tacka för det stöd som givits av den svenska ambassadören i Tallin, Ingrid Tersman, och personalen vid ambassaden, som så vänligt hjälpte oss få kontakt med relevanta aktörer. Vidare vill vi tacka alla de medarbetare som deltog i granskningsseminariet av denna rapport, här vill vi särskilt framhålla Lisa Bergsten, Malin Granath och Per-Erik Nilsson för deras föredömliga granskning av rapporten, vilken ledde till många förbättringar av både struktur och innehåll. Karin Blext, Patric Karlsson och Kristina Gavhed ska också nämnas för sitt fina stöd vad gäller layout och figurer.

Stockholm, december 2024

Krister Pallin

Projektledare för Försvarspolitiska studier

1. Inledning

I en intervju med svenska medier sommaren 2024 underströk den estniska statsministern Kaja Kallas vikten av att ta tillvara på estniska erfarenheter i samband med det svenska Nato-inträdet.

> ”Lyssna på oss. I dag pågår det konventionella kriget i Ukraina, men också ett ´skuggkrig´ som pågår i cyberrymden, i rymden, i informationsrymden.” (Küchler 2024)

Kallas uttalande illustrerar väl vikten av vaksamhet i både Sveriges geografiska närområde och i den digitala världen, där geografisk närhet inte har samma betydelse. Med de senaste årens omvärldsutveckling och det resulterande försämrade säkerhetspolitiska läget i åtanke bedömer flera underrättelseaktörer hotbilden från främmande makt som hög (FRA 2024; Must 2024; Säpo 2024). Kvalificerade statliga och statsunderstödda cyberangrepp utgör en del av hotbilden mot Sverige, och har enligt underrättelseaktörer ökat i både omfattning och förmåga (Ds 2023:34). Teknikutvecklingen och digitaliseringen av samhället utvecklas, vilket innebär nya metoder för cyberangrepp med informationspåverkan, spionage, terrorism och sabotage som motiv (Jonsson et al, 2023). Flera rapporter som publicerats det senaste året beskriver en ökning av cyberangrepp mot europeiska intressen sedan Rysslands fullskaliga invasion av Ukraina (bland annat Europol 2023a). I en artikel från Dagens Nyheter publicerad i samband med den franske presidentens Emmanuel Macrons besök i Sverige beskrivs hur angreppen från proryska grupper har ökat kraftigt både i Frankrike och i Sverige. Macron konstarerade att:

> ”Vi drabbas nu av krigets följder i vår vardag. Vi utsätts redan för attacker. Flera sjukhus har paralyserats i dagar på grund av den här ryska aggressiviteten. /…/ Situationen har förvärrats de senaste månaderna. Regimen i Kreml har mångdubblat sina desinformations- och cyberattacker mot oss i Frankrike, liksom i övriga Europa.” (de la Reguera 2024)

Det försämrade säkerhetspolitiska läget innebär således ett ökat behov av motståndskraft mot cyberangrepp (MSB 2024a). Utgångspunkten för denna rapport är att undersöka vad som utgör motståndskraft mot cyberhot och cyberangrepp i ett modernt och högt digitaliserat samhälle. Vi har tagit avstamp i en fallstudie, där vi valt att titta närmre på Estland. I likhet med Sverige, är Estland ett litet land med en tidig och omfattande digitalisering av samhället. Landet har kommit långt när

det kommer till införandet av digital teknik, men även i arbetet med digital säkerhet, och framställs ofta som ett föregångsland inom området.

1.1 Syfte och frågeställning

Rapporten skrivs på uppdrag av Försvarsdepartementet. Ambitionen är att ge en övergripande beskrivning av försvar och säkerhet inom cyberområdet, med Estland som fallstudie. Syftet är att sprida kunskap om cyberhot och cyberförsvar inom det svenska totalförsvaret. Rapporten utgår från följande frågeställningar:

- Vad utgör samhällelig motståndskraft mot cyberhot och cyberangrepp i Estland?
- Vilka lärdomar från Estlands arbete inom cyberområdet kan utgöra inspiration för Sverige?

1.2 Data och metod

Rapporten baseras på öppen litteratur samt en mindre intervjustudie med estniska experter på cyberförsvarsområdet. I rapporten används därmed både primärkällor, i form av intervjuer, och sekundärkällor, i form av akademisk och policyorienterad litteratur.

1.2.1 Insamling av empiri

En intervjuresa till Estland genomfördes i samband med projektet. Sammanlagt gjordes fem intervjuer, varav två var gruppintervjuer med tre deltagare i varje grupp. Totalt deltog nio respondenter. Samtliga intervjuer utom en (som gjordes via videolänk) skedde på plats i Tallinn. Respondenterna intervjuades dels utifrån den roll de nu har vid sin arbetsplats, dels som experter inom området utifrån att de har haft flera olika roller och erfarenheter inom cyberområdet. Organisationer som är representerade är[1]:

- Estlands Information System Authority (RIA)
- Cyber Defence Unit, e-Governance Academy (eGA)

1 Organisationerna beskrivs i korthet i bilaga 1.

- NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)
- Center for digital forensic and cyber security, CDFCS (Taltech)
- Respondenter med relevant erfarenhet från den politiska sfären.

Intervjuguiden utarbetades med frågor som anpassades efter respondenternas yrkesroll och expertområde. Intervjuerna var semistrukturerade med övergripande frågeområden utifrån studiens syfte och frågeställningar, vilket även gav utrymme för följdfrågor. Det gavs vidare möjlighet att stämma av att den information som respondenterna lämnade blev rätt uppfattad av oss som höll i intervjun. Båda författarna har en gedigen erfarenhet av att genomföra och analysera intervjuer.

Samtliga respondenter fick ta del av ett informationsbrev om studiens syfte i samband med inbjudan. Samtycke att medverka inhämtades muntligen vid intervjutillfället. Alla respondenter tillfrågades om tillåtelse att referera till deras arbetsplats. Enskilda respondenter har hållits anonyma.

Alla intervjuer utom en genomfördes av båda författarna, som även gemensamt bearbetade materialet i direkt anslutning till intervjutillfället. Intervjuerna spelades inte in utan anteckningar fördes istället. Intervjuerna pågick i snitt mellan en och två timmar.

Utdrag från intervjuerna översattes från engelska till svenska av författarna och har vid några fåtal tillfällen förenklats något för att öka läsbarheten.

1.2.2 Analys av empiri

Intervjumaterialet kodades med koder[2] som sedan tematiserades – grupperades under olika rubriker – för att slutligen sammanställas i fyra huvudteman:

- Militär-civil samverkan
- Utbildning och informationsinsatser
- Informationsdelning och nätverk
- Transparens och öppenhet.

Det teoretiska ramverket för studien är baserat på Sternudds (2023) cyberförsvarsmodell och Klimburgs (2011) beskrivning av *whole-of-nation*-ansatsen, se

2 Exempelvis nätverk, samarbeten, informationsflöden, sekretess, mindset.

vidare kapitel 2. Pyramidformer kan användas för att ge en sammanhängande förklaringsmodell mellan dels olika kärnuppdrag och dels mellan olika funktioner. I denna rapport används cyberförsvarspyramiden som ett verktyg för att analysera förhållandet mellan säkerhet och försvar och vidare på vilket sätt som *whole-of-nation*-ansatsen i Estland förhåller sig till upprätthållandet av ett motståndskraftigt samhälle mot cyberhot och cyberangrepp. Dessa modeller används sedan för att strukturera dels den insamlade litteraturen och dels intervjumaterialet för att kunna besvara rapportens två frågeställningar om vad som utgör samhällelig motståndskraft mot cyberhot och cyberangrepp och vilka lärdomar som går att hämta från den estniska kontexten.

1.2.3 Begränsningar

En risk i denna kvalitativa studie är att respondenterna — oavsiktligt eller ej — lyfter fram en onyanserad bild av Estland som lednade inom cyberområdet. För att hantera detta har det varit viktigt att göra en så bred inhämtning som möjligt för att ge utrymme för andra tolkningar och observationer. Författarna har bland annat intervjuat personer med olika relation (yrkesroller och arbetsplatser) till studiens syfte och frågeställningar och inkluderar även en övergripande redogörelse av hur Estland står sig i jämförelse med andra länder inom cyberområdet. Det har även varit viktigt att författarna under arbetsts gång varit uppmärksamma på hur den insamlade information kan tolkas.

En ytterligare begräsning var att vi inte fick svar från alla de personer som vi kontaktade med förfrågan om intervju. Aktörer som var svåra att komma i kontakt med inkluderar Estlands nationella beredskapsenheter för cyberförsvar (CERT-EE, Computer Emergency Response Team Estonia) och Estlands militära CERT.[3] Detta innebar att frågor om incidentrapportering och informationsflöden mellan civila och militära aktörer har begränsats, vilket även inkluderar möjligheten att få svar på frågor om förvarning inom cyberområdet. Samverkan mellan det civila och militära försvaret angränsar till underrättelsetjänstens arbete, där det är genomgående prioriterat att hemlighålla källor och metoder. Detta är viktigt att ha i åtanke när det kommer till steget att tolka resultatet. Denna studie baseras endast på öppna källor och är inte heller sekretessbelagd.

3 CERT (Computer Emergency Response Team) ansvarar för att ta emot, granska och svara på rapporter om datasäkerhetsincidenter och aktiviteter som rapporteras in av användare, företag, myndigheter eller organisationer. Enheten består vanligtvis av säkerhetsanalytiker som är organiserade för att utveckla, rekommendera och samordna omedelbara begränsningsåtgärder och återställning till följd av datasäkerhetsincidenter. Det kallas också för ett Computer Incident Response Team (CIRT) eller ett CIRC (Computer Incident Response Center, Computer Incident Response Capability).

1.3 Disposition

I kapitel 2 ges en beskrivning av begreppen hot, angrepp, försvar och säkerhet inom cyberområdet. I kapitel 3 presenteras en beskrivning av Estland som cybersäkerhetsaktör utifrån styrdokument och av landets cybersäkerhetsstruktur. Kapitlet inkluderar även en översikt av de större aktörerna och samverkansfora, samt en historisk tillbakablick på händelser inom cyberdomänen som format Estlands cybersäkerhetspolitik. I kapitel 4 introduceras analysen av det insamlade materialet baserat på de frågeställningar som ligger till grund för studien, med stöd av Sternudds modell för cyberförsvar och *whole-of-nation*-strategin. Detta följs av en diskussion om och hur lärdomar från Estland kan ge inspiration till utformningen av det svenska cyberförsvaret. I kapitel 5 ges sammanfattande reflektion. Resultaten av intervjuerna lyft i bilaga 2.

2. Försvar och säkerhet inom cyberområdet

I DETTA KAPITEL FÖRKLARAS begreppen cyberhot och cyberangrepp samt cybersäkerhet och cyberförsvar. Sternudds cyberförsvarspyramid används som modell för att illustrera hur frågor kring cyberförsvar och cybersäkerhet kan förhålla sig till varandra och genomsyra hela samhället. *Whole-of-nation*-modellen används sedan för att visa hur Sternudds teori kan förstås från ett mer praktiskt perspektiv.

2.1 Hot och angrepp

Redan i en utredning från 1953 lyfts behovet av information för att skapa ett motståndskraftigt samhälle: ”må det framhållas att man i regel är betydligt mer motståndskraftig om man känner till vad det är man kan råka ut för” (SOU 1953:27 s. 62). Behovet av information och kunskap betonas ofta som en central del av ett motståndskraftigt samhälle, och ovanstående citat understryker att detta behov inte är något nytt. För att kunna skapa ett robust cyberförsvar krävs alltså en förståelse av vad som ska försvaras och mot vilken typ av hot.

2.2 Cyberhot

Vad som utgör en hotbild förändras till följd av både den tekniska utvecklingen och samhällsutvecklingen i stort (Agrell 2011). Cyberhot och cyberangrepp används ofta som parord i formuleringar för att beskriva behovet av åtgärder inom cyberdomänen. En skillnad är dock att den först nämnda betonar potentialen att kunna utnyttja sårbarheter hos ett system, medan den sist nämnda betonar själva aktiviteten, en avsiktlig obehörig åtgärd på ett datasystem (National Institute of Standards and Technology).[4]

4 National Institute of Standards and Technology definition av cyberhot: “any circumstance or event with the *potential* to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service” och av cyberangrepp “any kind of malicious *activity* that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself”. Se NIST hemsida: *https://csrc.nist.gov/glossary/term/Cyber_Threat*

2.3 Cyberangrepp

Det finns många olika sätt att begå cyberangrepp.[5] De flesta av dessa angrepp initieras genom att gärningsaktörer olovligen tar sig in i ett datasystem genom dataintrång[6]. En hotaktör kartlägger först vilka sårbarheter som kan nyttjas i ett system. Detta innebär att det finns en viktig tidsaspekt att ha i åtanke i processen; från kartläggning till den initiala åtkomsten av ett system – för att exempelvis verkställa skadlig kod i systemet – för att vid ett givet tillfälle kunna påverka eller för att nå viss information i systemet (Försvaret Radioanstalt m.fl. 2020). Beroende på motiv och tillvägagångssätt för cyberangreppet kan det vara svårt att identifiera att en attack har skett samt att fastställa när själva intrånget ägde rum. Det är även svårt att attribuera angreppet till en specifik aktör (Lindskog m.fl. 2022).

2.4 Exemplifiering av cyberangrepp

För att ge en illustration av bredden av cyberhot utgår denna rapport från Zegarts (2022) typologi där antagonistiska cyberhot sorteras in i fem kategorier; störning, sabotage, spionage, stöld och vilseledning. Motivet bakom angreppet kan även vara en kombination av dessa. Nedan följer en övergripande exemplifiering av dessa cyberhot:

Störning: att störa eller slå ut tillgången till nätverk, ett datasystem, webbplats eller liknade genom en överbelastningsattack, på engelska Distributed denial of service, (DDoS), är en vanligt förekommande typ av cyberangrepp. Enligt Europol har överbelastningsattacker ökat markant i väst sedan Rysslands anfallskrig mot Ukraina (Europol 2023a). I samband med det svenska Nato-inträdet utsattes ett stort antal svenska myndigheter – bland annat Kronofogden, Skatteverket och Försäkringskassan – av just sådana överbelastningsattacker. En samling proryska grupper tog på sig de misstänkta cyberattackerna (Balcer Bednarska 2024).

Sabotage: möjliggörs genom kartläggning av svenska nätverk. För att skapa förutsättningar för att vid behov kunna genomföra sabotage, vid tillfälle som kan ligga längre fram i tiden, genomför Ryssland aktiviteter som ”underrättelseinhämtning,

5 Se Säpos beskrivning av hur främmande makt bedriver cyberangrepp utifrån fem olika faser: 1. Kartläggning, 2. Försök, 3. Access, 4. Exfiltrering och 5. Sabotage. Säkerhetspolisens hemsida: *Cyberangrepp från främmande makt - Säkerhetspolisen (sakerhetspolisen.se)*

6 I brottsbalken 4 kap. 9c§ beskrivs dataintrångsbestämmelsen enligt följande: “Den som olovligen bereder sig tillgång till en uppgift som är avsedd för automatiserad behandling eller olovligen ändrar, utplånar, blockerar eller i register för in en sådan uppgift som döms för dataintrång till böter eller fängelse i högst två år. Detsamma gäller den som olovligen genom någon annan liknande åtgärd allvarligt stör eller hindrar användningen av en sådan uppgift. Är brottet grovt, döms för grovt dataintrång till fängelse i lägst sex månader och högst sex år”.

etablering av stödjepunkter och rekrytering av potentiella ombud" (MUST 2024: 48). Gisslanattack, på engelska ransomware[7], är ett exempel på skadlig programvara som gör det möjligt för en angripare att kryptera och därmed begränsa åtkomsten till en individs eller ett företags viktiga information. Ofta kräver angriparen betalning för att häva begränsningen (Brewer 2016). Ett exempel på gisslanattack inträffade i januari 2024, då hackergruppen Akira genomförde en cyberattack mot it-leverantören Tietoevry. Attacken innebar att över 120 svenska myndigheter drabbades och en stor mängd information förstördes (Balcer Bednarska 2024). Ett kanske tydligare exempel på just sabotage är NotPetya-attacken 2017, där gärningspersonerna visserligen begärt en lösensumma, men där det senare visade sig omöjligt att betala lösensumman då länken till utbetalningen inte fungerade. Det är därför rimligt att dra slutsatsen att syftet var sabotage: att helt enkelt förstöra information.

Spionage och stöld av känslig information: cyberspionage kan beskrivas som en metod för att få otillbörlig tillgång till konfidentiell information, vanligtvis stats- eller affärshemligheter (Enisa 2020a). Cyberspionage som sponsras av stater uppges vara ett växande hot mot industrisektorer, men även mot kritisk och strategisk infrastruktur som exempelvis järnvägar, telekommunikationsleverantörer, banker och sjukhus (ibid). Enligt flera underrättelseaktörer pågår det ständigt ett systematiskt och långsiktigt arbete med inhämtning av information om Sverige från främmande underrättelse- och säkerhetstjänster (FRA 2024; MUST 2024). Att Ryssland varit den dominerande utföraren av spionage i Europa framkommer i Jonsson och Gustafssons (2022) rapport om spionage som utförts av européer mellan 2010 och 2021 (studien inkluderar dock inte cyberspionage). Att främmande makt använder cyberspionage lyfts dock i Säkerhetspolisen årsredovisning:

> "cyberspionage sker både i syfte att stjäla information och för att förbereda sabotage, och kan pågå under lång tid utan att den verksamhet som utsätts för det upptäcker intrånget." (Säkerhetspolisen 2023:26).

Vilseledning: enligt en vedertagen definition innebär vilseledning "information, förmedlad via ett uttalande, en handling eller ett objekt, med syftet att manipulera målgruppers beteenden genom att få dem att acceptera en falsk eller förvrängd uppfattning av verkligheten" (Whaley 2007:6). Redan 2018 uppmärksammade EU-kommissionen utmaningar med påverkansoperationer i sin första "Action Plan Against Disinformation", där just rysk desinformation pekades ut som det största hotet mot EU. Påverkansoperationer beskrivs ofta som just cyberhot, men Sternudd

7 Ransomware definieras av Enisa (2022) som "a type of attack where threat actors take control of a target's assets and demand a ransom in exchange for the return of the asset's availability and confidentiality". Ransomware kallas på svenska för "utpressningstrojan" eller "gisslanprogram". Det är en typ av skadlig programvara som krypterar en användares filer eller låser deras system och kräver en lösensumma för att återställa åtkomsten.

(2023) menar att det egentligen inte blir en cybersäkerhetsfråga förrän angriparen gör ett intrång i ett informationssystem för att exempelvis sprida ett budskap. Ett exempel på detta är dataintrånget mot demokraternas mejlservrar under den amerikanska presidentvalskampanjen 2016, där e-postmeddelanden stals av hackare och läcktes. Läckan orsakade betydande skada för Clinton-kampanjen och väckte frågor om i vilken utsträckning hackare med band till den ryska underrättelsetjänsten påverkat det amerikanska presidentvalet (Inkster 2016).

2.4.1 Aktörer

Karlzén (2019: 56) framhåller att en stor del av angreppens tillvägagångssätt har en relativt låg sofistikationsgrad, med vilket han menar att de flesta gärningsaktörer använder sig av ”relativt enkla osofistikerade tillvägagångssätt”:

> ”Det finns gott om standardmässiga angreppsverktyg, användare är ganska lättlurade, sårbarheter finns och förblir länge, och de flesta har inte vetskap om vad som sker i deras system eller i omvärlden.”

