Utredning om myndigheternas verksamhetsförutsättningar i fråga om cybersäkerhet

STATSRÅDETS PUBLIKATIONER 2023:70 vn.fi

VALTIONEUVOSTO
STATSRÅDET

Statsrådets publikationer 2023:70

Utredning om myndigheternas verksamhetsförutsättningar i fråga om cybersäkerhet

Statsrådet Helsingfors 2023

Julkaisujen jakelu
Distribution av publikationer

Valtioneuvoston julkaisuarkisto Valto

Publikations-
arkivet Valto

julkaisut.valtioneuvosto.fi

Statsrådet
Inrikesministeriet
Försvarsministeriet

ISBN pdf: 978-952-383-534-4
ISSN pdf: 2490-0966

Layout: Statsrådets förvaltningsenhet, publikationsverksamheten

Helsingfors 2023

Presentationsblad
28.9.2023

Utredning om myndigheternas verksamhetsförutsättningar i fråga om cybersäkerhet

Statsrådets publikationer 2023:70

Utgivare	Statsrådet		
Utarbetad av	Arbetsgruppen för projektet för cyberutredning		
Språk	svenska	**Sidantal**	53

Referat

Den 15 februari 2022 tillsatte inrikesministeriet och försvarsministeriet ett utredningsprojekt för att bedöma myndigheternas verksamhetsförutsättningar i fråga om tryggandet av den nationella cybersäkerheten, bekämpandet av cyberbrottslighet, cyberförsvaret och situationer som utvecklas snabbt och som hotar cybersäkerheten i samhället.

I projektet har det gjorts en bedömning av de nuvarande verksamhetsförutsättningarna i fråga om att trygga cybersäkerheten och de viktigaste utvecklingsbehoven har identifierats. Det har även gjorts en bedömning av den nuvarande verksamhetsmodellen vid situationer där cybersäkerheten är allvarligt hotad och av utvecklingsbehov som gäller informationsutbytet och samarbetet mellan myndigheterna samt getts förslag på åtgärder som utvecklar lagstiftningen.

Rapporten har beretts i brett samarbete mellan de ministerier och ämbetsverk som har att göra med cybersäkerhet. I nuläget har myndigheterna inte tillräckliga verksamhetsförutsättningar för en effektiv beredskap för och bekämpning av allvarliga cyberhot som äventyrar den nationella cybersäkerheten och försvaret. Rapporten innehåller arbetsgruppens förslag på både utvecklingsåtgärder som kan genomföras inom kort och utvecklingsåtgärder som kräver ändringar i lagstiftningen inom sju viktiga delområden: den strategiska målbilden för cybersäkerheten, samarbete och myndighetsprocesser, lägesbild, informationsutbyte, påverkan och motåtgärder, informationsinhämtning och skydd av myndighetsnätverk.

Nyckelord	cyberförsvar, cyberhot, cyberpåverkan, myndighetsverksamhet, cybersäkerhet, nationell säkerhet, cyberbrottslighet, beredskap

ISBN PDF	978-952-383-534-4	**ISSN PDF**	2490-0966
Ärendenummer	VN/2434/2022	**Projektnummer**	PLM003:00/2022

URN-adress https://urn.fi/URN:ISBN:978-952-383-534-4

Kuvailulehti
28.9.2023

Selvitys viranomaisten toimintaedellytyksistä kyberturvallisuudessa

Valtioneuvoston julkaisuja 2023:70

Julkaisija	Valtioneuvosto		
Yhteisötekijä	Kyberselvityshankkeen työryhmä		
Kieli	ruotsi	**Sivumäärä**	53

Tiivistelmä

Sisäministeriö ja puolustusministeriö asettivat 15.2.2022 selvityshankkeen viranomaisten toimintaedellytysten arvioimiseksi kansallisen kyberturvallisuuden varmistamisessa, kyberrikollisuuden torjunnassa, kyberpuolustuksessa sekä nopeasti kehittyvissä yhteiskunnan kyberturvallisuutta uhkaavissa tilanteissa.

Hankkeessa on arvioitu viranomaisten tämän hetken toimintaedellytyksiä kansallisen kyberturvallisuuden varmistamisessa vakavia kyberuhkia vastaan sekä tunnistettu keskeiset kehittämistarpeet, arvioitu tämän hetken toimintatapamallia vakavissa kyberturvallisuutta vaarantavissa tilanteissa sekä viranomaisten välistä tiedonvaihtoa ja yhteistoimintaa koskevia kehittämistarpeita sekä ehdotettu toimenpiteitä lainsäädännön kehittämiseksi.

Raportti on valmisteltu laajassa yhteistyössä kyberturvallisuuteen liittyvien ministeriöiden ja virastojen kanssa. Nykytilassa viranomaisilla ei ole riittäviä toimintaedellytyksiä tehokkaasti varautua ja torjua vakavimpia, kansallista kyberturvallisuutta ja maanpuolustusta vaarantavia kyberuhkia. Raportti sisältää työryhmän ehdotukset sekä nopeasti toimeenpantavista että lainsäädäntömuutoksia vaativista kehittämistoimenpiteistä seitsemältä keskeiseltä osa-alueelta: kyberturvallisuuden strateginen tavoitetila, yhteistoiminta ja viranomaisprosessit, tilannekuva, tiedonvaihto, vaikuttaminen ja vastatoimet, tiedonhankinta ja viranomaisverkkojen suojaus.

Asiasanat	kyberpuolustus, kyberuhat, kybervaikuttaminen, viranomaistoiminta, kyberturvallisuus, kansallinen turvallisuus, kyberrikollisuus, varautuminen		
ISBN PDF	978-952-383-534-4	**ISSN PDF**	2490-0966
Asianumero	VN/2434/2022	**Hankenumero**	PLM003:00/2022
Julkaisun osoite	https://urn.fi/URN:ISBN:978-952-383-534-4		

Description sheet
28 September 2023

Report on the authorities' capacity to act in cyber security matters

Publications of the Finnish Government 2023:70

Publisher	Finnish Government		
Group author	Working group on cyber security project		
Language	Swedish	**Pages**	53

Abstract

The Ministry of the Interior and the Ministry of Defence set up a project on 15 February 2022 to assess the capacity of authorities to ensure national cyber security, prevent cybercrime, implement cyber defence and respond to rapidly evolving situations that threaten society's cyber security.

The project assessed the current capacity of authorities to ensure national cyber security against serious cyber threats, identified key development needs, assessed both the current operating model in situations that seriously endanger cyber security and the exchange of information between authorities with related development needs. The working group also proposed measures to develop legislation.

The report was prepared in broad-based cooperation with the ministries and agencies that deal with cyber security. In the current situation, the authorities do not have sufficient capacity to effectively prepare for and combat the most serious cyber threats that endanger national cyber security and national defence. The report contains the working group's proposals, for both development measures that can be rapidly implemented and those that require legislative amendments, in seven key areas: the desired strategic end state in cyber security, cooperation and official processes, situation awareness, exchange of information, influencing and countermeasures, information gathering and protection of the authorities' networks.

Keywords cyber defence, cyber threats, cyber interference, official activities, cyber security, national security, cybercrime, preparedness

ISBN PDF	978-952-383-534-4	**ISSN PDF**	2490-0966
Reference number	VN/2434/2022	**Project number**	PLM003:00/2022

URN address https://urn.fi/URN:ISBN:978-952-383-534-4

Innehåll

1 Inledning

Finlands säkerhetsmiljö har förändrats betydligt och blivit komplicerad, särskilt efter Rysslands invasion av Ukraina i februari 2022. Samtidigt har digitaliseringen tagit fart, vilket har gjort samhällena allt mer beroende av att informationsnäten och systemen fungerar utan störningar. Digitaliseringsutvecklingen har gett stater och icke-statliga aktörer möjlighet att allt effektivare använda cybermiljön som påverkanskanal. Den tekniska utvecklingen har i sin tur gjort det möjligt att inom allt kortare förberedelsetid i cybermiljön genomföra allt mer förtäckta åtgärder som riskerar den nationella säkerheten och som har allt mer allvarliga konsekvenser. På så sätt har även vår cybermiljö förändrats för gott.