Med standardmässiga angreppsverktyg menas bland annat att det går att köpa tjänster för angrepp, ”*crime-as-a-service*”, (CaaS)[8] för att exempelvis begå överbelastningsattacker, vilket innebär att gärningsaktören inte behöver ha en god teknisk kompetens (Europol 2023b). Samtidigt lyfter Thomas (2022: 785) att kapaciteten att orsaka de riktigt stora skadorna ligger hos statliga aktörer:

> “Cyberattacks vary in difficulty and requisite capabilities and resources. The pool of possible attackers shrinks the greater the difficulty; some attacks can be carried out only by the most capable states.”

Denna bild återspeglas i Försvarsberedningens rapport Kraftsamling som konstaterar att de mest kvalificerade hoten inom cyberområdet kommer från stater och statsfinansierade aktörer eftersom dessa aktörer har kapacitet att kunna störa eller helt slå ut samhällsviktiga funktioner (Ds 2023:34). Cyberangrepp kan i vissa fall liknas vid ett väpnat angrepp och kan ”utgöra en delmängd av eller en indikator för ett sammansatt antagonistiskt angrepp, s.k. hybridaktiviteter” (Prop. 2020/21:30 s. 151). Att cyberoperationer kan används som militärt maktmedel i en upptrappningssituation inför en väpnad konflikt lyfts även fram av Försvarsberedningen*:*

8 För mer information om Crime-as-a-service se Europols hemsida: *https://www.europol.europa.eu/iocta/2014/chap-3-1-view1.html*

> ”Ett väpnat angrepp kan inledas med en förbekämpning av basområden, ledningsnoder, transport- och energisystem och annan kritisk infrastruktur. Det kan också rikta sig mot rent civila objekt i syfte att slå mot bland annat försvarsviljan. Bekämpningen kan genomföras med kryssningsrobotar, ballistiska robotar, bombflyg, attackflyg, cyberattacker och genom sabotage.” (Ds 2023:34 s. 33)

Rysslands anfallskrig mot Ukraina exemplifierar detta. I FOI-rapporten ”*Unravelling the Myth of Cyberwar – Five Hypotheses on Cyberwarfare in the Russo-Ukrainian War*” (Nilsson 2023:3) kommer författaren till slutsatsen att:

> ”även om nuvarande bevis tyder på frånvaron av omfattande destruktiv cyberkrigföring, är rysk cyberkrigföring fortfarande en kraft att räkna med, särskilt som en möjliggörare av informationspåverkan och som komplement till militära kinetiska operationer.”

Just den senare punkten adresseras i FOI-rapporten ”*Russian attacks on the Ukrainian power system*” (Odell m.fl. 2024), där missil- och drönarkampanjen mot elsystemet under vintern 2022-2023 åtföljdes av kraftfulla cyberattacker.

2.5 Situationsförståelse för cyberhot

Informationsinhämtning och analys av information utgör ett underlag till skapandet av lägesbilder.[9] Ett sätt att inhämta information är genom incidentrapportering. Inom EU ska alla medlemsländerna ha en organisation för hantering av it-incidenter och varje medlemsland måste även rapportera it-incidenterna till EU-kommissionen (MSB 2024b). NIS-direktivet[10], som kommer att ersättas av NIS2-direktivet och genomföras som lag i Sverige från början av 2025, föreskriver att både myndigheter och leverantörer av samhällsviktiga tjänster och digitala tjänster måste utföra denna rapportering. Det är medlemsländernas nationella CSIRT (Computer Security Incident Response Team)-enheter som ska samverka med unionens CSIRT-nätverk.[11]

9 Inom krisberedskap används begreppet lägesbild för att beskriva kommunikation och informationsutbytet mellan aktörer vid händelse av samhällsstörningar (Landgren & Borglund 2016).

10 EU-direktivet NIS (Network and Information Security Directive) började gälla 2018 genom lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster. Det ersattes av NIS2-direktivet i december 2022

11 CERT-SE är Sveriges nationella CSIRT och har i uppdrag att stötta samhället i arbetet med att hantera och förebygga it-incidenter genom bland annat rådgivning under pågående it-incident. MSB sammanställer varje år trender och slutsatser om samhällets informations och cybersäkerhet utifrån de it-incidenter som inrapporteras. MSB framhåller i årsredovisningen för 2023 att antalet rapporterade cyberangreppsförsök mot statliga myndigheter ökade kraftigt jämfört med tidigare år (ibid). Tidigare år har lägesbilden varit att de flesta it-incidenter har berott på systemfel eller den mänskliga faktorn (misstag), men för 2023 utgör angrepp den största kategorin, vilket delvis kan bero på rapporteringsbenägenheten har minskat samt att antalet rapporterade överbelastningsattackerna var fler 2023.

Ett annat sätt att inhämta information är genom underrättelseverksamhet. Underrättelseinformation ligger till grund för beslutsunderlag kring åtgärder och utgör även en förutsättning för aktörer att varna för cyberhot (Frisk 2019).

2.5.1 Identifiering av hot

Förvarning inom cyberområdet utgör en utmaning då hot och angrepp kan vara svåra att upptäcka. Att förlita sig på tidigare erfarenheter som en referensram för att upptäcka hot riskerar att ”osynliggöra det som inte kan uppfattas eller tolkas” (Agrell 2011: 187). Svårigheter med förvarning kan således kopplas till utmaningar med att varsebli, dvs. bli medveten om, och att identifiera vad som utgör faktiska hot. Agrell konstaterar också att det är svårt att förebygga för att förhindra angrepp om man ännu inte lyckats identifiera vilken form hotet kan ta. En oväntad utveckling eller plötsliga incidenter utgör en utmaning i förvarningsarbetet, eftersom det samtidigt innebär en begränsad tidsrymd för informationsinhämtning, bearbetning, analys och beslut om åtgärder. Därför krävs förmågan att tidigt kunna upptäcka förändrade mönster och skapa strategiska översikter av ”anomalier, det vill säga signifikanta förändringar i normalläget”, för att kunna förvarna om cyberhot och cyberangrepp (Severin 2018: 38).

Privatiseringen i länder som Sverige har inneburit en förskjutning från offentligt ägande till privat ägande. Detta innebär att många av de sensorer som tidigare fanns inom det offentliga återfinns idag hos aktörer i näringslivet (Severin 2018). Det finns således ett behov av att civila aktörer delger information om anomalier för att bidra till civil-militära cyberlägesbilder, vilket innebär ett behov av fördjupad samverkan och informationsdelning mellan en bredare krets samhällsaktörer, underrättelsetjänster och säkerhetstjänster (Sternudd 2023; Severin 2018). Severin (2018) lyfter att svårigheterna med förvarning inneburit att en förskjutning skett, från att övervaka potentiella hotaktörers beteenden till ett mer risk- och sårbarhetsfokuserat synsätt på nationens egna sårbarheter. Detta synsätt lägger fokus på samhällets motståndskraft och vikten av att öka robustheten i kritisk infrastruktur, nätverk och finansiella system.

2.5.2 Behov av förvarning

På senare tid har klassiska förvarningsmetoder som Indications and Warning (I&W) återigen lyfts som ett arbetssätt som kan anpassas för att möta aktuella utmaningar inom cyberområdet.[12] En vedertagen åsikt är att de mer kvalificerade hoten inom cyberområdet kommer från stater och statsfinansierade aktörer (Ds 2023:34) och att det därför krävs en förvarningsmetod som fokuserar på kunskapsinhämtning om motståndarens doktrin, militära kapacitet och hur motståndaren har agerat vid tidigare konflikter (Severin 2018). I&W är en metod i vilket man skapar en mängd hotscenarier som är mer eller mindre sannolika, vilka i sin tur hjälper analytiker att identifiera indikatorer som behöver bevakas, samt vilka åtgärder som behöver vidtas vid olika händelseutvecklingar. INSA[13] (2018: 3) menar att ett ramverk för cyberindikationer och varning utgörs av en:

> ”analytisk process där ett förväntat scenario inom cyberområdet bryts ner i indikatorer som kan övervakas kontinuerligt för att ge en varning om att scenariot kommer att förverkligas.”

Med andra ord, en anpassad version av I&W där upplevda faror (varningar) ska ses i en vidare bemärkelse där även säkerhetspolitiska faktorer inkluderas och att fokus flyttas från att enbart titta på de rent tekniska varningstecknen. Även Gentry (2022:5) menar att vi inte behöver uppfinna nya vägar, utan att vi kommer långt genom att läsa av den politiska atmosfären: ”traditional warning techniqes are adaptable to cyber space”. Lilly m.fl. (2019: 6) har en liknande utgångspunkt där författarna konstaterar att en “all-source intelligence analysis is very important for effectively assessing adversaries’ intentions in cyber space”.

12 Indications and Warning (I&W) utvecklades som en strategi främst under andra världskriget och kalla kriget, men konceptet har äldre rötter inom militär underrättelseverksamhet. Det formella ramverket för I&W togs fram för att förbättra förmågan att förutse och varna för fientliga militära handlingar, särskilt i samband med hotet om plötsliga angrepp eller eskalationer under kalla kriget.

13 The Intelligence and National Security Alliance (INSA) är en ideell, opolitisk yrkesorganisation för medlemmar från den offentliga och privata sektorn inom USA:s underrättelsegemenskap. *https://www.insaonline.org/*

2.6 Cybersäkerhet och cyberförsvar

Med det försämrade säkerhetspolitiska läget, som följt på bland annat konflikterna i Ukraina och Gaza[14], ökar behovet av ett motståndskraftigt samhälle mot cyberhot och cyberangrepp, vilket inkluderar förmågan att tidigt kunna agera på hot eller tecken på hot.

Definitioner inom cybersfären är notoriskt flytande. Cybersäkerhet och cyberförsvar är ytterligare exempel på begrepp som används tillsammans, som parord, i formuleringar för att beskriva åtgärder mot cyberhot och cyberangrepp. Det finns många exempel på hur antaganden om ett begrepp görs utan att samsyn kring de relevanta begreppen säkerställts (se Svahn m.fl. (2004) för en övergripande terminologisk beskrivning av cyberrelaterade termer). Det kan i vissa fall finnas ett mer eller mindre uttalat syfte med att inte definiera begreppen, så kallad strategisk ambivalens.

2.6.1 Definition av cybersäkerhet

Som ett exempel på det ovan nämnda begreppet strategisk ambivalens, menar Eidenskog m.fl. (2023) att det inte finns något behov av en tydlig och enad definition av cybersäkerhet då området är för brett och därmed svårdefinierat. De anger dock vidare att:

> ”det är mer relevant med en definition utifrån aktuell kontext i respektive fall då olika organisationer lägger in olika aspekter i termerna.” (Eidenskog m.fl. 2023: 9)

För denna rapport utgår vi dock från den definition framtagen av EU:s cybersäkerhetsorganisation Enisa (2017), där cybersäkerhet anses omfatta:

> ”alla aspekter av förebyggande, prognoser; tolerans; upptäckt; begränsning, avlägsnande, analys och utredning av cyberincidenter. Med tanke på de olika typerna av komponenter i cyberrymden bör cybersäkerheten omfatta följande egenskaper: tillgänglighet, tillförlitlighet, säkerhet, konfidentialitet, integritet, underhållsmässighet (för materiella system, information och nätverk) robusthet, överlevnadsförmåga, resiliens (för att stödja cyberrymdens dynamik), ansvarsskyldighet, autenticitet och oavvislighet (för att stödja informationssäkerhet).”

14 Den militära konflikten mellan Hamas och Israel har enligt RIA inneburit en ökning av ”ideologisk hacktivism” som syftar till att det egna landet kan drabbas när andra länder utsätts för cyberattecker. Ett exempel som RIA lyfter fram är cyberattacken mot programmerbara logiska styrenheter tillverkade i Israel, som störde driften i lokala estniska fjärrvärme- och pumpstationer (RIA 2024).

2.6.2 Definition av cyberförsvar

Cyberförsvar och cybersäkerhet är sammanflätade begrepp men i och med att cyberoperationer och cyberattacker har fått en allt större betydelse som maktmedel för stater (och statsunderstödda grupper) så ”knyts begreppet cyberförsvar allt närmre den nationella försvarsförmågan” (Sternudd 2023:13). Vi kommer i denna rapport utgå ifrån denna definition av cyberförsvar:

> ”En nations eller annan aktörs samlade förmågor och åtgärder, såväl offensiva som defensiva, till skydd för dess kritiska cyberinfrastruktur som syftar till att säkerställa kritiska samhällsfunktioner samt förmågan att försvara sig mot kvalificerade angrepp.” (Zouave 2020:7)

2.6.3 Förhållandet mellan cyberförsvar och cybersäkerhet

Efter att ha analyserat de grundläggande begreppen, diskuteras nedan hur dessa interagerar och förhåller sig till varandra. Den modell som vi valt att använda oss av är Sternudds cyberförsvarspyramid. I Sternudds rapport Cyberförsvar och cybersäkerhet (2023) illustreras cyberförsvar i form av en pyramid i fem nivåer som beskriver cyberförsvar utifrån dess kärnuppgifter och samverkande funktioner (se figur 1), av vilka cybersäkerhet är en sådan funktion.

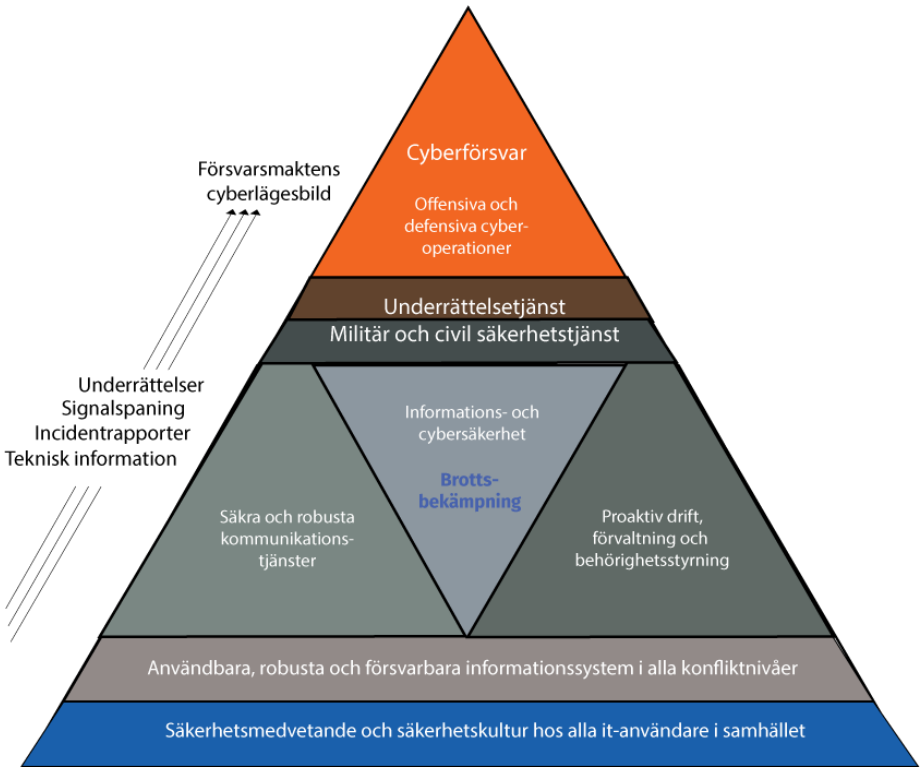
Sternudds cyberpyramid visar på hur alla nivåer i pyramiden behövs för att upprätthålla ett nationellt cyberförsvar. Information i form av underrättelse, signalspaning, incidentrapportering och teknisk information flödar genom cyberförsvarspyramiden, från bottenplattan mot toppen. Det är dock viktigt att understryka att om det inte finns en mottagare eller en väluppbyggd organisation och funktion för att ta hand om informationen och har möjlighet att agera och fatta beslut om åtgärder blir utfallet ineffektivt.[15]

Ett motståndskraftigt samhälle mot cyberangrepp bygger därför dels på ett aktivt cyberförsvar, med möjligheten att både upptäcka och förvarna om cyberhot, och dels på en cybersäkerhetsstrategi och en säkerhetsmedvetenhet som genomsyrar hela samhället. Cyberpyramiden blir mer motståndskraftig om förebyggande aktiviteter genomförs i basen av pyramiden, med andra ord på en bred samhällsförankring.

Integreringen av cybersäkerhet inom det nationella cyberförsvaret bör enligt Sternudd ses som en totalförsvars- och samhällsangelägenhet. För ett motståndskraftigt samhälle mot cyberhot behöver cybersäkerhetsmedvetenheten vara starkt förankrad bland samhällets it-användare. Det är därför viktig att tydliggöra att det breda samhällsperspektivet inte ska tolkas som att:

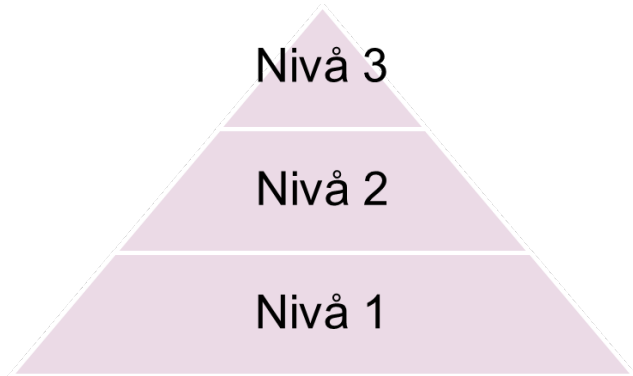
15 Se exempelvis Sternudd 2023; Severin 2018, och Ödlund 2019.

”alla medborgare är en del av cyberförsvaret, men väl att de utgör en del i samhällets totala motståndskraft och robusthet. Däremot är de tveklöst en del av samhällets cybersäkerhet, vilket är en förutsättning för ett starkt cyberförsvar.” (Sternudd 2023: 19)



Figur 2.1 Cyberförsvarspyramiden
Källa och illustration: Patrick Sternudd (2023: 38) med författarens medgivande.

I denna rapport används en förenkling av Sternudds cyberförvarspyramid. Den har tagits fram iterativt, under arbetets gång, och korrelerar till punkterna i analysen. Sternudds cyberförvarspyramid har delats upp i tre olika nivåer. Den grundläggande nivån är säkerhetsmedvetenheten och säkerhetskulturen hos samhällets it-användare, den andra nivån inkluderar information- och cybersäkerhet och den översta nivån är de offensiva och defensiva cyberoperationerna (cyberförsvar), se figur 2.2 nedan.



Figur 2.2 Förenkling av Sternudds cyberförsvarspyramid

2.6.4 Whole-of-nation

Hur kan Sternudds cyberpyramid appliceras i praktiken? Ett sätt är att tillämpa en s.k. *whole-of-nation*-strategi, vilken involverar gemensamma insatser från regeringen, den privata sektorn och civilsamhället för att hantera utmaningar.