En fientlig cyberverksamhet har blivit en etablerad del av cybermiljön. Den är inte enbart begränsad till undantagsförhållanden, utan den drivs varje dag även i Finland i form av cyberpåverkan, cyberspionage och cyberbrottslighet. Såväl de statliga aktörernas som cyberbrottslingarnas förmåga att göra intrång i informationssystem har utvecklats snabbt och på så sätt har cybersäkerhetshoten blivit mångformigare och antalet cybersäkerhetshot ökat.

En kontinuerlig och ofta till och med oväntad utveckling som är karaktäristisk för allvarliga cyberhot förutsätter att beredskapen mot och hanteringen av cyberhot utvecklas ständigt. Inom statsförvaltningen i Finland ligger informationssäkerheten på en god nivå och beredskapen mot cyberhot är en del av myndigheternas dagliga verksamhet. Trots det har statsförvaltningen funnit behov av att vidareutveckla myndigheternas verksamhetsförutsättningar för att förbereda sig på och hantera allvarliga cyberhot, såväl för att kunna skydda den nationella säkerheten som för att säkerställa en effektiv myndighetsverksamhet.

1.1 Bakgrunden till utredningen

Cybersäkerhet behandlades redan i säkerhetsstrategin för samhället 2010 (statsrådets principbeslut 16.12.2010). I strategin identifierades cyberhot som ett potentiellt hot och det konstaterades att intrång i informationssystem under vissa förhållanden rent av kan motsvara kännetecknen på användning av militära maktmedel. I strategin för cybersäkerheten i Finland 2013 (statsrådets principbeslut 24.1.2013) fastställs en vision om att

Finland år 2016 är en global föregångare inom beredskapen inför cyberhot och hanteringen av de störningssituationer som de förorsakar. I strategin fastställs dessutom flera viktiga faktorer och detta dokument presenterar utvecklingen av de faktorerna.

I strategin för cybersäkerheten i Finland 2019 (statsrådets principbeslut 3.10.2019) ställs de viktigaste nationella målen upp för utvecklingen av cybermiljön och säkerställandet av de vitala funktioner som anknyter till den. Syftet med strategin är också att stödja tillgången till pålitliga digitala tjänster och utvecklingen av affärsverksamheten i anslutning till dem. Genomförandet av den nationella cybersäkerheten som ett delområde för säkerhet och försvar är kopplad till säkerhetsstrategin för samhället 2017 (statsrådets principbeslut 2.11.2017) och till de allmänna principer för samordning av beredskapen med säkerheten som beskrivs i strategin samt till den behöriga myndighetens principer. Finlands ståndpunkter på folkrätten i cybermiljön beskrivs i sin tur i en ståndpunkt som offentliggjordes 2020 (internationell rätt i cybermiljön, Finlands nationella ståndpunkter, USP 13/2020 rd).

Den 15 februari 2022 tillsatte inrikesministeriet och försvarsministeriet ett gemensamt utredningsprojekt enligt den inre säkerheten och riktlinjerna i försvarsredogörelserna samt enligt Utvecklingsprogrammet för cybersäkerheten (statsrådets principbeslut 10.6.2021) i syfte att bedöma myndigheternas verksamhetsförutsättningar i fråga om tryggandet av den nationella cybersäkerheten, bekämpandet av cyberbrottslighet och situationer som utvecklas snabbt och som hotar cybersäkerheten i samhället, med beaktande av den kontinuerliga utvecklingen av den nationella respektive internationella hotmiljön (PLM003:00/2022).

Petri Knape, direktör för enheten för nationell säkerhet vid inrikesministeriet, har varit ordförande för arbetsgruppen, Mikko Soikkeli, dataadministrationsdirektör vid försvarsministeriet, har varit vice ordförande och Hannu Kotipelto, specialsakkunnig vid inrikesministeriet, och Kosti Honkanen, äldre regeringssekreterare vid försvarsministeriet, har varit sekreterare. Medlemmarna i arbetsgruppen har varit Outi Slant, specialsakkunnig vid kommunikationsministeriet, Kimmo Janhunen, ledande sakkunnig vid justitieministeriet, Harri Ohra-aho, konsultativ tjänsteman vid försvarsministeriet, Tiina Ferm, lagstiftningsråd vid inrikesministeriet, Aliisa Tornberg, rådgivare i internationella frågor vid Republikens presidents kansli, Stefan Lee, teamledare vid utrikesministeriet (till och med den 7 december 2022), Marko Sjöroos, specialsakkunnig vid Statsrådets kansli, och Tuija Kuusisto, informationsförvaltningsråd vid finansministeriet.

Sakkunniga i arbetsgruppen har varit specialforskare Sari Kajantie och chefsjurist Jan Sjöblom vid Skyddspolisen, Anu Jaakkola, kriminalinspektör vid Centralkriminalpolisen, Janne Jokinen, biträdande avdelningschef, ingenjörsöverste vid Försvarsmakten, enhetschef Jani Mattila och produktchef Kasperi Havupolku vid Valtori, Kirsi Karlamaa, generaldirektör för Transport- och kommunikationsverket, Sauli Pahlman, överdirektör vid

Cybersäkerhetscentret vid Transport- och kommunikationsverket, Kimmo Ulkuniemi, polisinspektör vid Polisstyrelsen, och Rauli Paananen, statens cybersäkerhetsdirektör vid kommunikationsministeriet.

I arbetsgruppens arbete deltog även Tarja Fernández, ledande sakkunnig vid utrikesministeriet, Stefan Lee, biträdande cybersäkerhetsdirektör vid kommunikationsministeriet (från och med den 8 december 2022), Tuomo Rusila, avdelningsstabsofficer, överstelöjtnant vid Försvarsmakten, och Timo Nuutinen, informationsförvaltningsråd vid finansministeriet. Under arbetet hördes också en del andra sakkunniga. I arbetsprojektgruppens arbete deltog även Tarja Fernández, ledande sakkunnig vid utrikesministeriet, Stefan Lee, biträdande cybersäkerhetsdirektör vid kommunikationsministeriet (från och med den 8 december 2022), Tuomo Rusila, avdelningsstabsofficer, överstelöjtnant vid Försvarsmakten, och Timo Nuutinen, informationsförvaltningsråd vid finansministeriet. Under arbetet hördes också en del andra sakkunniga.

1.2 Mål och uppgifter för utredningsarbetet

Målet för utredningsarbetet, som inleddes i mars 2022, var att ta fram utvecklingsförslag för att förbättra myndigheternas verksamhetsförutsättningar i fråga om att trygga den nationella cybersäkerheten, bekämpa cybersäkerhet, cyberförsvaret och situationer som utvecklas snabbt och som hotar cybersäkerheten i samhället. Som precisering i beslutet om tillsättande konstaterades det att uppgiften för utredningsarbetet var att

- bedöma myndigheternas nuvarande verksamhetsförutsättningar i fråga om att trygga den nationella cybersäkerheten mot allvarliga cyberhot, och att identifiera de viktigaste utvecklingsbehoven,
- utvärdera utvecklingsbehov som uppstår till följd av förändringar i den nationella respektive internationella omvärlden,
- utvärdera den nuvarande verksamhetsmodellen i allvarliga situationer som äventyrar den nationella cybersäkerheten, att vid behov utarbeta ett förslag till en verksamhetsmodell som gör det möjligt att fatta beslut i rätt tid och på rätt nivå och effektivt bedriva proaktiv verksamhet och reagera samt vidta eventuella motåtgärder,
- i anslutning till föregående punkt utvärdera utvecklingsbehoven på olika lednings- och samarbetsnivåer i fråga om informationsutbytet och samarbetet mellan myndigheterna,
- i behövlig utsträckning utreda verksamhetsförutsättningarna för myndigheterna i de länder som är centrala med tanke på projektet när det gäller förebyggande och bekämpning av cyberhot,
- vid behov lägga fram ett förslag i fråga om ändringsbehov i lagstiftningen,

– samordna projektåtgärderna med andra projekt för cybersäkerhets-utveckling och med beredningen av en säkerhetsstrategi för samhället.

Utredningen fokuserade inte på bekämpning av nätbrottslighet som betraktas som vanlig, utan fokus låg på att upptäcka och identifiera de cyberhot och cyberbrott – vanligen mot den nationella säkerheten och försvaret – som är mest allvarliga med tanke på samhället, och på att möjliggöra bekämpning och ingripa i hoten. Syftet var att ta fram utvecklingsförslag som möjliggör bättre verksamhetsförutsättningar för säkerhetsmyndigheterna att skydda den nationella säkerheten.