Whole-of-nation ska inte blandas samman med närbesläktade begreppet *whole-of-government*. Båda strategierna syftar till att förbättra effektivitet och respons, men där *whole-of-nation* har en bredare samhällsinriktning har *whole-of-government* en mer administrativ inriktning och fokuserar på samordning inom regeringen. (Doyle 2019). Genom att implementera en *whole-of-nation*-approach kan länder mobilisera resurser och expertis från hela samhället för att hantera komplexa och tvärsektoriella utmaningar. Begreppet används inte bara inom cyberdomänen, utan används även inom andra områden, såsom hälsofrågor**,** konflikthantering**,** nationell beredskap och katastrofhantering.[16] Exempelvis beskriver WHO en *whole-of-nation-approach* i sin beredskap för pandemier, där organisationen noterar att approachen:

> ”innebär att statliga myndigheter engagerar alla relevanta intressenter, inklusive (men inte begränsat till) mellanstatliga organisationer, den privata sektorn, civilsamhället, samhällen, familjer och individer, i stöd av gemensamma ansträngningar för att förebygga och kontrollera epidemier.” (WHO 2022)

Whole-of-nation-strategin inom cyberdomänen handlar om att skapa en enhetlig och koordinerad insats som utnyttjar hela samhällets styrkor och resurser för att skydda mot cyberhot. Här utgår strategin från att cybersäkerhet är ett delat ansvar

16 Whole-of-nation i samband med konflikter: Doyle, B. (2019). The Whole-of-nation and Whole-of-Government Approaches in Action. *InterAgency Journal*, 10, 105-122, I samband med hälsokriser: Hsieh, C. W., Wang, M., Wong, N. W., & Ho, L. K. K. (2021). A whole-of-nation approach to COVID-19: Taiwan’s National Epidemic Prevention Team. *International Political Science Review*, 42(3), 300-315.

och kräver aktivt deltagande från flera intressenter över olika sektorer (Klimburg 2011). I denna rapport har vi adapterat Alexander Klimburgs (2011) grundläggande principer för *whole-of-nation*-ansatsen till cyberdomänen:

- Nationell Cyberdoktrin: Upprätta en tydlig och sammanhängande nationell strategi och policyer för cybersäkerhet som definierar roller och ansvar för alla intressenter.
- Offentlig-privat partnerskap: Främja starkt samarbete mellan statliga enheter och den privata sektorn, som äger och driver mycket av den kritiska infrastrukturen.
- Engagemang av civilsamhället: Involvera civilsamhällesorganisationer, akademin och allmänheten i cybersäkerhetsinsatser.
- Internationellt samarbete: Engagera sig med internationella partners för att hantera den globala karaktären av cyberhot.
- Kapacitetsbyggande: Utveckla och förbättra färdigheter och kapaciteter hos alla intressenter, inklusive statlig personal, privata sektorns anställda och medborgare.
- Resiliens och redundans: Bygga robust och motståndskraftig cyberinfrastruktur som kan motstå och återhämta sig från attacker.
- Delning av hotinformation: Upprätta mekanismer för realtidsdelning av hotinformation mellan intressenter.
- Regulatoriska och rättsliga ramar: Utveckla och genomdriva lämpliga regleringar, standarder och rättsliga åtgärder för att säkerställa cybersäkerhet.
- Incidentrespons och hantering: Skapa samordnade och effektiva incidentresponsramar som involverar alla relevanta intressenter.
- Ansvarsskyldighet och styrning: Säkerställa tydliga styrstrukturer och ansvarsmekanismer för cybersäkerhetsinsatser.

De grundläggande principerna för *whole-of-nation*-strategin återspeglas i cyberförsvarspyramiden, vilket i sin tur påvisar hur alla nivåer i pyramiden kan engageras för att upprätthålla ett nationellt cyberförsvar. Det innebär att det finns en samklang mellan Sternudds cyberförsvarspyramid och *whole-of-nation*-strategin, som används som grund för analysen i denna studie.

2.7 Sammanfattning

För att skapa ett robust cyberförsvar krävs en förståelse av cyberhot och cyberangrepp, där hot definieras som omständigheter med potential att skada verksamheter, medan angrepp är skadlig aktivitet. Cyberförsvar involverar både offensiva och defensiva åtgärder för att skydda kritisk infrastruktur, medan cybersäkerhet (som utgör en del av cyberförsvaret) handlar om att skydda mot incidenter genom att upprätthålla systemens tillgänglighet, tillförlitlighet och integritet. För att effektivt hantera cyberhot krävs båda, i ett samhällsgemensamt grepp som involverar samarbete mellan regering, privat sektor och civilsamhälle. Detta illustreras genom Sternudds teoretiska tankar om cyberförsvarspyramid och den praktiska applikationen av *whole-of-nation*-strategin.

3. Estland inom cyberdomänen

Detta kapitel ger en bakgrundsbild av Estland som aktör inom cyberdomänen. Först ges en beskrivning av hur den estniska cyberorganisationen är uppbyggd och vilka målen är för den estniska cyberstrategin. Efter detta följer en översikt av hur Estland står sig i ett internationellt perspektiv, baserat på cyberindex och internationella jämförelser.

Estland är en baltisk nation vars moderna historia präglats av perioder av ockupation, med över femtio år av sovjetiskt styre som sträckt sig från andra världskrigets slut till självständigheten 1991. Efter att ha återfått sin självständighet omvandlades Estland till en modern och digitalt avancerad ekonomi (Kohler 2020) och integrerades snabbt i västliga institutioner som EU och Nato. En anledning till medlemskapen, särskilt i Nato, var att bättre kunna försvara sig mot Ryssland (Gustafsson 2021).

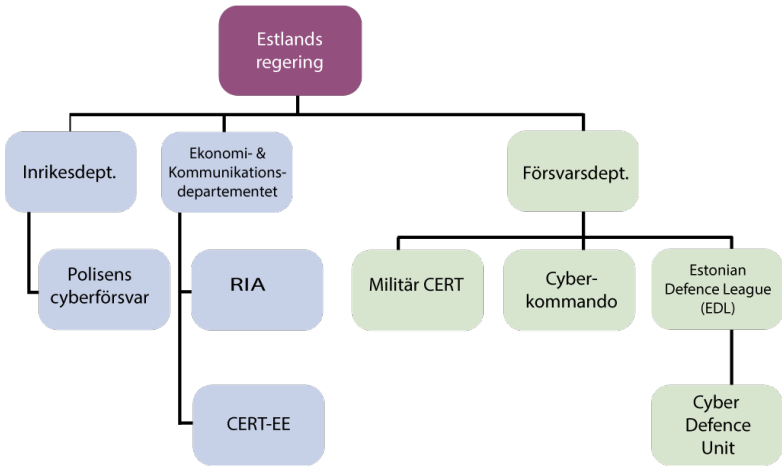
Direkt efter Estlands självständighet identifierades digitalisering och potentialen i cyberdomänen som viktiga byggstenar för landets utveckling och säkerhet. Beslutet att prioritera digitalisering som en del av det moderniserade utbildningssystemet togs tidigt, och bara fem år efter frigörelsen lanserades det så kallade *Tiger Leap*-programmet (Tiigrihüpe) för att utnyttja teknik för undervisning och lärande med målet att bygga upp skolornas tekniska infrastruktur (Kohler 2020).

3.1 Estlands cyberorganisation

Denna rapport gör inte anspråk på att ge en uttömmande beskrivning av samtliga aktörer och samverkansorgan inom det estniska cyberområdet, detta kapitel syftar snarare till att ge en överblick av de viktigaste aktörerna.

Ansvaret för cybersäkerhetsfrågor ligger i Estland på Inrikesdepartementet, vilket inkluderar polisen som arbetar mot cyberrelaterad brottslighet, samt Ekonomi- och Kommunikationsdepartementet, under vilket den nationella cybersäkerhetsbyrån RIA och CERT-EE är placerade.[17] Cyberförsvar å sin sida ligger på Försvarsdepartementet och inkluderar den militära CERT:en och Cyberkommando (Kohler 2020). Se organisationsbild nedan.

17 RIA står för Riigi Infosüsteemi Amet. CERT-EE är en nationell estnisk aktör vars motsvarighet i Sverige heter CERT-SE (*https://www.cert.se/*).



Figur 3.1 Organisationsbild (författarnas egna)

3.1.1 Aktörer

- Polisens cyberförsvar: Enheten för cyberbrott vid Estlands polis- och gränsbevakningsmyndighet (PPA), hanterar utredningar av cyberbrott som hacking, bedrägeri och andra digitala brott. Den samarbetar nära med lokala och internationella brottsbekämpande organ.[18]

- RIA: Estlands centrala myndighet för övervakning och hantering av cyberhot. De ansvarar för att övervaka cybersäkerhetsläget i landet, utfärda varningar om hot och ge råd om säkerhetsåtgärder. Organisationen arbetar brett med cybersäkerhetsmedvetenhet och informationsinsatser. Ur ett operativt perspektiv har RIA har två huvudsakliga grenar: cybersäkerhet och informationssystem. Den förstnämnda övervakar den nationella incidenthanteringsgruppen CERT-EE (*Computer Emergency Response Team* - Estonia), som spelar en nyckelroll i skyddet av kritisk infrastruktur och har omfattande tillsynsbefogenheter över nationella och lokala myndigheters informationssystem, leverantörer av viktiga tjänster, telekommunikationsföretag och andra leverantörer av digitala tjänster. Det statliga informationssystemet ansvarar för förvaltningen av säkert informationsutbyte. Estlands nationella CERT-EE har en central roll i att samordna insatser vid cyberincidenter och förebygga attacker (Kohler 2020:8).

18 Läs mer här: *https://www.politsei.ee/.*

- Estlands militära CERT (Computer Emergency Response Team): En specialiserad enhet inom Estlands försvarsmakt som ansvarar för att skydda militära nätverk och system mot cyberhot.[19]

- Estlands Cyberkommando (*Cyber Command*): En gren inom Estlands försvarsmakt som ansvarar för att leda och genomföra operationer i cyberdomänen. Det inrättades 2018 för att skydda Estlands militära system och infrastruktur mot cyberattacker samt för att genomföra offensiva och defensiva cyberoperationer. Det spelar en nyckelroll i Estlands nationella försvarsstrategi, särskilt med fokus på hot från statsaktörer och andra avancerade cyberangripare.[20]

- Estonia Defence League: En frivillig nationell försvarsorganisation som verkar under Estlands försvarsministerium. Den är organiserad enligt militära principer, har tillgång till vapen och genomför övningar av militär karaktär. Cyber Defence Unit (CDU) är placerad inom Estonia Defence League (EDL, en frivillig militär nationell försvarsorganisation med liknande uppgifter som det svenska Hemvärnet). CDU har en bred uppgift med syfte att bistå civila cyberstrukturer i fredstid och skapa stödresurser som kan tillhandahållas i kristider. Enheten skapades 2010 som en följd av 2007 års cyberattacker (Cardash m.fl. 2013).

3.1.2 Samverkansstrukturer

Det estniska cybersäkerhetsrådet (*Estonian Cyber Security Council*) är en central del av Estlands cybersäkerhetsinfrastruktur, med ansvar för strategisk planering, samordning av statliga insatser och utveckling av policyer. Dess uppgifter inkluderar utarbetande och uppdatering av den nationella cybersäkerhetsstrategin (mer om detta nedan).

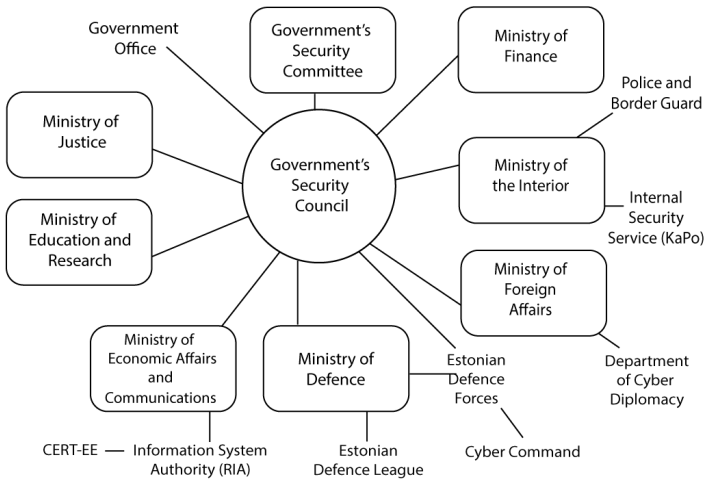
Cybersäkerhetsrådet inrättades 2017 för att stärka Estlands förmåga att hantera cybersäkerhetshot och för att samordna nationella cybersäkerhetsinsatser. De ansvarar för att utveckla och implementera Estlands nationella cybersäkerhetsstrategi, övervaka cybersäkerhetssituationen och föreslå förbättringar samt policyändringar (Kohler 2020). Rådet består av representanter från olika ministerier och statliga myndigheter som har en roll i cybersäkerhetsfrågor. Dessutom inkluderar rådet representanter från andra relevanta statliga organ och ibland även privata sektorns experter (IISS 2024).

19 Mer information om hur CERT är uppbyggt finns på *www.RIA.EE*.

20 Läs mer här: *https://mil.ee/en/landforces/cyber-command/*.

Cybersäkerhetsrådet spelar en viktig roll vid hanteringen av cyberincidenter genom att samordna statlig respons och säkerställa att alla relevanta aktörer arbetar tillsammans effektivt. Det övervakar nationella cybersäkerhetsincidenter och arbetar med RIA och andra organisationer för att utveckla responsplaner och åtgärder.

I juni 2021 trädde EU:s förordning om inrättande av Europeiska centrumet för cyberkompetens (ECCC) och nätverket av nationella samordningscentrum (National coordination center, NCC-EE) i kraft. Inrättandet av det nationella



Figur 3.2 Organisationsbild över det estniska cybersäkerhetsrådet
Källa: Kohler (2020:8) med författarens tillåtelse.

centret i Estland ses som en del av landets satsning på att stärka sin cybersäkerhetskapacitet och att samordna nationella insatser i linje med Europeiska unionens cybersäkerhetsstrategi och Digital Europe Programme.[21]

3.2 Styrdokument för cybersäkerhet

Estlands strategi har inte tillkommit i ett vacuum. Kohler (2020) konstaterar att medan landet har ett stort antal olika strategier och policydokument, har de gjort ett viktigt arbete i att se till att dessa samverkar genom att i styrdokument lyfta fram relaterade sektorsstrategier och integrera dessa. Estlands digitala agenda, nationella säkerhetsstrategi och nationella säkerhetskoncept utgör tillsammans ett ramverk för landets cybersäkerhetsarbete.

21 Läs mer om centret här: *https://www.ria.ee/en/cyber-security/national-coordination-center-ncc-ee/national-coordination-center-ncc-ee.*

3.2.1 Den digitala agendan

Estland har sedan cyberattackerna 2007 satsat på den digitala utvecklingen och den digitala agendan uppdateras regelbundet. Den nuvarande versionen beskrivs som:

> ”en långsiktig strategi för att säkerställa framgången för ett kraftfullt estniskt digitalt samhälle, där alla människor får den bästa digitala upplevelsen.” (Digital Agenda 2030)

Den digitala agendan är indelad i tre områden: e-stat, konnektivitet och cybersäkerhet. Den senast publicerade digitala agendan sträcker sig till 2030 och målsättningen innehåller flera viktiga punkter gällande cybersäkerhet:

- Nationell cybersäkerhetsstruktur: Etablera en robust ram för att säkerställa säkerheten för Estlands digitala infrastruktur.
- Hotanalys och riskhantering: Förbättra kapaciteten att analysera trender, risker och effekter relaterade till cyberhot.
- Ökad cybersäkerhetskapacitet: Bygga upp resurser och kapaciteter för att upprätthålla och förbättra cybersäkerhetsåtgärder.
- Krisrespons: Utveckla effektiva strategier för att hantera cyberincidenter och kriser.
- Innovationspolitik: Uppmuntra innovation inom cybersäkerhet för att ligga steget före nya hot.
- Kompetensutveckling: Hantera bristen på arbetskraft genom att utbilda och behålla skickliga cybersäkerhetsproffs.

3.2.2 Estlands nationella säkerhetsstrategi

Som noteras ovan ingår Estlands nationella cybersäkerhetsstrategi i den digitala agendan. Centrala mål inkluderar etablering av en robust cybersäkerhetsram, förbättrad hotanalys och riskhantering, ökad kapacitet, effektiv krishantering, främjande av innovation och kompetensutveckling. Strategin revideras vart fjärde år med en halvtidsöversyn och prioriterar teknologisk motståndskraft, krishantering och integrerat ledarskap. Utmaningar som identifierats i arbetet med cybersäkerhetsstrategin inkluderar resursbrist, implementeringssvårigheter, snabb teknologisk utveckling och behovet av ökad medvetenhet och utbildning. Den första cybersäkerhetsstrategin

publicerades 2008 och har sedan dess uppdaterats två gånger. Ett hållbart digitalt samhälle och ett cyberkunnigt samhälle är prioriterade områden för cybersäkerhetsstrategin, vilket går i linje med de grundläggande principerna för *whole-of-nation*-strategin inom cyberdomänen.

I litteraturen finns få exempel på kritik av den estniska cybersäkerhetsstrategin. De utmaningar som nämns är väldigt övergripande och kan appliceras på denna typ av strategi i allmänhet (se bland annat Odebade & Benkhelifa, 2022). Den kritik som lyfts är bland annat att för att strategin ska vara effektiv behöver hela samhället vara medvetna om cybersäkerhetsfrågor och ha en grundläggande kunskap om hur man skyddar sig. Den snabba teknologiska utvecklingen inom teknik innebär att en nationell cybersäkerhetsstrategi snabbt blir föråldrad. Cybersäkerhetsstrategin måste därför vara flexibel och uppdateras regelbundet för att vara effektiv. Samtidigt som implementeringen av en omfattande cybersäkerhetsstrategi kan vara utmanande och kräver samordning mellan olika myndigheter, företag och organisationer, vilket ibland kan leda till byråkratiska hinder och ineffektivitet.

3.2.3 Estlands nationella utbildningsstrategi

Något som är indikativt för hur Estland ser på vikten av en befolkning förankrad i det digitala samhället är hur digitaliseringen prioriterats i den nationella utbildningsstrategin. Den så kallade ”strategin för livslångt lärande” är en utbildningsplan som uppdateras regelbundet. I den förra upplagan (2014) diskuteras bland annat vikten av att integrera cybersäkerhet i samhället (*Lifelong Learning Strategy* 2030) medan det i den nu gällande strategin (2021) konstateras att digitala lösningar och digital kompetens har både ökat och förbättrats.

En tolkning är att initiativen utgjort en grundläggande förutsättning för Estlands höga digitaliseringsgrad. Estland har sedan dess fortsatt prioritera utbildning samt delgivning av cyberinformation på en bred front i samhället.

3.2.4 Estlands nationella säkerhetskoncept

Estlands nationella cybersäkerhetsstrategi är en del av landets nationella säkerhetskoncept. Det nationella säkerhetskonceptet lyfter särskilt fram cyberdomänen och Natos artikel 5:

> ”Cyberrymden är både en oberoende domän och en möjliggörare av andra domäner, och de medföljande riskerna får inte underskattas. /.../ En hybridattack skulle kunna leda till att Natos artikel 5 utlöses.” (MKM 2023:7)

Nato artikel 5 innebär att ”ett väpnat angrep mot en eller flera av parterna i Europa eller Nordamerika betraktas som ett angrepp mot samtliga parter” (Regeringskansliet 2024). Frågan kring hur cyberangrepp ska tolkas i ljuset av artikel 5 är något som Estland lyft i samband med cyberattackerna mot landet 2007 och har varit föremål för viss debatt. Kritiker varnar för att det är oklart om det är lämpligt eller möjligt att likställa cyberangrepp med militära angrepp som skulle kunna aktivera exempelvis Natos artikel 5 (van Ooijen 2020).

3.3 Internationella jämförelser

För att få en bild av hur Estland står sig i jämförelse med andra länder ges i bilaga 4 en översikt av tre olika internationella cyberindex där det framgår att Estland placeras högt jämfört med andra länder. Detta gäller framför allt i områdena globalt ledarskap, utbildning, medvetandegörande arbete, personaldatahantering, incidenthantering och hantering av cyberbrott (*National Cyber Security Index*[22]). I kategorin cyberförsvar hamnar Estland på plats 12 i en jämförelse med 30 länder (*Cyber Power Index*[23]).

Det finns även ett index för digital ekonomi och digitalt samhälle (Desi) som publiceras av EU-kommissionen och som följer EU-ländernas framsteg när det gäller digital konkurrenskraft. Här uppvisade Estland särskilt bra resultat i kategorin it-expertis, där it-specialister utgjorde 6,2 % av arbetskraften i landet – i EU som helhet ligger siffran på 4,5% (EU-kommissionen, 2022).

3.3.1 Cybersäkerhetsstrategier och hantering av cyberhot

Det finns en uppsjö av olika perspektiv på cybersäkerhet och cyberförsvar. I denna studie studeras specifikt cybersäkerhetsstrategier och hanteringen av cyberhot. En cybersäkerhetsstrategi är givetvis inte ensamt en indikation på hur väl cybersäkerhetsarbetet genomförts, men ger en viss vägledning för att uppnå ett mål. Det är rimligt att utgå från att länder som har strategier som löser viktiga frågor på ett heltäckande sätt har ett bättre verktyg för det fortsatta arbetet med att säkerställa cybersäkerheten.

Estlands förmåga att möta cyberhot och cyberangrepp rankas högt i ett flertal internationella jämförelser. I en internationell jämförelse med 20 länders nationella cybersäkerhetsstrategier lyfts Estland cybersäkerhet som världsledande, vilket anses vara ett resultat av cyberattackerna mot den estniska ekonomin 2007 (Odebade &

22 *https://ncsi.ega.ee/* även Osula (2022).

23 *https://www.belfercenter.org/publication/national-cyber-power-index-2022.*

Benkhelifa 2022). Estland är även ett av de få länder som uppdaterar sin cybersäkerhetsstrategi regelbundet, till skillnad från ett flertal länder som inte har uppdaterat sina ursprungliga cybersäkerhetsstrategier en enda gång. Estland är även ett av fyra länder som hänvisar till cyberkrigsföring i sina strategier (övriga länder är USA, Tyskland och Nederländerna) (Shafqat & Masood 2016). För mer detaljerad redogörelse se bilaga 3.

Gemensamt för samtliga jämförda länder är de otydliga avgränsningarna mellan cybersäkerhet och cyberförsvar. Shafqat & Masood (2016:132) noterar att Estland och Nederländerna endast implicit definierat cyberrymden i sina cybersäkerhetsstrategier och har inte lämnat fullständiga definitioner och Odebade & Benkhelifa (2022) konstaterar att det inte finns en enhetlig förståelse av termen "cybersäkerhet" och att detta gör att jämförelser är svåra (men inte omöjliga) att göra. Även Štitilis et al (2016:1162) lyfter att det i ländernas olika strategier sällan ges definitioner på vad som menas med säkerhet kontra försvar, men att de få länder som skiljer på cybersäkerhet och cyberförsvar pekar ut just försvarsfrågor som ett viktigt mål. När det gäller cyberförsvar nämner Estland, Belgien, Tjeckien, Estland, Ungern, Nederländerna och Spanien sitt samarbete med Nato, och hänvisar till kollektivt försvar. En observation är att det i de flesta nationella strategier finns frågor relaterade till skydd av kritisk infrastruktur, utan att termen cyberförsvar nämns explicit.

3.4 Cyberangrepp – då och nu

I början av 00-talet inträffade ett flertal händelser som underströk behovet av motståndskraft. Idag testas och utmanas Estlands cybersäkerhetsstrukturer som en följd av regionala spänningar som kriget i Ukraina medfört. Dessa händelser har bidragit till att forma landets cybersäkerhetspolicy som den ser ut idag.

3.4.1 Då: Cyberangrepp som nationell formativ faktor

I Kevin Kohlers (2020) rapport *Estonia's National Cybersecurity and Cyberdefense Posture* hänvisas till några viktiga incidenter som *trigger events* eller utlösande händelser. Angreppet 2007, mer om detta nedan, beskrivs som en nationell formativ faktor, både i litteraturen och i de intervjuer som genomförts inom ramen för detta projekt.

3.4.1.1 2007 års attack

Estland har i många år varit måltavla för politiskt motiverade cyberattacker från aktörer med kopplingar till Ryssland. Idag ses Ryssland som den dimensionerande motståndaren för det estniska försvaret.[24] Att det estniska cyberförsvaret behövde ha en beredskap för att möta stora utmaningar blev uppenbart i samband med en storskalig strategisk cyberattack mot den estniska infrastrukturen 2007. Efter flytten av ett kontroversiellt monument från Sovjettiden, utsattes Estland för vad som beskrivits som ”en tidigare aldrig skådad” nivå av distribuerade överbelastningsattacker som varade i 22 dagar och riktade sig mot det estniska parlamentet, banker, ministerier, tidningar och radio- och tv-bolag (Ottis 2018:1). Attackerna orsakade ingen bestående skada, men de fungerade som en kraftfull väckarklocka. Konsekvenserna innebar att Estland påbörjade arbetet med att ta fram en övergripande nationell strategi för cybersäkerhet – och blev det första europeiska landet att ta fram en sådan strategi.

2007 års cyberattacker var formativa inte bara för Estland, utan även globalt. Shafqat & Masood (2016) beskriver hur attackerna fick många länder att inse att deras nationella informationsinfrastruktur var mycket sårbar för cyberattacker och Štitilis et al (2017) konstaterar att attackerna ledde till att statliga företrädare för första gången officiellt begärde att artikel 5 i Nordatlantiska fördraget skulle kunna användas i en cyberattack. Shafqat (2016) konstaterar att:

> “De framträdande cyberattackerna i det förflutna, särskilt attackerna mot Estlands internetinfrastruktur 2007 /…/ fick många länder att inse att /…/ deras nationella informationsinfrastruktur var mycket sårbar för cyberattacker. Det ledde också till inrättandet av cyberkapacitet på federal nivå och utarbetandet av en handlingsplan på hög nivå, dvs. den nationella cybersäkerhetsstrategin (NCSS).”

Andra erfarenheter såsom sårbarheter i estniska e-ID, den ryska annekteringen av Krim och cyberangreppen *WannaCry* och *NotPetya* har varit mindre dramatiska, men icke desto mindre viktiga i att understryka vikten av cybersäkerhet.

3.4.1.2 Sårbarheter i estniska e-ID

En incident som bekräftade vikten av ett fungerande cyberförsvar, inträffade 2017. Den utgör ett gott exempel på den motståndskraft som landet uppvisat i just cybersfären, även om krisen inte utlöstes av en antagonistisk attack, utan snarare handlade om en förebyggande ansats. CERT-EE informerades av ett schweiziskt forskarteam om en sårbarhet i estniska e-ID den 30 augusti.[25] Den 25 oktober

24 I Estlands nationella säkerhetskoncept (Estonia National Security Concept 2023) konstateras att “the greatest security threat to Estonia is the Russian Federation, whose objective is to dismantle and rewrite Europe’s security architecture and the rules-based international order, and to restore the politics of spheres of influence. The threat to Estonia based on these objectives is an existential one. /…/ The threat the Russian Federation poses to Estonia is a long-term one” (2023:6).

25 Den estländska digitaliseringsmyndighetens konstaterar att 99% av estniska medborgare använder sig av e-ID *https://e-estonia.com/wp-content/uploads/e-identity-factsheet-okt2023.pdf*

hade landet hunnit utvecklat nya krypteringssystem för ID-kortet och testat hur den nya uppdateringen skulle påverka existerande e-ID:n. Den 30 oktober gick man ut med information till alla medborgare där de uppmanades uppdatera sina ID:n (Atna-Dvořák m.fl. 2021). Tre dagar efter det blockerades alla ouppdaterade ID-kort, som alltså inte kunde användas om de inte uppdaterades.

3.4.1.3 Den ryska annekteringen av Krim

I samband med annekteringen förekom flera ryska cyberattacker mot ukrainska myndigheter, vilket gjorde att den redan uppkomna frågan om cyberförsvar av digitala monument (dvs. webbplatser med symbolisk status, t.ex. president.ee), Estlands digitala kontinuitet och statens funktion i alla nödsituationer aktualiserades ytterligare (Kohler 2018). Estland utvecklade då cyberkapacitet utanför landets gränser.[26] 2017 nådde landet en överenskommelse med Luxemburg om att öppna världens första dataambassad, vilket gjorde det möjligt för esterna att lagra data i ett fysiskt datacenter som verkar under estnisk jurisdiktion men på ett annat lands territorium.[27]

3.4.1.4 Cyberangrepp

Cyberangreppen *WannaCry* och *NotPetya* hade inte någon större inverkan på det estniska systemet, då man sedan tidigare haft en långtgående strategi att uppdatera gamla system och kommunicera ut vikten av att uppdatera programvara. Strategin tycks ha burit frukt, då effekterna av attackerna varit betydligt lägre än i andra länder, vilket indikerar att landets strategi utvecklats i rätt riktning. Statliga RIA hade dessutom varit både proaktiva och reaktiva i sina kontakter med drabbade företag och organisationer, vilket har skapat en grogrund för fortsatt förtroende och god samverkan framöver.

3.4.2 Nu: Cyberangrepp i skuggan av Ukrainakriget

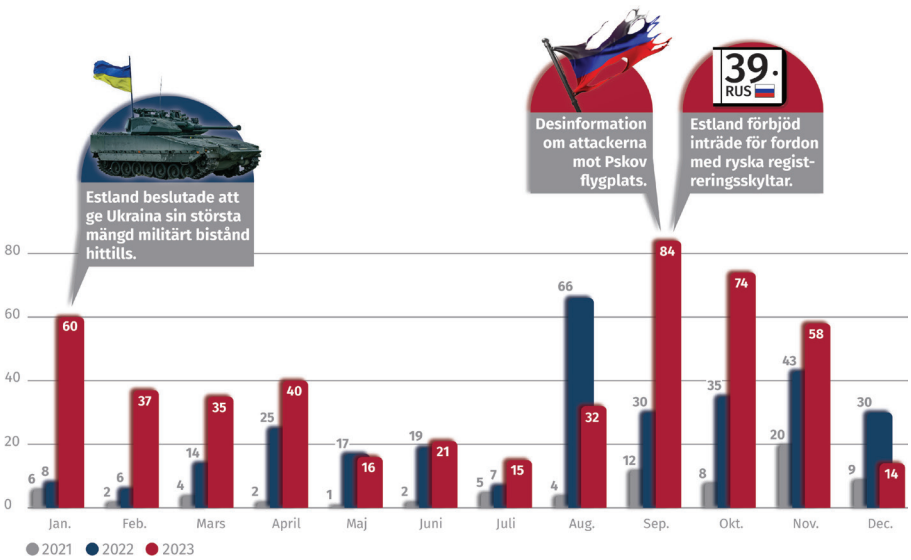
Idag är den dimensionerande motståndaren i Estlands cybersäkerhetsarbete Ryssland (Bartoszewicz & Prucková 2024). Esterna har varit tydliga med att Rysslands agerande i samband med annekteringen av Krim och de efterföljande cyberattackerna mot Ukraina tjänstgör som en påminnelse om hotet från ryska aktörer. Estland har under de senaste åren varit bland de mest uttalade kritikerna av Rysslands agerande i närområdet, vilket har lett till reaktioner av olika slag. Det är, som tidigare noterat, svårt att attribuera cyberattacker, och korrelation är inte samma sak som kausalitet, men vi vill ändå argumentera för att denna korrelation ändå avslöjar något.

26 Läs mer här: *https://e-estonia.com/solutions/e-governance/data-embassy/*

27 Enligt uppgift från IISS finns planer för ytterligare en estnisk data-ambassad, denna gång i ett icke-europeiskt land, men det finns ingen mer information om detta (IISS, 2023).

3.4.2.1 Överbelastningsattacker

Ett exempel på hur det kan se ut ges i nedan illustration över utvecklingen av överbelastningsattacker mot estniska intressen. RIA konstaterar i sin årsrapport för 2024 att antalet överbelastningsattacker på estniska system har ökat markant sedan den ryska invasionen av Ukraina 2022 (se figur 3.5, nedan). Överbelastningsattacker orsakar inte samma nivå av skada som exempelvis gisslanprogram (*ransomware*), men utgör ändå ett problem. RIA beskriver dessa attacker som politiskt motiverade och menar att de främst utförs av Kremlvänliga hacktivister[28] och grupper. Överbelastningsattackerna uppges ha kommit i vågor. En av de tidigaste vågorna kom i april 2022 under Nato-cyberövningen *Locked Shields* som ägde rum i Tallinn, och hade enligt RIA ingen större påverkan på den digitala infrastrukturen. De följande



Figur 3.3 Antalet DDoS-attacker i Estland, för åren 2021 - 2024

Källa: Cyber Security In Estonia (Information System Authority, RIA 2024:27), med författarens tillåtelse. Layouten är omarbetad av Patric Karlsson, FOI. Bilderna ovanför stapeldiagramet är hämtade från Adobe, Försvarsmakten, Shutterstock

28 Ordet hacktivism är en sammanslagning av hacking och aktivism. Karatzogianni (2015) beskriver fenomenet mycket brett som operationer där hackningstekniker används mot ett måls webbplats i syfte att störa normal verksamhet men inte orsaka allvarlig skada och ger exempel som virtuella blockader, webbhackningar, dataintrång och datavirus. Det finns ett ryskt kluster av hacktivister som inkluderar hotaktörer såsom Killnet (men även Fancy Bear och Sandworm, som tagit på sig ansvaret för hackningar av USA:s demokratiska nationella kommitté respektive lanseringen av den förödande ransomwaren NotPetya). Dessa är ryska grupper som främjar ryska narrativ och utför attacker för att stödja Rysslands geopolitiska agenda. Många av dessa grupper misstänks ha nära band till den ryska regeringen (Truesec, 2023). Det är som tidigare nämnts svårt att attribuera attacker, och än svårare att diskutera i vilken mån dessa attacker är spontana angrepp av enskilda grupper eller attacker utförda av betalda ombud.

vågorna åsamkade enligt uppgift inte heller några allvarligare skador men det finns ett tydligt mönster som visar att cyberattackerna följer på den politiska utvecklingen.[29] Exempelvis riktades en våg av överbelastningsattacker mot det estniska parlamentet direkt efter fördömandet av den ryska fullskaliga invasionen 2022 (RIA 2023).

Estland genomförde en rad åtgärder för att stärka motståndskraften inom civilsamhället direkt efter invasionen av Ukraina. Bland annat assisterade regeringen 100 av de viktigaste websidorna att uppdatera sina cybersäkerhetsverktyg, vilket troligtvis bidrog till att mildra effekterna av överbelastningsattackerna som riktades mot landet (IISS 2023). Rysslands anfallskrig mot Ukraina har tydliggjort vikten av ett starkt cyberförsvar.

3.4.2.2 Påverkan

Utöver cyberangrepp finns givetvis även andra sätt för motståndaren att utnyttja cyberdomänen. Vad gäller den estniska informationsmiljön och påverkan, är detta ett problem som den estniska staten är väl medveten om. De baltiska länderna har starka historiska och etniska band till forna Sovjetunionen och det finns ett stort antal rysktalande minoritetsgrupper i dessa länder, vilket kan göra landet extra sårbart för ryska påverkanskampanjer (MKM 2019). I Estland talar 39 procent av befolkningen ryska (*Statistics Estonia* 2021), vilket möjliggör för ryska medier att påverka delar av befolkningen. Analyser av budskapen visar bland annat hur rysk TV sprider narrativ om att Europa övergivits av sina amerikanska allierade, och att den estniska ekonomin och sociala system är i kollaps (se bland annat Denisa-Liepniece 2017).

Omedelbart efter den ryska invasionen av Ukraina uppdaterade Estland sitt nationella säkerhetskoncept, och i samband med detta ökade man finansieringen med särskilt fokus på civilsamhällets uppdrag att bemöta ryska politiska påverkanskampanjer och desinformation (IISS 2023).

Det kan också diskuteras huruvida 2007 års cyberattacker skulle kunna anses vara en typ av påverkansoperation. Det är inte en fråga som besvaras i denna rapport, men det är värt att notera att gränsen mellan cyberkrigföring och påverkansoperation är otydlig, och de går ofta hand i hand.

3.5 Sammanfattning

Estlands cybersäkerhetsstruktur baseras på de styrdokument som tagits fram som ett helhetsgrepp av cyberdomänen. Både struktur och strategi står sig väl i jämförelse med andra länder, och är föremål för kontinuerlig utvärdering och uppdatering för att upprätthålla en hög nivå. Flera cyberincidenter har ökat Estlands profil inom cybersäkerhet och understrukit behovet av motståndskraft. En av de mest

29 För en djupare diskussion kring detta ämne, se Lilly, B. (2022). Russian Information Warfare: Assault on Democracies in the Cyber Wild West. Naval Institute Press.

betydande händelserna var cyberattacken 2007, som riktade sig mot olika estniska institutioner, vilket ledde till utvecklingen av landets första nationella cybersäkerhetsstrategi. Angreppen ledde till att Estland var tidigt ute med ett omfattande cybersäkerhetsarbete, men innebar också att det fanns en samhällelig förankring. Esterna fick en tydlig bild av följderna av ett bristande cyberförsvar och angreppen skapade en höjd medvetenhet och gav legitimitet till de åtgärder som genomfördes i efterdyningarna av angreppen.

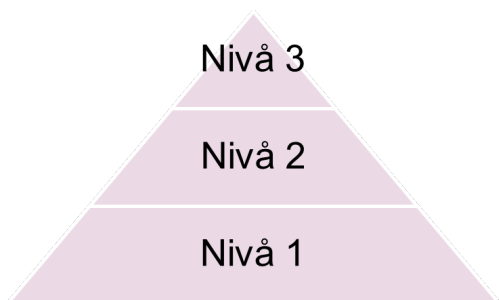
4. Cybersäkerhet och cyberförsvar i Estland

I DETTA KAPITEL DISKUTERAS de frågeställningar som ligger till grund för studien med stöd av Sternudds modell för cyberförsvar och *whole-of-nation*-strategin. Här identifieras också de lärdomar om vad som utgör samhällelig motståndskraft mot cyberhot och cyberangrepp. Vidare diskuteras vilka av dessa lärdomar som kan utgöra inspiration för Sverige. Detta kapitel bygger delvis på de intervjuer som hållits inom ramen för rapporten. Intervjuerna redovisas i bilaga 2.

4.1 Vad utgör samhällig mostståndskraft mot cyberhot och cyberangrepp i Estland?

För ett motståndskraftigt samhälle mot cyberhot och cyberangrepp kan tre punkter särskilt lyftas fram från litteraturen och intervjumaterialet:

- Vikten av en säkerhetskultur och en medvetenhet hos alla it-användare.
- Tydliga strategier för arbetet med information- och cybersäkerhet som kontinuerligt prioriteras, finansieras, implementeras och uppdateras.
- Ett välorganiserat cyberförsvar, vilket inkluderar struktur för informationsdelning och metod för förvarning inom cyberdomänen.



Figur 4.1 Förenkling av Sternudds cyberförsvarspyramid

Sternudds cyberförvarspyramid har förenklats till tre nivåer för att motsvara dessa tre punkter. Den grundläggande nivån är säkerhetsmedvetenheten och säkerhetskulturen hos samhällets it-användare, den andra nivån inkluderar information- och cybersäkerhet och den översta nivån är de offensiva och defensiva cyberoperationerna (cyberförsvar).

Nivå 1. Höjd säkerhetsmedvetenhet och säkerhetskultur

För ett motståndskraftigt samhälle behöver det finnas en säkerhetsmedvetenhet och säkerhetskultur hos alla it-användare i samhället och för att upprätthålla samt öka säkerhetsmedvetenheten behövs utbildningsinsatser, på alla nivåer i samhället. Enligt Sternudds modell så utgörs detta av den breda basen eller bottenplattan för cyberpyramiden (nivå 1). I intervjuerna framkommer *whole-of-nation* som en strategi för att förankra en säkerhetskultur hos it-användarna i samhället och som upprätthålls av RIA. Att involvera civilsamhället i cybersäkerhetsinsatser lyfts även fram i Klimburgs principer för *whole-of-nation* (se bilaga 5 för en sammanställning av Klimburgs principer applicerat på Estland). Att involvera civilsamhället innebär enligt detta antagande att medvetenheten hos it-användare ökar samt att den digitala kompetensen främjas, vilket i sin tur uppmuntrar proaktivt deltagande i att säkra cybermiljön. Att bygga motståndskraft mot cyberangrepp och cyberhot som har en bred samhällsförankring innebär enligt en respondent att tröskeln för en angripare höjs samtidigt som att konsekvenserna (skadan) vid genomförda angrepp minskar.

Det innebär samtidigt en viss förskjutning från ett statligt ansvar till att medborgarna är delaktiga för samhällets säkerhetskultur. I de intervjuer och de underlag som ligger till grund för denna rapport har medborgarnas engagemang och mobilisering inom cyberförsvaret presenterats som positiv; en central funktion i motståndskraften mot cyberhot och angrepp. Det finns dock röster som menar på att det är omdömeslöst att lägga ansvaret för cybersäkerhet på individen. De menar att om en individ inte hanterar eller skyddar sina egna internetanslutna enheter på ett korrekt sätt kan den resulterande attacken leda till en slags smittspridning, vilket påverkar samhället i stort (Renaud m.fl. 2018). De likställer denna typ av smittspridning med en biologisk smitta, där det är accepterat och förväntat att staten tar ansvar för att hantera den.

Detta resonemang grundas i så kallad *responsibilisation theory,* som framarbetas av den brittiske kriminologen David Garland (1996). Garland beskrev på nittiotalet hur staten övergick från att ha ett primärt ansvar för att hantera brott och säkerhet till att delegera dessa uppgifter till individer och samhällsgrupper. Kärnan i denna teori ligger i att ansvaret för att förebygga brott och skydda sig mot brottslighet inte längre enbart vilar på statliga institutioner utan delas med och läggs på individer, företag och samhällsorganisationer. Medborgarna förväntas ta en mer aktiv roll i sitt eget skydd och säkerhet, vilket kan inkludera allt från grannsamverkan till användning av säkerhetssystem och egenförsvar.

Detta fenomen innebär en förskjutning av ansvaret från staten till individen, under antagandet att detta ger medborgarna den självständighet och det inflytande som de har rätt till (Wakefield & Fleming 2008). Inom ramen för detta projekt konstateras endast att samhällsengagemanget lyfts fram som positivt utan fördjupade analys av dess konsekvenser eller effektivitet.

Nivå 2: Prioritera information- och cybersäkerhet

Estland har en tydlig nationell cyberdoktrin med sammanhängande strategier och policydokument som tillsammans verkar för säkra och robusta informationssystem, vilket även är en av Klimburgs principer för *whole-of-nation*-ansatsen. Estland tog tidigt (2008) fram en nationell cybersäkerhetsstrategi efter cyberangreppen 2007.

Motståndskraft mot cyberhot och cyberangrepp kräver även en internationell samverkan eftersom cyberoperationer ofta sker över nationella gränser och därmed kräver samarbete mellan stater och internationella institutioner (Osula 2022). Enligt Klimburgs principer för *whole-of-nation*-ansatsen lyfts även det internationella samarbetet som central, vilket inkluderar diplomatiska insatser, deltagande i internationella cybsersäkerhetsforum och samarbete om gränsöverskridande initiativ och informationsdelning. Cyberdiplomati är därför en viktig del av Estlands cyberprioriteringar. Landet har visserligen prioriterat att utveckla intern spetskompetens inom cybersäkerhet, men att detta har skett i kombination med målet att ”utveckla starka allianser och spela en fullvärdig roll i diplomatiska cyberforum” (IISS 2024: 31). Estland har länge haft ett internationellt engagemang, vilket återspeglas i landets intensiva deltagande i Nato, FN och EU. *NATO Cooperative Cyber Defence Centre of Excellence* (CCDCOE) är ett exempel på Estlands internationella engagemang då Estland är ramverksnation för CCDCOE, belägget i Tallinn. CCDCOE bildades efter de omfattande cyberangreppen mot Estland 2007. Syftet var att utveckla medlemmarnas förmåga inom cyberförsvarsområdet.

I intervjun med RIA framkommer det att även om Estlands cybersäkerhetsarbete har varit en prioriterad fråga så krävs det fortsatt prioritering, att det finns resurser, både ekonomiska och mänskliga för att genomföra, upprätthålla och utveckla det strategiska säkerhetsarbetet. Respondenterna menar att även om landet har lärt sig från tidigare erfarenheter så utgör den säkerhetspolitiska utvecklingen att Estlands cybersäkerhetsstrategi måste vara flexibel och uppdateras regelbundet för att vara effektiv.

Nivå 3: Välorganiserat cyberförsvar

I toppen av cyberförsvarspyramid återfinns cyberförsvar och dess offensiva och defensiva cyberoperationer. Enligt Klimburgs principer för *whole-of-nation* är cyberförsvar beroende av att hotinformation delas mellan aktörer. Effektiv informationsdelning bidrar till situationsmedvetenheten och möjliggör i sin tur proaktiva åtgärder mot framväxande hot. Information i form av underrättelse, signalspaning, incidentrapportering och teknisk information, som enligt Sternudds modell flödar genom cyberförsvarspyramiden från bottenplattan mot toppen av cyberförsvarspyramiden, behöver samordnas. Vid intervjuerna med cyberexperterna lyfts de överlappande nätverken som centrala för att dela information, framför allt när brister i rapporteringsstrukturer riskerar att situationsförståelsen för cyberhot och cyberangrepp begränsas.

Klimburgs principer for *whole-of-nation* lyfter även behovet av ett offentlig-privat partnerskap eftersom många av de sensorer för att upptäcka anomalier, som tidigare fanns inom det offentliga idag återfinns hos aktörer i näringslivet (Severin 2018). Det finns således ett behov av att civila aktörer delger information för att bidra till civil-militära cyberlägesbilder, för vilket det krävs en fördjupad samverkan mellan olika aktörer (Sternudd 2023; Severin 2018). Information om hur detta samarbete ser ut i Estland ryms inte inom ramen för denna studie. Det framgår dock i intervjuerna att den estniska CERTen har ett fått resurser för att ha fler sensorer inom den kritiska infrastrukturen, men att det måste vara frivilligt och att det måste finnas en företroenderelation mellan aktörerna.

Rysslands invasion av Ukraina har, enligt RIA, inneburit att Estland utsatts för en ökad aktivitet av cyberangrepp från pro-ryska grupper. Det försämrade säkerhetspolitiska läget innebär att en förskjutning till ett risk- och sårbarhetsfokuserat perspektiv på nationens egna sårbarheter behöver balanseras med bevakning av hotaktörers beteenden. Därför höjs röster som menar att förvarning för cyberhot behöver följa den säkerhetspolitiska utvecklingen där analys av underrättelser från en bredd av källor är viktig för att effektivt kunna bemöta antagonistiska cyberangrepp (Gentry 2022; Lilly m.fl. 2019). Det strategiska arbetet behöver med andra ord vara både proaktivt och reaktivt på hotsignaler.

Den klassiska försvarningsmetoden *Indications and Warning* (I&W) lyfts fram i litteraturen som en metod som går att anpassa till utmaningar inom cyberområdet (Gentry 2022; Healey & van Bochoven 2012; INSA 2018; Lily m.fl. 2019). En I&W-anpassad metod innebär att indikatorer identifieras för att bevaka det som är observerbart, och för fenomen som inte är direkt observerbara baseras analyserna på hot-scenarier (Healey & van Bochoven 2012; Lilly m.fl. 2019).

Det defensiva försvaret inkluderar behovet av cyberexperter som kan stötta kritisk infrastruktur och företag under pågående cyberangrepp. I intervjuerna lyfts Cyber Defence Unit som en väl fungerande funktion för att stötta utsatt verksamhet under cyberangrepp. Det framkommer även i intervju med respondenten från

CDFCS Taltech att det finns behov av cybersoldater som kan agera både defensivt och offensivt. Enligt respondenterna vid intervjun med NATO Cooperative Cyber Defence Center of Excellence lyfts deras övningsverksamhet som central för att utbilda exempelvis penetrationstestare, experter på situationsmedvetenhet och experter på digital kriminalteknik, vilket inkluderar cyberkinetiska operationer.

4.2 Vilka lärdomar från Estlands arbete inom cyberområdet kan utgöra inspiration för Sverige?

Det finns aspekter av det estniska cybersäkerhetsarbetet som kan utgöra inspiration för dess svenska motsvarigheter. Vissa estniska fenomen kan vara svåra att imitera eller skapa, såsom täta nätverk mellan en mindre grupp experter eller den cybersäkerhetsmedvetenheten som skapades i samhället till följd av cyberattackerna 2007. Informella strukturer behöver växa fram organiskt och upplevda erfarenheter från en kris kan inte helt ersättas av åtgärder såsom utbildning och kommunikationsinitiativ. Det finns dock flera likheter mellan Estland och Sverige som kan utgöra inspiration för det svenska arbetet inom cyberområdet.

4.2.1 Militär-civil samverkan

Estlands cyberhemvärn *Cyber Defence Unit* utgör en möjlighet att mobilisera frivilliga att hjälpa till och avlasta ordinarie personal vid långvariga cyberattacker. Det pågår en debatt i Sverige om behovet och funktionen av en svensk motsvarighet. Det finns idag en väletablerad struktur för frivilliga försvarsorganisationer i Sverige, men bara ett Hemvärn. Organisationer med specialistkompetens som radiokommunikation organiseras som just frivilliga försvarsorganisationer. Ett exempel på denna utveckling är att Frivilliga radioorganisationen, FRO har blivit utpekad som samordnare för frivilliga cybersäkerhetsspecialister.[30] Den förordning som reglerar dessa försvarsorganisationer innebär att myndigheter som ska bistå totalförsvaret kan teckna avtal med frivilliga cybersäkerhetsspecialister, vilket öppnar upp möjligheten att krigsplacera individer i myndighetens krigsorganisation. En krigsplacering innebär inte att befintlig personal ersätts, men att individen kan fungera som ett stöd vid särskilda händelser (Sternudd 2023).

Fördelar som lyfts fram är dels den centrala funktion som utbildningsverksamheten har i de frivilliga försvarsorganisationer och dels att de utgör ett informellt kompetensnätverk för informationsutbyte. FROs medlemmar kan således stödja varandra i den utsträckning som arbetsgivaren och lagens krav tillåter med hänvisning

30 Läs mer om detta här: *https://www.fro.se/web/cybersakerhet/*

till att sekretess och bevarandet av företagshemligheter måste uppfyllas (ibid). Vad gäller estniska CDU lyftes i intervjun, med respondenten från CDFCS Taltech, just det faktum att medlemmarna kommer från en bredare bakgrund som en fördel; de för med sig ett större nätverk in i cyberförsvaret.

Att bygga upp en frivilligorganisation är enligt respondenten från eGA något som behöver vara en politisk prioritering, eftersom det tar både tid och resurser i anspråk.

4.2.2 Utbildnings- och informationsinsatser

Estland valde tidigt en väg in i digitaliseringen, där landet prioriterade utbildning av lärare och sedan studenter för att få fram en generation av digitaliserade medborgare. RIA har ett brett uppdrag som innebär att säkerställa en långsiktig planering för digital förvaltning och cybersäkerhet. Målsättningen är enligt RIAs hemsida att bygga den ”bästa digitala staten, som skapar nya möjligheter för människor och samhälle”[31]. Det är, enligt respondenten från eGA, RIA som håller samman Estlands *whole-of-nation*-mentalitet.

I Estland inkluderas cybersäkerhet och cyberförsvar som en del av utbildningen i skolan. Även i Sverige har regeringen, enligt ett pressmeddelande från utbildningsdepartementet, beslutat om nya ämnesplaner som ska inkludera Nato- och totalförsvarskunskap i gymnasieskolan från och med 2025 (Regeringskansliet 2023). Detta skulle potentiellt kunna skapa ett större engagemang bland alla it-användare, på samma sätt som Estland sökt höja it-kunskapen bland skolelever genom sitt *Tiigrihüpe*-program (se sida 29).

4.2.3 Informationsdelning och nätverk

Behovet av kunskap och information för att skapa situationsförståelse för hotbilden är en viktig del av samverkan. Försvarsmakten beskriver i Perspektivstudien[32] (Försvarsmakten, 2022a) behovet av förbättrade lägesbilder och förstärkt förmåga till förvarning om cyberangrepp för att bemöta just de hot som uppstår i gråzonen.[33] I

31 Se RIAs hemsida för mer information: *https://www.ria.ee/en/authority-news-and-contact/authority-and-management/ria-strategy*

32 Perspektivstudien är Försvarsmaktens återkommande regeringsuppdrag som omfattar analtsarbete och förslag som ligger till grund för Försvarsmaktens underlag för fortsatta politiska ställningstagande. Se Försvarsmaktens hemsida: *https://www.forsvarsmakten.se/sv/aktuellt/2022/12/ryssland-fortsatt-storsta-hotet-enligt-forsvarsmaktens-framtidsstudie/*

33 ”Under gråzonen kan en antagonist använda sig av flera olika maktmedel. Exempel på sådana är desinformationskampanjer, cyberoperationer, strategiska uppköp, propaganda, illegal underrättelseinhämtning och sabotage.” Jonsson, D.K, Eriksson, C., Ingemarsdotter, J., Rossbach, N.H., Wedebrand, C. (2023). Gråzonslägen i krig och fred. FOI-R--5447--SE. Mer om just gråzonsproblematik finns att läsa om i flera FOI-rapporter.

Riksrevisionens (2023) granskning av informations- och cybersäkerhet lyfts avsaknaden av en gemensam lägesbild inom cybersfären som en nyckelfråga. Myndigheterna tillhandahåller flera olika lägesbilder, vilket leder till en fragmenterad bild av området som i sin tur begränsar informationsunderlaget för beslut om åtgärder (ibid).

En av de slutsatser som lyftes i Severins (2018:35) rapport var just att det krävs en ”fördjupad samverkan och utökat informationsutbyte mellan underrättelse- och säkerhetstjänster å ena sidan och aktörer som inte har rikets säkerhet som sin kärnverksamhet å den andra”, vilket inkluderar en både statliga och icke-statliga aktörer och organisationer att kunna skapa civil-militära cyberlägesbilder. Behovet av bättre informationsdelning och samverkan lyfts även fram i Riksrevisionens (2023) granskning av regeringens styrning av samhällets informations och cybersäkerhet.

En del av samverkan innebär även att dela information i omvänt flöde, tillbaka till aktörer i samhället. 2023 gav den svenska regeringen Försvarets radioanstalt, MSB, Försvarsmakten och Säkerhetspolisen i uppdrag att utarbeta lägesbilder som riktar sig till aktörer inom näringslivet samt till statliga myndigheter, regioner och kommuner (Skr. 2023/24:26). Behovet av att delge information för att öka säkerhetsmedvetande på bred front i samhället är även en viktig slutsats från intervjuerna med de estniska cyberexperterna. Som den tidigare citerade SoU:n från 1953 betonar, är information och kunskap om hot grundläggande för samhällets motståndskraft (SOU 1953).

Det estniska förhållningssättet till detta problem är de överlappande sociala nätverk som kopplar ihop olika delar av cyberstrukturen. På frågan om hur man centraliserar den information som flödar i systemen för att skapa samlade lägesbilder framhöll respondenten från CDFCS Taltech att det är viktigare med överlappande nätverk där information delas, framför en mer formell delgivning av information till en central mottagare. Samtidigt framgår det i intervjuarna utmaningar med att information hålls i ”silos”. Utmaningar som kvarstår även om de överlappande nätverken underlättar för informationsdelning. Nätverksstrukturerna i Estland tycks möjliggöras genom att landet är en liten nation med korta avstånd till beslutsfattare, bokstavligen och bildligt.

Areng (2018) konstaterar i sin analys av små staters cybersäkerhetskapacitet att små stater i allmänhet har mycket att vinna på informationssamhällets framsteg. Hon lyfter att när det gäller styrning och byråkrati är det en fördel att ha korta kommunikationsförbindelser inom och mellan offentliga organ och drar slutsatsen att mindre politiskt avstånd mellan lokalt och nationellt styre leder till betydande självständighet i beslutsfattandet.[34] Detta innebär dock inte att fördelarna med nätverksstrukturerna i ett land som Estland är direkt överförbara till andra länder.

34 Diskussioner kring små staters cyberkapacitet har diskuterats i flera studier, där man tittat på hur cyberförsvar ser ut i stater såsom Estland (Crandall & Allan 2015), men även Nya Zeeland (Burton 2013), och Singapore (Tan 2019).

4.2.4 Transparens och öppenhet

En annan intressant reflektion är i vilken utsträckning som cyberförsvaret ska sträcka sig i förhållande till åtgärder? Estlands utsatthet för påverkanskampanjer har lett fram till beslut om att belägga vissa nyhetssajter med förbud efter att de har bedömts sprida rysk information. Det kan diskuteras om statlig censur av medier, även om de identifierade medierna sprider desinformation, kan skapa farliga precedensfall och leda till en urholkning av yttrande- och pressfrihet som är en grundläggande rättighet och viktig i det demokratiska samhället. Ett argument är att Estland, genom att censurera nyhetssajter, hindrat möjligheten till öppen debatt och diskussion kring kontroversiella frågor. Internationella organisationer som bevakar pressfrihet, såsom Reportrar utan gränser och *Human Rights Watch*, har uttryckt oro över att sådana åtgärder kan användas för att legitimera liknande inskränkningar i andra länder, inklusive auktoritära stater.[35]

Det finns även frågor kring effektiviteten av sådana förbud, då de inte nödvändigtvis stoppar informationsflödet utan potentiellt enbart omdirigerar det.[36] Det vore inte orimligt att dra paralleller till utvecklingen då EU 2022 förbjöd de statligt kontrollerade ryska medierna RT och Sputnik från att sända i unionen. Ryssland svarade med att i sin tur förbjuda europeiska journalister från att verka i landet, vilket minskade västvärldens insyn i Ryssland (Kudo 2022). Även om det finns stöd för Estlands beslut, särskilt i ljuset av den ryska desinformationskampanjen och pågående spänningar i regionen, är det tydligt att frågan om att balansera säkerhet och frihet är komplex och omstridd. Med detta sagt, så ligger Estland högt i flera undersökningar över pressfrihet.[37] Denna diskussion är viktig även för Sverige att delta i.

35 I en studie som tagits fram av Reportrar utan gränser (RSF) och Balticada Investigations Studio konstateras att informationsfriheten i Estland, Lettland och Litauen lider av anmärkningsvärda brister trots ländernas höga rankning i pressfrihetsindex. Se *https://www.reportrarutangranser.se/anmarkningsvarda-brister-i-baltlandernas-pressfrihet/*

36 Kritiken liknar den som riktas mot den brottsförebyggande ansatsen ”situational crime prevention” som fokuserar på att identifiera och implementera strategier som minskar möjligheterna till brott genom att förändra de omedelbara omständigheterna och miljöerna där brott kan uppstå. I kritiken diskuteras fenomenet “displacement”, vilket innebär att brott inte förhindras utan snarare flyttas till en annan tid, plats eller form. Läs mer om dessa teorier i Oxford Research Encyclopedias *https://oxfordre.com/criminology/display/10.1093/acrefore/9780190264079.001.0001/acrefore-9780190264079-e-3*

37 Se exempelvis: *https://freedomhouse.org/country/estonia/freedom-net/2020*

5. Sammanfattande reflektion

Estland har genom *whole-of-nation*-strategin inom cyberdomänen sökt skapa en enhetlig och koordinerad ansats som utnyttjar hela samhällets styrkor och resurser för att skydda samhället mot cyberhot. Ett robust försvar behöver vara både reaktivt och proaktivt. Cybersäkerhet och cyberförsvar är begrepp som ofta flätas samman och gränserna förblir otydliga. Men i och med att cyberangrepp från statliga aktörer eller statsunderstödda grupper kan användas som militärt maktmedel i en upptappningssituation inför en väpnad konflikt eller som hybridaktiviteter knyts cyberförsvar närmare det nationella försvaret, vilket inkluderar både offensivt och defensivt försvar mot cyberhot och cyberangrepp.[38]

> Ett robust cyberförsvar innebär att information- och cybersäkerhet är väl förankrat i samhällskroppen. För att uppnå effektiv informationsdelning behöver samverkan mellan underrättelsetjänster, säkerhetstjänster och en bredare krets samhällsaktörer fördjupas (Sternudd 2023; Severin 2018). Det är svårt att bedöma hur väl detta genomförs i Estland, men det är desto lättare att konstatera att det är ett område som ständigt behöver uppdatering och utveckling.

Ytterligare en viktig poäng som lyftes både i våra intervjuer och i litteraturen är att hur väl ett land än arbetar med att föra information via nätverk eller kanaler, behöver det finnas en mottagare för informationen som har mandat att agera snabbt. Det framgår i intervjuerna med RIA att resurser har tilldelats för att ha fler sensorer inom den kritiska infrastrukturen, men samtidigt var våra respondenter noga med att understryka att en stor del av samverkan bygger idag på aktörernas frivilliga deltagande, och att det krävs en stark förtroenderelation mellan aktörerna. Givet det vi har sett, kan det vara värt att titta vidare på RIAs roll och funktion, utbildnings- och informationsinsatser samt informationsinhämtning inom cyberområdet.

I det budgetförslag som lades fram av den svenska regeringen i september 2024, föreslogs en stor satsning på namngivna aktörer för att öka cybersäkerheten för att ge ett ”mer effektivt stöd till samhällsaktörer för att förebygga, motstå och hantera cyberincidenter”.[39] I Estland är det RIA och CERT-EE som står för dessa funktioner, och en större studie som ser närmare på några av de frågor som identifierats

38 Med hybridhot eller hybridaktiviter menas att både militära och icke-militära medel kan användas i en gråzonssituation. Se: *https://fra.se/underrattelser/hybridhot.4.55af049f184e92956c42d27.html*

39 Pressmeddelande från Regeringskansliet. Se: *https://www.regeringen.se/pressmeddelanden/2024/09/historisk-satsning-pa-cybersakerhet/*

i denna rapport skulle därför vara av värde. RIA:s roll i Estlands cyberförsvar uppmärksammades dessutom i Försvarsberedningens totalförsvarsapport Kraftsamling (2023) som en särskilt intressant aktör att analysera mot bakgrund av övervägandet av att överföra ansvaret för cyber- och informationssäkerhet till FRA/NCSC och skulle därmed kunna bidra med inspiration kring hur en omstrukturering skulle ske.

Hur effektiva är de nuvarande utbildnings- och informationsinsatserna inom cybersäkerhet i Sverige när det gäller att öka medvetenheten och kompetensen bland både offentliga och privata aktörer, och vilka förbättringar kan göras för att maximera deras inverkan? Denna fråga syftar till att utvärdera hur väl nuvarande utbildningsprogram och informationskampanjer uppfyller sina mål, såsom att höja cybersäkerhetsmedvetenheten, förbättra kunskaper och färdigheter, och förebygga cyberhot. Andra frågor som behöver besvaras är vilka aktörer som står bakom de olika utbildningskampanjerna, om de når rätt målgrupp, och vad ”rätt” målgrupp är.

I och med införandet av NIS2-direktivet har Sverige och Estland, som medlemsländer i EU, fått nya uppgifter och ramar. Direktivet betonar bland annat vikten av samarbete mellan privata och offentliga aktörer. Informationsdelning om hot och sårbarheter ska främjas, och mekanismer för detta ska etableras. Hur påverkar det här ländernas förmå till informationsinhämtning? NIS2 ställer högre krav på incidentrapportering än tidigare, och vi har i denna rapport nämnt vikten av just sådan rapportering i informationsinhämtningsprocessen. Hur påverkar direktivet informationsinhämtning och – delning inom cyberförsvaret? Vilka utmaningar uppstår? Vilka möjligheter? Skiljer sig dessa åt mellan Sverige och Estland?

Referenser

Agrell, W. (2011). *Förvarning och samhällshot.* Studentlitteratur: Lund.

Agrell, W. (2022). *Vi såg det inte komma.* Studentlitteratur: Lund.

Areng, L. (2014). *Lilliputian states in digital affairs and cyber security*. The NATO Cooperative Cyber Defense Centre of Excellence Archive, Tallinn Paper Series, 4.

Atna-Dvořák, A., Lips, S., Tsap, V., Ottis, R., Priisalu, J., Draheim, D. (2021). *Vulnerability of State-Provided Electronic Identification: The Case of ROCA in Estonia*. In: Kö, A., Francesconi, E., Kotsis, G., Tjoa, A.M., Khalil, I. (eds) Electronic Government and the Information Systems Perspective. EGOVIS 2021. Lecture Notes in Computer Science, vol 12926. Springer, Cham.

Balcer Bednarska, J. (2024). 120 myndigheter drabbade av it-attack – tiotusentals anställda påverkade. *Sveriges Television.* 25 januari. URL: *https://www.svt.se/nyheter/inrikes/120-myndigheter-drabbade-av-it-attack-tiotusentals-anstallda* (Åtkomstdatum: 14 mars 2024).

Baltic Times. (2022). "Estonian Cyber Security Council discusses strengthening of cyber defense in context of war". *Baltic Times*, 25 mars, URL: *https://www.baltictimes.com/estonian_cyber_security_council_discusses_strengthening_of_cyber_defense_in_context_of_war/* (Åtkomstdatum: 25 juli 2024).

Bartoszewicz, M. G., & Prucková, M. (2024). Enemy image? A comparative analysis of the Russian federation's role and position in the leading national security documents of Estonia and the Czech Republic. *Journal of Contemporary European Studies*, 32(1), s. 215-227.

Belfer Centre, *Cyber Power Index* (2022) URL: *https://www.belfercenter.org/publication/national-cyber-power-index-2022* (Åtkomstdatum 23 juli 2024).

Brewer, R. (2016). Ransomware attacks: detection, prevention and cure. *Network security*, 2016(9): s. 5-9.

Burton, J. (2013). Small states and cyber security. *Political Science*, 65(2): s. 216-238.

Buzan, B., Wæver, O. & De Wilde, J. *Security: A new framework for analysis.* Lynne Rienner Publishers, 1998

Cardash, S., Cilluffo, F. & Ottis, R. (2013). Estonia's Cyber Defence League: A Model for the United States? *Studies in Conflict & Terrorism* 36(9): s. 777-787.

Çifci, H., 2022. Comparison of National-Level Cybersecurity and Cyber Power Indices: A Conceptual Framework (*preprint, not peer reviewed*).

Crandall, M. & Allan, C. (2015). Small States and Big Ideas: Estonia's Battle for Cybersecurity Norms. *Contemporary Security Policy*, 36(2): s. 346-368.

De la Reguera, E. (2024). Frankrike angrips av rysk grupp som attackerade Sverige: "Kriget följder i vår vardag". *Dagens Nyheter*, 24 mars. URL: *https://www.dn.se/varlden/frankrike-angrips-av-rysk-grupp-som-attackerade-sverige-krigets-foljder-i-var-vardag/* (Åtkomstdatum: 24 mars 2024)

Denisa-Liepniece, S. (2017). A case of Euroscepticism: Russian speakers in Latvian and Estonian politics. I Austers, A. & Bukovskis, K. (red.). *Euroscepticism in the Baltic States: Uncovering Issues, People, and Stereotypes*. Latvian Institute of International Affairs, s: 69-87.

Doyle, B. (2019). The Whole-of-Nation and Whole-of-Government Approaches in Action. *InterAgency Journal*, 10, 105-122

Ds 2023:34. *Kraftsamling - Inriktningen av totalförsvaret och utformningen av det civila försvaret.*

E-Estonia (2017). *Data Embassy*. URL: https://e-estonia.com/wp-content/uploads/factsheet_data_embassy.pdf (Åtkomst 19 juli 2024).

eGA: *National Cyber Security Index* (2024). URL: *https://ncsi.eGA.ee/* (Åtkomstdatum: 23 juli 2024).

Eidenskog, D., Eckersand, U. & Mittenmaier, E. (2023). *Digitaliseringens risker i hälso- och sjukvård*. FOI. FOI-R--5367--SE.

Enisa (2017). ENISA overview of cybersecurity and related terminology. URL: *https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology* (Åtkomstdatum 24 juli 2024).

Enisa (2020a). *Enisa Threat Landscape – Cyber espionage*. URL: *https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends/enisa-threat-landscape/enisa-threat-landscape-2020* (Åtkomstdatum: 1 november 2023).

Enisa (2020b). *Threat Landscape 2020 – Malware.* URL: *https://www.enisa.europa.eu/publications/malware* (Åtkomstdatum: 6 december 2023).

Enisa (2022). *Threat Landscape For Ransomware Attacks.* URL: *https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-ransomware-attacks* (Åtkomstdatum: 6 december 2023).

EU-kommissionen (2022). *Digital Economic and Society Index (DESI) 2022 – Estonia*'.URL: *https://ec.europa.eu/newsroom/dae/redirection/document/88701* (Åtkomstdatum: 25 juli 2024).

EU-kommissionen (2018). *Action Plan against Disinformation*. URL: *https://www.eeas.europa.eu/sites/default/files/action_plan_against_disinformation.pdf* (Åtkomstdatum: 6 december 2023).

Europol (2023a). *Europol Spotlight. Cyber-Attacks: The Apex of Crime-As-A-Service, IOCTA*. The Hague: European Cybercrime Centre, Europol. URL: *Cyber-attacks: the apex of crime-as-a-service (IOCTA 2023) | Europol (europa.eu)* (Åtkomstdatum: 7 december 2023).

Europol (2023b). *The Internet Organised Crime Threat Assessment, IOCTA*. The Hague: European Cybercrime Centre, Europol. URL: *https://www.europol.europa.eu/cms/sites/default/files/documents/IOCTA%202023%20-%20EN_0.pdf* (Åtkomstdatum: 6 december 2023).

Frisk, R. (2019). *Strategisk förvarning för väpnat angrepp – metodreflektioner*, FOI Memo 6636.

Fö 2024/00785. *Ett nytt Nationellt cybersäkerhetscenter.* Försvarsdepartementet. Stockholm 19 april 2024.

Försvarets Radioanstalt (2024). *Fler hot och större osäkerhet. FRA Årsrapport 2023.*

Försvarets Radioanstalt, Försvarsmakten, MSB, Polisen och Säkerhetspolisen (2020). *Cybersäkerhet i Sverige. Hot, metoder, brister och beroenden. URL: rapport-cybersakerhet-i-sverige-2020--hot-metoder-brister-och-beroenden.pdf* (Åtkomstdatum: 6 maj 2024).

Försvarsmakten och Försvarets Radioanstalt (2016). *Överenskommelse om gemensamma begrepp för Cyberområdet*, Bilaga 1 Till FM 2016-129 50

Försvarsmakten (2022a). *Slutredovisning Av Försvarsmaktens Perspektivstudie 2022: ett starkare försvar för en utmanande framtid.* URL: *https://www.forsvarsmakten.se/siteassets/2-om-forsvarsmakten/dokument/perspektivplan/perspektivstudie-2022-forsvarsmakten.pdf* (Åtkomstdatum: 15 november 2023).

Försvarsmakten (2022b). För ett vassare cyberförsvar. URL: *https://www.forsvarsmakten.se/sv/aktuellt/2022/03/for-ett-vassare-cyberforsvar/* (Åtkomstdatum: 25 mars 2024).

Garland, D. (1996) The Limits of the Sovereign State: Strategies of Crime Control in Contemporary Society. *British Journal of Criminology*. (36), s. 445–471.

Gentry, J. (2022). Cyber Intelligence: Strategic Warning Is Possible. *International Journal of Intelligence and CounterIntelligence* 36(3): s. 1–26.

Giles, K. (2016). *Handbook of Russian Information Warfare*. Research Division, NATO Defense College. URL: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/resources/docs/NDC%20fm_9.pdf (Åtkomstdatum: 20 november 2023).

Gold, J. (2019). Estonia as an international cybersecurity leader. E-Estonia.

Greenberg, A. (2018) The untold story of NotPetya. *Wired*. 22 augusti. URL: *https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/* (Åtkomstdatum: 20 augusti 2024).

Gustafsson, J. (2021). Estonia. I Hagström Frisell, E. & Pallin, K. (eds.). *Western Military Capability in Northern Europe 2020. Part II: National Capabilities.* FOI-R--5013--SE.

Healy, J & van Bochoven, L. (2012). *Strategic Cyber Early Warning: A Phased Adaptive Approach for NATO*. URL: *https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/strategic-cyber-early-warning-a-phased-adaptive-approach-for-nato/* (Åtkomstdatum 17 maj 2024).

Hsieh, C. W., Wang, M., Wong, N. W., & Ho, L. K. K. (2021). A whole-of-nation approach to COVID-19: Taiwan's National Epidemic Prevention Team. *International Political Science Review*, 42(3), 300-315.

Inkster, N. (2016). Information Warfare and the US Presidential Election. *Survival*, 58(5): s. 23-32.

INSA (2018). A framework for cyber indications and warning. Intelligence and National Security Alliance.

International Institute for Strategic Studies (2023) *Cyber Capabilities and National Power: A Net Assessment vol. 2.* URL: *https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2023/09/cyber-capabilities-and-national-power-vol-2/cyber-capabilities-and-national-power_volume-2.pdf* (Åtkomstdatum 25 juli 2024).

ITU (2021). *Global Cybersecurity Index 2021.* ITU Publications. URL: https://www.itu.int/pub/D-STR-GCI.01-2021 (Åtkomstdatum: 3 november 2023).

Jonsson, D., Eriksson, C., Ingemarsdotter, J., Rossbach, N. & Wedebrand, C. (2023). *Gråzonslägen i krig och fred*. FOI-R--5447--SE.

Jonsson, M. & Gustafsson, J. (2022). Espionage by Europeans 2010–2021 A Preliminary Review of Court Cases. FOI-R--5312--SE.

Kaitseministeerium (2023). *Estonia National Security Concept* URL: *https://kaitseministeerium.ee/sites/default/files/eesti_julgeolekupoliitika_alused_eng_22.02.2023.pdf* (Åtkomstdatum 19 juli 2024).

Karatzogianni, A. (2015). *Firebrand waves of digital activism 1994-2014: The rise and spread of hacktivism and cyberconflict*. Palgrave Macmillan London.

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

Klimburg, A. (2011). The whole of nation in cyberpower. *Georgetown Journal of International Affairs*, s. 171–179.

Kohler, K. (2020). *Estonia's National Cybersecurity and Cyberdefense Posture: Policy and Organizations*. ETH Zurich. URL: *https://www.research-collection.ethz.ch/handle/20.500.11850/438276* (Åtkomstdatum: 15 oktober, 2023).

Küchler, T. (2024). "Jag begår politiskt självmord – har inget val", *Svenska Dagbladet* (2024-03-22). URL: *https://www.svd.se/a/0QeqdE/estlands-kaja-kallas-jag-beGAr-politiskt-sjalvmord* (Åtkomstdatum: 25 mars 2024).

Künnapu, M. (u.a.) *Cyber Security in Estonia: A National Response in the New Risk Environment*. Ministry of Justice, Republic of Estonia. URL: *https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa06f#:~:text=A%20National%20Response%20in%20New%20Threat%20Environment.%20Markko* (Åtkomst: 7 oktober 2024).

Kudo, P. (2022). EU-förbud mot rysk tv kan leda till motåtgärd, *Svenska Dagbladet* (2022-03-01). URL: https://www.svd.se/a/G3grmm/forbud-mot-ryska-medier-kan-leda-till-motatgard (Åtkomst: 30 juli 2024).

Landgren, J. & Borglund, E. (2016). *Lägesbilder. Att skapa och analysera lägesbilder vid samhällsstörningar*. Myndigheten för samhällsskydd och beredskap, MSB. URL: *https://www.msb.se/sv/publikationer/lagesbilder--att-skapa-och-analysera-lagesbilder-vid-samhallsstorningar/* (Åtkomstdatum: 15 oktober 2023).

Light, M., Singh, A. M., & Gold, J. (2022). Private security and national security: The case of Estonia. *Theoretical criminology*, 26(4): s. 664-683.

Lilly, B., Ablon, L., Hodgson, Q. E., & Moore, A. S. (2019). Applying indications and warning frameworks to cyber incidents. I: *2019 11th international conference on cyber conflict (Cycon)*. URL: *https://www.rand.org/pubs/external_publications/EP68144.html* (Åtkomstdatum: 6 november 2023).

Lindskog, E., Huuva, L., Lethinen, S., & Shannon, D. (2022). *Polisanmälda dataintrångsbrott: Karaktär, utmaningar, utvecklingsområden*. Brå. Rapport 2022:8. URL: *https://bra.se/publikationer/arkiv/publikationer/2022-10-31-polisanmalda-dataintrang.html* (Åtkomstdatum: 10 oktober 2023).

Ministry of Education and Research (2014) *The Estonian Lifelong Learning Strategy, 2020.* URL: *https://planipolis.iiep.unesco.org/sites/default/files/ressources/estonia_lll-strategy-2020.pdf* (Åtkomstdatum 23 juli 2024).

MKM (2019). *Cyber Security Strategy 2019-2022*, Ministry of Economic Affairs and Communication, Republic of Estonia.

MKM (2021) *Digital Agenda 2030*, Ministry of Economic Affairs and Communication, Republic of Estonia. URL: *https://mkm.ee/en/e-state-and-connectivity/digital-agenda-2030* (Åtkomst: 20 september 2024).

Must (2024). Årsöversikt *2023*. Försvarsmakten. URL: *forsvarsmakten.se/siteassets/2-om-forsvarsmakten/dokument/musts-arsoversikter/must-arsoversikt-2023.pdf* (Åtkomstdatum: 24 februari 2024).

Myndigheten för samhällsskydd och beredskap, MSB (2021). *Hoten mot de digitala leveranskedjorna.* URL: *https://rib.msb.se/filer/pdf/29829.pdf* (Åtkomstdatum: 15 maj 2024).

Myndigheten för samhällsskydd och beredskap, MSB (2024a). *Cyberangrepp mot samhällsviktiga informationssystem. 25 rekommendationer för stärkt skydd mot cyberangrepp.* URL: *https://www.msb.se/sv/publikationer/cyberangrepp-mot-samhallsviktiga-informationssystem--25-rekommendationer-for-starkt-skydd-mot-cyberangrepp/* (Åtkomstdatum: 17 januari 2024).

Myndigheten för samhällsskydd och beredskap, MSB (2024b). *EU förändrar cybersäkerhetsområdet : årsrapport it-incidentrapportering 2023*". URL: *https://www.msb.se/sv/publikationer/eu-forandrar-cybersakerhetsomradet--arsrapport-it-incidentrapportering-2023/* (Åtkomstdatum: 20 september 2026).

Nilsson, P-E. (2023). *Unravelling the Myth of Cyberwar. Five Hytpotheses on Cyberwarefare in the Russ-Ukrainian War (2014-2023)*. FOI-R--5513--SE.

NIST Resource Centre, *Cyber Threat*. URL: *https://csrc.nist.gov/glossary/term/Cyber_Threat* (Åtkomstdatum: 23 juli 2024).

Odebade, A. T. & Benkhelifa, E. (2023). A Comparative Study of National Cyber Security Strategies of ten nations." *ArXiv* 2303:13938 .

Odell, A. Lioufas, A., Olsén, M., Mossberg Sonnek, K. och Welander, F. (2024). *Russian Attacks on the Ukrainian power system*. FOI-R--5596--SE.

Osula, A-M. (2022*). How do global engagements matter for national cyber resilience?* I Upgrading National Cyber Resilience. NCSI, National Cyber Security Index. E-Governance Academy, Estonia. URL: *https://eGA.ee/wp-content/uploads/2021/05/NCSI-Cyber-Resilience-Digi_F.pdf* (Åtkomstdatum: 9 oktober 2023).

Ottis, R. (2018). *Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare perspective*, CCDCOE, Tallinn. URL: *https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf* (Åtkomstdatum: 9 oktober 2023).

Oyetunde, B. (2023). *Estonia saw a record number of cyber attacks in 2022.* E-Estonia. URL: *https://e-estonia.com/in-2022-estonia-had-the-highest-number-of-cyber-attacks/* (Åtkomstdatum: 1 mars 2024).

Pala, A. & Zhuang, J. (2019). Information sharing in cybersecurity: A review. *Decision Analysis* 16(3): s. 172-196.

Petersson, O. (2023). *Motståndskraft*. Myndigheten för psykologiskt försvar. URL: *https://www.mpf.se/publikationer/publikationer/2022-03-01-motstandskraft* (Åtkomstdatum: 9 april 2024).

Prop. 2020/21: 31. *Totalförsvaret 2021-2024*. Stockholm, 14 oktober, 2020. URL: *https://data.riksdagen.se/fil/B7B561D3-E597-42D9-9CEA-0AE2C171AF44* (Åtkomstdatum: 17 maj 2024).

Regeringskansliet (2017). *Nationell säkerhetsstrategi*. Statsrådsberedningen.

Regeringskansliet (2023). *Nya ämnesplaner för gymnasieskolan med fokus på ämneskunskaper.* Utbildningsdepartementet. URL: *https://www.regeringen.se/pressmeddelanden/2023/12/nya-amnesplaner-for-gymnasieskolan-med-fokus-pa-amneskunskaper/* (Åtkomstdatum: 6 februari 2024).

Regeringskansliet (2024). *Detta är Nato.* URL: *https://www.regeringen.se/regeringens-politik/sverige-i-nato/detta-ar-nato/* (Åtkomstdatum: 6 februari 2024).

Renaud, K., Flowerday, S., Warkentin, M., Cockshott, P. och Orgeron, C., (2018). Is the responsibilization of the cyber security risk reasonable and judicious?. *Computers & Security* (78) s.198-211.

RIA (2023). *Digital Agenda 2030*, Republic of Estonia Information System Authority, Tallinn. URL: *https://mkm.ee/en/e-state-and-connectivity/digital-agenda-2030* (Åtkomstdatum 24 juli 2024).

RIA (2023). *Cyber Security In Estonia 2023*, Republic of Estonia Information System Authority, Tallinn. URL: *https://www.ria.ee/sites/default/files/documents/2023-02/Cyber-Security-in-Estonia-2023.pdf* (Åtkomstdatum: 10 oktober 2023).

Riksrevisionen (2023). *Regeringens styrning av samhällets informations- och cybersäkerhet* (RiR 2023:8).

Severin, M. (2018). *Tidig förvarning och icke-militära angreppssätt - Utmaningar för underrättelsetjänsten*. FOI-R--4577--SE.

Shafqat, N., & Masood, A. (2016). Comparative analysis of various national cyber security strategies. *International Journal of Computer Science and Information Security*, 14(1), s. 129-136.

Skr. 2023/24:26. *Riksrevisionens rapport om regeringens styrning av samhällets informations- och cybersäkerhet.* Stockholm 5 oktober 2023. URL: *Riksrevisionens rapport om regeringens styrning av samhällets informations- och cybersäkerhet* (Åtkomstdatum: 1 februari 2024).

SOU 1953:27. *Psykologiskt Försvar*.

Statistics Estonia (2021). *Population Census 2021*. URL: *https://www.regeringen.se/contentassets/cd23ea9b36fd4d59b990f7541023214d/riksrevisionens-rapport-om-regeringens-styrning-av-samhallets-informations--och-cybersakerhet-skr.-20232426.pdf* (Åtkomstdatum: 1 mars 2024).

Sternudd, P. (2023). *Cyberförsvar och cybersäkerhet*, Kungl Krigsvetenskapsakademin. URL: *https://kkrva.se/bookstore/produkt/sternudd-cyberforsvar/* (Åtkomstdatum: 1 mars 2024).

Štitilis, D., Pakutinskas, P., & Malinauskaitė, I. (2017). EU and NATO cybersecurity strategies and national cyber security strategies: a comparative analysis. *Security journal*, 30, s. 1151-1168.

Svahn, M., Jarlsbo, M., Michélsen Forsgren & M., Lindahl, D. (2024). *Delat ansvar är ingens ansvar? En analys av den svenska statsförvaltningens ansvara och styrning vad gäller svenskt informations- och cybersäkerhetsarbete.* FOI-R--5546—SE.

Säkerhetspolisen (2024). *Lägesbild 2023/2024*.

Säkerhetspolisen (2024). Säkerhetspolisens årsberättelse. URL:*https://www.sakerhetspolisen.se/om-sakerhetspolisen/publikationer/sakerhetspolisens-arsberattelse/sakerhetspolisen-2023-2024/sammanfattning.html* (Åtkomst: 20 september 2024).

Tan, E.E.G. (2019). A Small State Perspective on the Evolving Nature of Cyber Conflict: Lessons from Singapore, *PRISM*, 8(3): s. 158-171.

The Cyber Defence unit of the Estonian Defence League: Legal, Policy and Organisational Analysis, CDCOE. Tallinn. URL: *https://ccdcoe.org/uploads/2018/10/CDU_Analysis.pdf* (Åtkomstdatum: 25 mars 2024).

Thomas, M. A. (2022). Distinguishing Cyberattacks by Difficulty. *International Journal of Intelligence and CounterIntelligence*, *35*(4): s. 784-805.

Truesec (2023). *Anonymous Sudan: Threat Intelligence Report*. URL: *https://insights.truesec.com/hub/report/anonymous-sudan-threat-intelligence* (Åtkomstdatum: 9 oktober 2023).

Van Ooijen, M. (2020). *Cyber securitization or cyberization of conflict?–the militarization of Cyber Security in Estonia*. Master's Thesis, Utrecht University.

Wakefield, A. och Fleming, J. red., (2008). *The Sage dictionary of policing*. SAGE Publications Ltd.

Whaley, B. (2007). *The Prevalence of Guile: Deception through Time and across Cultures and Disciplines*, i Foreign Denial & Deception Committee, National Intelligence Council, Office of the Director of National Intelligence, Washington, 1-101.

WHO (2022). *COVID-19 Strategic Preparedness and Response Plan Operational Planning Guideline* URL: *https://www.who.int/publications/m/item/covid-19-strategic-preparedness-and-response-plan-operational-planning-guideline* (Åtkomstdatum 24 juli 2024).

Zegart, A. (2022). *Spies, Lies, and Algorithms: The History and Future of American Intelligence*, Princeton, NJ: Princeton University Press.

Zibak, A. & Simpson, A. (2019). *Cyber Threat Information Sharing: Perceived Benefits and Barriers, ARES '19: Proceedings of the 14th International Conference on Availability, Reliability and Security*, s. 1–9.

Zouave, E. (2020). *De svenska definitionerna inom aktivt cyberförsvar*, FOI-D--0981--SE.

Zrahia, A. (2014). A multidisciplinary analysis of cyber information sharing. *Military and Strategic Affairs*, 6(3): s. 59-77.

Ödlund, A. (2018). *Informationsdelning och lägesbild*, FOI MEMO 6588.

Bilaga 1. Respondenter

Våra intervjurespondenter representerar följande organisationer:

RIA är Estlands centrala myndighet för övervakning och hantering av cyberhot. De ansvarar för att övervaka cybersäkerhetsläget i landet, utfärda varningar om hot och ge råd om säkerhetsåtgärder. Organisationen arbetar brett med cybersäkerhetsmedvetenhet och informationsinsatser. Ur ett operativt perspektiv har RIA har två huvudsakliga grenar: cybersäkerhet och informationssystem. Den förstnämnda övervakar den nationella incidenthanteringsgruppen CERT-EE, som spelar en nyckelroll i skyddet av kritisk infrastruktur och har omfattande tillsynsbefogenheter över nationella och lokala myndigheters informationssystem, leverantörer av viktiga tjänster, telekommunikationsföretag och andra leverantörer av digitala tjänster. Det statliga informationssystemet ansvarar för förvaltningen av säkert informationsutbyte. Estlands nationella CERT har en central roll i att samordna insatser vid cyberincidenter och förebygga attacker (Kohler 2020:8). *Läs mer här: Home | RIA*

Cyber Defence Unit (CDU) är placerad inom Estonia Defence League (EDL är en frivillig militär nationell försvarsorganisation med liknande uppgifter som det svenska Hemvärnet). CDU har en bred uppgift med syfte att bistå civila cyberstrukturer i fredstid och skapa stödresurser som kan tillhandahållas i kristider. Enheten skapades 2010 som en följd av 2007 års cyberattacker (Cardash m.fl. 2013:779).

e-Governance Academy (eGA) beskriver sig själva som ”ett kompetenscentrum för att öka välståndet och öppenheten i samhällen genom digital transformation”. De har skapat National Cyber Security Index och organiserar årligen den internationella e-Governance Conference. *Läs mer här: About us - e-Governance Academy (eGA.ee)*

Center for digital forensic and cyber security, CDFCS (Taltech) ligger vid Tallinn University of Technology. Centrets målsättning är ”att arbeta för att förbättra kompetensen och förmågan inom estniskt datasäkerhetsområde genom utbildning, forskning och utveckling”. *Läs mer här: Centre for Digital Forensics and Cyber Security | TalTech*

NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) bildades efter de omfattande cyberattackerna mot Estland 2007 med Estland som ramverksnation, vilket innebär att landet står för markservice, såsom lokaler och administration (Försvarsmakten 2022b). Syftet var att utveckla medlemmarnas förmåga inom

cyberförsvarsområdet. CCDCOEs har inget operativt uppdrag och det är det upp till de enskilda medlemsnationerna att besluta om åtgärder vid cyberattacker. *Läs mer här: CCDCOE - The NATO Cooperative Cyber Defence Centre of Excellence is a multinational and interdisciplinary hub of cyber defence expertise.*

Bilaga 2. Resultat från intervjuerna

I denna bilaga redovisas primärt den empiri som samlats in genom intervjuer, men även andra källor för att beskriva kontexten för intervjumaterialet. Inledningsvis beskriver respondenterna för den mentalitet som format Estlands cyberkultur. Sedan diskuteras de svar/ämnen som framkommit i intervjuerna, enligt tematiseringen militär-civil samverkan, utbildning och informationsinsatser, informationsdelning och nätverk och till sist transparens och öppenhet.

Övergripande bild av estniskt cyberförsvar

I samtliga intervjuer framkommer en tydlig bild av hur 2007 års attacker format både ett tankesätt och en cyberstruktur. Attackerna 2007 uppges ha format en vilja till motstånd som i sin tur lade grunden för en beredskap för framtida attacker:

> ”Efter cyberattacken 2007 insåg vi att vi inte har tillräckligt med folk för att hantera cyberattacker, det fanns inga centraliserade styrkor eller någon kedja av funktioner.” (CDFCS, Taltech)

Attacken 2007 kan enligt respondent från eGA liknas vid ett vaccin. Respondenten noterade att denna första cyberattack var som:

> ”starka vitaminer som stärkte vår e-identitet när vi attackerades /…/ Ryssland gjorde oss en tjänst som uppmärksammade oss på cyberhot /…/ de fick oss att inse att vi kan utvecklas bättre om vi delar information med varandra.”

Direktören för cybersäkerhet på RIA, Gert Auväärt, har konstaterat att ”cybersäkerhet är omöjligt att uppnå utan medvetenhet och åtgärder från alla organisationer och individer” (Oyetunde 2023: 1). Uttalandet indikerar hur viktigt RIA anser att det är att inkludera hela det estniska samhället för ett motståndskraftigt samhälle. Auväärt understryker att strategin utgör en grund för ett omfattande säkerhetssamarbete mellan det civila samhället och staten, och noterar att alla medborgare är ansvariga för den nationella säkerheten enligt estnisk lagstiftning (Light m.fl. 2022). I samtliga intervjuer underströks det upprepade gånger att erfarenheter från 2007 års cyberattacker bidragit till en *whole-of-nation*-mentalitet. Representanten från eGA beskriver begreppet på följande sätt:

> ”Whole-of-nation” är ett uttryck som anger att hela Estland bör inkluderas i försvaret av nationen. Kan ses som en gräsrotsrörelse. Samhället hålls samman av RIA. Även banker och telekomföretag samarbetade för att försvara sig under attacken 2007.” (eGA)

I den intervju som hölls med representanter från RIA inom ramen för projektet framgick det tydligt att även om attackerna 2007 och attackerna sedan Rysslands invasion av Ukraina har format och hjälpt till med att upprätthålla en medvetenhet i samhället om risker och sårbarheter, så krävs ett ständigt arbete för att upprätthålla medvetenheten i hela samhället:

> ”[whole-of-nation…] detta främjade ett tankesätt, men det finns behov av att fortsätta att vårda detta tankesätt, men också behov av fortsatt finansiering av detta område.” (RIA)

Det pågår ständigt cyberangrepp och i intervjun med en av respondenterna med erfarenhet från att ha arbetat politiskt lyfts även cyberspionage som ett stort problem:

> ”Ryssland är allt för framgångsrikt... Kina och Ryssland är de största aktörerna. De har avancerade metoder, till exempel sofistikerade maskar (datavirus) som tar sig in i system som borde vara isolerade.”

En notering är att *whole-of-nation*-strategin inte bara behöver upprätthållas, utan också öka i takt med digitaliseringen, för att motverka ett glapp mellan ökande digitalisering och säkerhetsfokus.

Militär-civil samverkan

Vid intervjun med en av våra respondenter konstateras att det pågår ett (cyber)krig och att landet har överlevt flera attackvågor:

> ”Cybersoldaterna har mycket att göra, men det märks inte utåt. Kriget förs bakom lykta dörrar och är osynligt för omvärlden.” (eGA)

I tre av intervjuerna (eGA, CCDCOE samt CDFCS Taltech) lyftes framförallt Estlands defensiva cyberoperationer där Cyber Defence Unit utgör en del av det defensiva arbetet under pågående cyberattacker. Respondenterna vid intervjun med *NATO Cooperative Cyber Defence Center of Excellence* (CCDCOE) (som är beläget i Tallinn) lyfte *Locked Shields*[39] som en viktig del av ett defensivt cyberförsvar.

39 För mer information om Locked Shields se CCDCOE hemsida: *https://ccdcoe.org/exercises/locked-shields/*

Locked Shields är en årlig övning som ger möjlighet för cybersäkerhetsexperter att utveckla sin förmåga i att försvara nationella civila och militära it-system och kritisk infrastruktur mot en storskalig realtidsattack. Den privata sektorn spelar en viktig roll i övningen eftersom cybersäkerhet är en gemensam angelägenhet för både statliga och privata aktörer. Privata företag (exempelvis Microsoft) bidrar med expertis och resurser, vilket ger en realistisk miljö för att simulera cyberangrepp och försvarsåtgärder. Respondenterna vid intervjun med CCDCOE lyfte att Nato återkommande genomför även offensiva cyberoperationer inom ramen för cyberövningen *Crossed Swords*[40]. Vid Crossed Swords övningar utbildas penetrationstestare, experter på digital kriminalteknik och experter på situationsmedvetenhet, vilket även inkluderar cyberkinetiska operationer.

Respondenterna från RIA underströk att Estland visserligen tagit stora steg för att stärka cyberförsvaret, men att arbetet med att skydda Estlands digitala infrastruktur kräver fortsatt engagemang. Överbelastningsattackerna under 2022 och 2023 anses inte ha haft någon större påverkan på den digitala infrastrukturen, men bör ändå inte avfärdas:

> ”Angriparen försöker lära sig, och vill gärna genomföra mer effektiva attacker. Än så länge har de inte haft några större effekter, men det betyder inte att det kommer att vara lika ofarlig i framtiden.” (RIA)

Det kanske tydligaste exemplet på hur man i Estland gjort medvetna val för att koppla ihop civilsamhället med försvaret är den estniska beväpnade frivilligstyrkan *Estonian Defence League (EDL)* som består av främst civila medlemmar som utbildas för krisberedskap samt civilt och militärt försvar. Organisationen kom efter överbelastningsattackerna 2007 att utveckla en frivillig sektion som fokuserar på cyberförsvar, *Cyber Defence Unit (CDU)* (Light m.fl. 2022). Enligt en av respondenterna uppkom detta som ett svar på de brister som synliggjordes under överbelastningsattackerna 2007, nämligen att cyberförsvaret inte var motståndskraftigt och att det fanns brist på cyberexperter inom polisen och den nationella CERTen:

> ”Vi behövde också mer cyberexpertis inom polisen, CERT, och därför behövde vi fylla roller och öka expertisen. År 2009 bad den första gruppen människor som redan var en del av EDL om att få bilda en cyberförsvarsenhet: för att skydda e-livsstilen i Estland.” (CDFCS Taltech)

40 För mer information om Crossed Swords se CCDCOE hemsida: *https://ccdcoe.org/exercises/crossed-swords/*

Utbildning och informationsinsatser

För att involvera allmänheten i cybersäkerhetsinsatser krävs en hög medvetenheten och en hög digital kompetens bland befolkningen, vilket är en fråga som samtliga respondenter lyfte. De menade att detta varit en tydlig estnisk målsättning ända sedan frigörelsen från Sovjetunionen. Tyngden i RIA:s uppdrag att informera och utbilda, bland annat genom att de regelbundet organiserar kampanjer för att höja kunskapen och informera om cyberhygien[41], underströks av respondenten från eGA.[42] Medlemmar från *Cyber Defence League* har också ett utbildningsuppdrag, och de genomför utbildningar i cybersäkerhet vid de estniska gymnasieskolorna (Ottis 2018). Även aktörer som eGA bidrar till detta arbete genom att erbjuda utbildningar och informationsmaterial.

I intervjuerna med representanter från RIA lyfte de vikten av att arbeta med just informationsinsatser och menade på att det var en av RIAs framgångsfaktorer:

> "Vi arbetar med medvetandehöjande aktiviteter och cyberskydd som helhet. Våra målgrupper är offentlig sektor, företag och privatpersoner. Många nationella mediekampanjer, radioprogram och så vidare. /…/ Översikter och årsböcker görs alla med syftet att öka medvetenheten. /…/ om vi lär föräldrar, kan de lära sina barn." (RIA)

Informationsdelning och nätverk

Att det finns hinder för informationsdelning inom cyberdomänen är välkänt och ett svårlöst problem. Litteraturen om problematiken kring informationsdelning inom cybersäkerhetssektorn är omfattande,[43] men trots de potentiella fördelarna är det svårt att uppnå ett framgångsrikt informationsutbyte om cybersäkerhet (Zibak & Simpson, 2019). Klimburg (2011:171) går så långt som att säga att "för att utöva

41 Cyberhygien är ytterligare en term som saknar en allmänt accepterad definition. Det kan beskrivas som en uppsättning av grundläggande rutiner och åtgärder som syftar till att skydda individer och organisationer från cyberhot, såsom dataintrång, virus, och andra typer av digitala attacker. Mer kring diskussionen av definitioner finns att läsa här: Vishwanath, A., Neo, L. S., Goh, P., Lee, S., Khader, M., Ong, G., & Chin, J. (2020). Cyber hygiene: The concept, its measure, and its initial tests. Decision Support Systems, 128, 113160 eller här: Singh, D., Mohanty, N. P., Swagatika, S., & Kumar, S. (2020). Cyber-hygiene: The key concept for cyber security in cyberspace. Test Engineering and Management, 83, 8145-8152.

42 RIA har även en nyckelroll vad gäller kommunikation. På organisationens webbsida finns att tillgå information om aktuella händelser och incidenter (exempelvis publiceras månatliga rapporter om "The situation in cyberspace" med både estniskt och internationellt fokus), men de genomför även regelbundna cybersäkerhetskampanjer riktade mot olika segment i samhället (äldre, skolungdomar etc). De har även regelbundna möten med föreläsningar och diskussioner, så kallade RIA Cyber meetups. Delar av dessa möten är öppna, och sänds på sociala plattformarna Facebook och YouTube. Mötena har flera syften; utöver utbildning och informationsspridning har de även en nätverkande funktion. De har även en tydlig internationell prägel, då de sker i samverkan med det europeiska kompetenscentrumet för cybersäkerhet (ECCC).

43 För mer kring denna diskussion se exempelvis Pala, A., & Zhuang, J. (2019) eller Zrahia (2014).

någon form av verklig *whole-of-nation*-cybermakt måste staten i slutändan tvinga, samarbeta med eller övertyga icke-statliga aktörer att samarbeta". En fördel som lyfts vid intervjutillfällena är att Estland är en liten nation där det blir mer naturligt med överlappande nätverk där många känner varandra.

> "Cybersäkerhetsektorn utgörs av en liten gemenskap, med många informella kanaler genom vilka information utbyts. De flesta känner varandra och /…/vi kan utbyta information om incidenter och annan information." (RIA)

Detta lyftes i intervjuerna med RIA och CDFCS Taltech som en fördel, men det är givetvis också möjligt att den "lilla gemenskapen" medför en risk, om den är alltför personberoende, och utan förankring i organisationerna. En annan risk är att det inte finns tillräckligt med redundans i landet eller organisationen. En tredje invändning är att det räcker med att en person visar sig utgöra en risk för att flera kanaler ska anses vara kompromitterade.

På frågan om hur information som flödar i systemen centraliseras för att skapa samlade lägesbilder framhöll en av respondenterna att det är viktigare med överlappande nätverk där information delas framför delgivning av information till en central mottagare:

> "En centraliserad mottagning är inte det önskade resultatet. Vad som hjälper oss lite mer är att vi inte har en enda mötesplats. Vi har många mötesplatser, med en betydande överlappning. Ett nät av nätverk, exempelvis ett som är mer finansiellt inriktat och ett inom CERT där några av samma personer deltar. Nyckeln är överlappning." (CDFCS Taltech)

Förmågan att tidigt kunna upptäcka förändrade mönster och skapa strategiska lägesbilder är beroende av informationsinhämtning och informationsdelning. Det är alltså av hög vikt att informationsflödet mellan privata och offentliga sektorer är välfungerande för att kunna skapa tydliga normalbilder för att vidare kunna identifiera anomalier. En av respondenterna menar att:

> "Estniska CERT har fått resurser för att ha fler sensorer inom den kritiska infrastrukturen, men det måste vara frivilligt. De (CERT) har kapacitet att läsa data och dela information. Båda sidor måste vara överens om det. CERT och cyber-infrastrukturen måste ha en förtroenderelation." (eGA)

RIAs roll i att inhämta och dela information från den civila delen av cybersfären i Estland var central i den bild som målades upp av samtliga intervjurespondenter.[44] Likaså att landet tidigt haft som ambition att dela det som delas kan och främja en mer öppen kultur. Analytiker från RIA konstaterade att de inte säkerhetsklassar

44 Den estniska myndighetslösningen med Information System Authority (RIA) och dess uppdrag är särskilt intressant att analysera i samband med diskussioner kring omstruktureringen av MSB (se Försvarsberedningens totalförsvarsrapport Kraftsamling, 2024).

information, utan istället fokuserar på informella överenskommelser snarare än hårda linjer. Samtidigt var det tydligt att den problematik som Sverige och andra stater ofta kämpar med, där information behålls i ”silos” och det finns en ovilja/rädsla att dela information, inte heller är ett okänt fenomen i Estland.[45] Men även här lyfts det civil-militära samarbetet som välfungerande:

> ”Det är samtidigt ett mer naturligt samspel i Estland. Samarbetet mellan oss, militären och allmänheten gör oss redo att agera.” (RIA)

Som ett exempel på hur information kan delas trots oro över att affärshemligheter kan läcka, lyfte två av respondenterna (eGA och RIA) hur bankerna samverkar under cyberattacker och övningar. För att uppmuntra till denna typ av samverkan spekulerade en av respondenterna att samtliga aktörer måste känna att de har att vinna på att dela med sig:

> ”De privata aktörerna kommer att tjäna på det (att samverka) genom att de får information tillbaka om hot och cyberattacker. Eller genom utbildningar som regeringen kan erbjuda gratis.” (eGA)

Transparens och öppenhet

Kan transparens ses som ett verktyg för att skapa robusta processer? Den offentliga kommunikationen om sårbarheterna i e-ID tillsammans med en lösning fick en motsvarande snabb reaktion från medborgarna, som inom tre dagar uppdaterat sina e-ID:n. Här var den estniska regeringens öppenhet om sårbarheterna något som lyftes även av våra intervjurespondenter:

> ”I Estland – när kris inträffar är regeringen öppen för att berätta om vad som har inträffat. Som 2017 års ID-kris, som gjorde det möjligt för Estland att be om hjälp och det hjälpte Nato att tänka på vad man skulle göra och hur man skulle agera om ett medlemsland drabbas av cyberattacker.” (Nato CCDCOE)

Transparens underströks ett flertal gånger vid intervjuerna. Även om underrättelsetjänstens önskan att sekretessmärka känslig information, näringslivets rädsla för att affärshemligheter ska läcka eller regeringens oro för att avslöja sårbarheter ses som fullt legitima skäl att begränsa information, kan dessa begränsningar utgöra hinder för försvarsförmågan.

45 För diskussioner kring informationssilos, se även Phillips, R., & Tanner, B. (2019). Breaking down silos between business continuity and cyber security, Journal of business continuity & emergency planning, Furnell, S., & Bishop, M. (2020). Addressing cyber security skills: the spectrum, not the silo. Computer fraud & security, 2020(2) och Hurel, L. M., & Lobato, L. C. Keeping silos or building bridges?. Routledge Companion To Global Cyber-Security Strategy, 504.

Sammanfattning

För att skapa en sammanhängande och motståndskraftig nationell hållning som effektivt kan hantera och mildra cyberhot behövs samordnade och integrerade insatser över alla samhällssektorer. I våra intervjuer lyfte respondenterna olika sätt på vilket detta arbete görs i Estland:

- Militär-civil samverkan inom cyberförsvaret har varit ett område som prioriterades efter överbelastningsattackerna 2007. Erfarenheterna har legat till grund för hur estniska cyberförsvaret har utvecklats sedan dess.

- Utbildningens roll: Estland har prioriterat digitalisering och cyberutbildning i den nationella strategin för livslångt lärande, vilket har lett till en hög digitaliseringsgrad.

- Informationsinsatser och medvetenhet: RIA och andra aktörer som EGA har spelat en central roll i att höja medvetenheten om cybersäkerhet genom kampanjer, utbildningar och regelbundna informationsinsatser riktade till olika samhällssegment.

- Nätverksbaserat informationsutbyte: I Estland sker informationsdelning genom överlappande nätverk snarare än centraliserade mottagningar. Estlands lilla cybersäkerhetsgemenskap har fördelen av informella kanaler och nära relationer, men detta kan också medföra risker om systemet blir för personberoende eller brist på redundans uppstår.

- Transparensens betydelse: Den estniska regeringens öppenhet om sårbarheter, (som under 2017 års e-ID-kris) har skapat förtroende och snabb respons från medborgarna samt hjälpt andra aktörer som Nato att utveckla strategier för cyberattacker.

Bilaga 3. Jämförelser av cybersäkerhetsstrategier

I denna bilaga sammanfattas tre större jämförelser av nationella cybersäkerhetsstrategier.

"A Comparative Study of National Cyber Security Strategies of ten nations", Odebade & Benkhelifa (2022)

Jämförelsen inkluderar tjugo nationella cybersäkerhetsstrategier (hädanefter NCSS:er) publicerade på engelska i tio länder. Studien fokuserar på ett flertal punkter, bland annat: Strategiska mål, vägledande principer, hot och mål för illasinnade hotaktörer, incidenthantering, mekanismer för skydd av barn på nätet, kapacitetsuppbyggande åtgärder (kampanjer för att öka allmänhetens medvetenhet, utbildnings- och fortbildningsprogram, forsknings- och utvecklingsprogram och incitamentsmekanismer) samt samarbetsåtgärder (internationellt samarbete och offentlig-privata partnerskap).

- Författarna drar slutsatsen att Estlands distinkta vision om "det mest motståndskraftiga digitala samhället" gör landet världsledande inom cybersäkerhet, och att detta i mångt och mycket är ett resultat av cyberattackerna mot den estniska ekonomin 2007.

- De konstaterar vidare att kombinationen med medvetenhet om cyberrisker och en högkvalificerad arbetskraft är avgörande för att uppnå visionen i Estlands strategi.

- De varnar dock för att Estland är starkt beroende av utländska IT-produkter och IT-tjänster, med produkter främst från Asien och USA, vilket innebär att den risk som är förknippad med sådana IT-lösningar också ärvs, vilket påverkar deras cybersäkerhetssituation (2022:9).

"Comparative analysis of various national cyber security strategies" Shafqat & Masood (2016).

Rapporten analyserar och jämför nationella cybersäkerhetsstrategier i tjugo länder. Analysen har skett på grundval av dokumenterade rättsliga, operativa, tekniska och policyrelaterade åtgärder. Den är något äldre, så vissa faktorer kan ha förändrats sedan dess.

Vad gäller Estland specifikt, noterades att:

- Estland är ett av få länder som uppdaterar sin cybersäkerhetsstrategi regelbundet, till skillnad från ett flertal länder som inte har uppdaterat sina ursprungliga cybersäkerhetsstrategier en enda gång (Sverige är ett av dessa länder).

- Estland var bland de första länder som inrättat samordningsorgan som centralt hanterar cyberhot och cyberattacker.

- Estland var ett av enbart fyra länder som hänvisat till cyberkrigföring i sina strategier (övriga länder var USA, Tyskland och Nederländerna).

- Estland hade (vid det tillfälle då rapporten skrevs) inte nämnt möjliga framtida risker, såsom risker i samband med molntjänster, vilket exempelvis de japanska och indiska strategierna lagt fram.

"EU and NATO cybersecurity strategies and national cyber security strategies: a comparative analysis" Štitilis et al (2017).

Även denna rapport är något äldre. Rapporten gör en jämförelse mellan hur Nato och EU:s cybersäkerhetsarbete ser ut, samt ställer frågan hur nationella cybersäkerhetsstrategier överensstämmer med framtagna cybersäkerhetspolicyer och strategiska inriktningar. Estland är ett av sex länder som uppfyller flest av de kriterier de inkluderat i sina egna strategier (övriga är Italien, Lettland, Spanien, Storbritannien och USA).

Bilaga 4. Jämförande index

National Cyber Security Index (2024)

National Cyber Security Index (NCSI)[46] är ett globalt liveindex som mäter länders beredskap att förebygga cyberhot och hantera cyberincidenter. Det är också en databas med offentligt tillgängligt material som syftar till att utgöra ett verktyg för nationell kapacitetsuppbyggnad inom cybersäkerhet. Det har utvecklats av Estland själva (*e-Governance Academy*) i samverkan med FN:s utvecklingsprogram (UNDP). Det baseras på tydliga indikatorer (med medföljande förklaring över metodologi och hur man arbetat med mätbara faktorer) som är indelade i 12 teman.

- I detta index hamnar Estland på fjärde plats globalt
- Högst ”betyg” (100%) får Estland i områdena globalt ledarskap, utbildning, medvetandegörande arbete, persondatahantering, incidenthantering och hantering av cyberbrottslighet.
- Lägst betyg får landet för forskning och utbildning (50%).

Global Cybersecurity Index, International Telecommunications Union (2020)

ITU publicerar regelbundet ett cybersäkerhetsindex[47], där man tittar på länders ”åtaganden för cybersäkerhet, identifierar brister, uppmuntrar god praxis och ger användbara insikter för länder att förbättra sin cybersäkerhetsposition” (ITU 2020).

Varje lands utvecklingsnivå eller engagemang bedöms utifrån fem pelare – (i) rättsliga åtgärder, (ii) tekniska åtgärder, (iii) organisatoriska åtgärder, (iv) kapacitetsutveckling och (v) samarbete – och aggregeras sedan till en övergripande poäng. Estland fick högsta poäng (20 av 20) i samtliga kategorier utom kapacitetsutveckling där landet fick 19,5.

Detta index har sina brister; det finns exempelvis ingen djupgående diskussion om respektive lands utmaningar och utveckling, och inte heller länkar till den information som inhämtats. Çifci (2022:3) noterar att en tabelljämförelse på en sida är på så aggregerad nivå att viktiga indikatorer inte tas med.

46 *https://ncsi.ega.ee/* även Osula (2022).

47 *https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx*

Estland har över åren alltid hamnat högt på denna rankning. Den senaste rankingen publicerades 2020, och då låg Estland på tredje plats globalt och andra plats i Europa (efter Storbritannien).

Cyber Power Index (2022)

I indexet beskrivs cybermakt som sammansatt av de mål som stater försöker uppnå i och genom cyberrymden[48]. Bland dessa ingår:

- att förstöra och oskadliggöra en motståndares infrastruktur och kapacitet
- att stärka och förbättra det nationella cyberförsvaret
- att manipulera informationsmiljön
- att utöka sitt inflytande genom att fastställa internationella cybernormer och tekniska standarder

Författarna menar att cybermakt bör betraktas mot bakgrund av en stats nationella mål och regeringarna bör, och gör det i allt högre grad, anta en strategi som omfattar hela nationen (*whole-of-nation*) när de försöker utnyttja sin cybermakt (2022:2). Index inkluderar mer proaktiva (till och med mer aggressiva) faktorer, där man bland annat tittar på en nations förmåga att förstöra eller inaktivera en angripares infrastruktur och kapacitet eller att kontrollera och manipulera informationsmiljön. Här hamnar Estland på 25:e plats i den övergripande rankingen.

Högst placerad blir Estland i kategorin cyberförsvar där landet hamnar på plats 12 av 30. Inom denna kategori ställs frågorna "Har staten publicerat en cybersäkerhetsplan som definierar hur den ska skydda statliga system och/eller kritisk nationell infrastruktur?", "Har staten genomfört medvetenhets- och cyberhygienkampanjer?" och "Har staten angett att den har för avsikt att genomföra proaktivt cyberförsvar?".

48 *https://www.belfercenter.org/publication/national-cyber-power-index-2022*

Bilaga 5. Klimburgs principer för *whole-of-nation*-ansatsen applicerat på Estland

Klimburgs principer	Estland
Nationell Cyberdoktrin: Upprätta en tydlig och sammanhängande nationell strategi och policyer för cybersäkerhet som definierar roller och ansvar för alla intressenter. Denna doktrin fungerar som en vägledande ram för sam-ordnade insatser.	I kapitel 3:2 avhandlas Estlands styrdokument relaterade till cyberdomänen, där slutsatsen är att cyberdoktrinen tagits fram med bas i flera sammanhängande styrdokument som tillsammans utgör en stark cyberdoktrin. I kapitel 3:3 konstateras att Estland står sig väl i jämförelse med andra länder.
Offentlig-privat partnerskap: Främja starkt samarbete mellan statliga enheter och den privata sektorn, som äger och driver mycket av den kritiska infrastrukturen. Effektiva partnerskap är väsentliga för informationsdelning, gemensamma initiativ och snabb respons på cyberhot.	I avsnitten om informationsdelning och nätverk (4:4 och 5:1:3) framgår hur man både i informella och i formella nätverk arbetar tillsammans med den privata sektorn för att underlätta flödet av information mellan den offentliga och den privata sektorn. I intervjumaterialet nämns inte frågan explicit, men vikten av samverkan underströks ett flertal gånger.
Engagemang av civilsamhället: Involvera civilsamhällesorganisationer, akademin och allmänheten i cybersäkerhetsinsatser. Detta inklu-derar att öka medvetenheten, främja digital kompetens och uppmuntra proaktivt deltagande i att säkra cybermiljön.	Det här är möjligtvis den princip som diskuterades mest i intervjuerna. Vikten av att upprätthålla en hög medvetenhet bland civilsamhället för att stärka motståndskraften mot cyberangrepp är central i det estniska systemet. Detta görs genom informationsinsatser, men även genom organisationer såsom CDU.
Internationellt samarbete: Engagera sig med internationella partners för att hantera den globala karaktären av cyberhot. Detta innebär diplomatiska insatser, deltagande i internationella cybersäkerhetsforum och samarbete om gränsöverskridande initiativ och informationsdelning.	Estland har på många sätt tagit en plats i täten bland EU-länderna vad gäller cyberförsvar, och landets värdskap för CCDCOE är ett uttryck för landets ambition att ligga långt framme i internationella cybersamarbeten.
Kapacitetsbyggande: Utveckla och förbättra färdigheter och kapaciteter hos alla intressenter, inklusive statlig personal, privata sektorns anställda och medborgare. Detta inkluderar utbild-ning, träningsprogram och investerin-gar i forskning och utveckling.	Cyberfärdigheter är en uttalad del av landets utbildningsstrategi. Organisationer såsom RIA och eGA arbetar med utbildningar och kampanjer för att upprätthålla den höga nivå av cybermedvetenhet och förståelse som finns i Estland. Däremot hamnar landet lite lägre i internationella index i frågor vad gäller forskning och utveckling (se exempelvis NCI 2024).

Resiliens och redundans: Bygga robust och motståndskraftig cyberinfrastruktur som kan motstå och återhämta sig från attacker. Denna princip betonar vikten av redundans, reservsystem och katastrofåterhämtningsplaner.	Som noteras hade attackerna 2007 den effekten att landets ledning och medborgare fick en stärkt förståelse för behovet av en motståndskraftig cyberstruktur. Det är svårt att avgöra landets kapacitet för redundans, men frågan tycks vara av stor vikt inom alla sektorer.
Delning av hotinformation: Upprätta mekanismer för realtidsdelning av hotinformation mellan intressenter. Effektiv informationsdelning förbättrar situationsmedvetenheten och möjliggör proaktiva åtgärder mot framväxande hot.	Under intervjuerna konstaterades att det i Estland (liksom i de flesta länder) finns ett problem med ”silo”-tänkande. Effektiv informationsdelning underlättas möjligtvis av landets ringa storlek, vilket möjliggör täta nätverk, men i hur hög grad informationsdelningen sker är svårt att avgöra.
Regulatoriska och rättsliga ramar: Utveckla och genomdriva lämpliga regleringar, standarder och rättsliga åtgärder för att säkerställa cybersäkerhet. Detta inkluderar att skapa lagar som hanterar cyberbrott, dataskydd och kritisk infrastruktursäkerhet.	Estlands regulatoriska arbete är väl utvecklat och står sig bra i internationella jämförelser. Det faktum att man, till skillnad från flera andra länder, uppdaterar sina strategier löpande kan ses som en indikation på att landet strävar efter att vara i framkant i domänen.
Incidentrespons och hantering: Skapa samordnade och effektiva incidentresponsramar som involverar alla relevanta intressenter. Denna princip fokuserar på snabb detektion, inneslutning, begränsning och återhämtning från cyberincidenter.	Detta område var svårt för rapportens författare att få information om. Det är vår förhoppning att i framtiden kunna återkomma till denna punkt. Hur väl implementeringen av NIS2 kommer att genomföras i landet bör ge oss mer information på området.
Ansvarsskyldighet och styrning: Säkerställa tydliga styrstrukturer och ansvarsmekanismer för cybersäkerhetsinsatser. Detta innebär att definiera roller, ansvar och tillsynsmekanismer för att säkerställa effektiv implementering och kontinuerlig förbättring.	Inte heller denna punkt återfinns i intervjumaterialet. En översikt av de formella strukturer som finns i Estland indikerar att man arbetat aktivt med denna fråga (se kapitel 3:1:2).

FOI
Swedish Defence Research Agency
SE-164 90 Stockholm

Phone: +46 8 555 030 00
Fax: +46 8 555 031 00

www.foi.se