En uppgift var även att samordna projektåtgärderna med andra projekt för cybersäkerhetsutveckling, såsom regeringens proposition av den 27 oktober 2022 till riksdagen med förslag till lagar om ändring av lagen om tjänster inom elektronisk kommunikation, 29 § i lagen om behandling av personuppgifter inom Försvarsmakten och 22 § i lagen om behandling av personuppgifter i polisens verksamhet (RP 243/2022 rd). Av denna anledning ansågs det att det i utredningsarbetet var ändamålsenligt att använda förarbetet för regeringens proposition ovan, när verksamhetsförutsättningarna för myndigheterna i de centrala länderna utreddes. I samband med beredningen av regeringens proposition utvärderades lagstiftningen och myndigheternas uppgifter i fråga om cybersäkerhet i Sverige, Norge, Tyskland, Storbritannien och Frankrike. I förarbetet upptäckte man att myndigheternas uppgifter och befogenheter varierar så mycket från stat till stat att utländska erfarenheter och utländsk praxis inte direkt har kunnat utnyttjas för att hitta en nationell lösning. I detta utredningsarbete ansågs det vara mer ändamålsenligt att fokusera på att ta fram utvecklingsförslag från nationella utgångspunkter, utöver att det sensitiva temat gör det mycket svårt för externa aktörer att tolka inskrivningarna i lagstiftningen i olika länder och utvärderingen av den verkliga praktiska implementeringen av inskrivningarna.

Eftersom cybermiljön har en mångsidig karaktär och genomsyrar hela samhället, granskade utredningen nuläget för informationsproduktionen och verksamhetsmöjligheterna för säkerhetsmyndigheterna och andra myndigheter och aktörer som har en central roll i cybermiljön och kartlade förslag till åtgärder för att utveckla informationsproduktionen och verksamhetsmöjligheterna. Enligt kartläggningen kunde vissa föreslagna utvecklingsåtgärder inledas utan att lagstiftningen behövde ändras, medan andra konstaterades kräva ytterligare utredningar för en detaljerad bedömning av behovet av att ändra lagar.

I enlighet med uppdraget fokuserade utredningsarbetet på att utvärdera myndigheternas verksamhetsförutsättningar och utvecklingsbehov. I utredningen lades dock märke till att en del av de föreslagna utvecklingsåtgärderna även hade samband med privata aktörer. I fråga om dessa förslag till utvecklingsåtgärder identifierades behovet av att inkludera den privata sektorn i en eventuell senare fortsatt beredning av förslagen.

2 Cybermiljö och hot mot cybermiljön

2.1 Cybermiljö

De vitala dagliga funktionerna i vårt moderna samhälle, det vill säga regering, vatten- och energiförsörjning, banksystem, hälso- och sjukvård och logistik, är allt mer beroende av informationsnät. Fungerande informationsnät och integritet, konfidentialitet och tillgång till myndigheternas informationslager är förutsättningar för en effektiv verksamhet i vårt digitaliserade samhälle och i staten. Dessutom erbjuds befolkningen allt större möjligheter att använda den offentliga förvaltningens digitala tjänster, och dessa tjänster har blivit en del av den normala vardagen. I och med att utbudet av digitala tjänster och antalet användare ökar, ökar också mängden data som brottslingar är intresserade av och möjligheterna till nätbrottslighet.

En cybermiljö som består av ett eller flera digitala informationssystem och som ofta också är geografiskt obegränsad har även blivit en allt viktigare del av utrikes- och säkerhetspolitiken. Cybermiljön används som kanal för både informationshämtning och informationspåverkan, till exempel som en del av urvalet av metoder för hybridpåverkan. Militärt sett har cybermiljön blivit en ny miljö vid sidan av de konventionella verksamhetsmiljöerna. Cyberoperationer som inleds i cybermiljön stöder den militära påverkan och möjliggör redan under normala förhållanden en fientlig påverkan mot målsamhället under tröskeln för ett konventionellt väpnat angrepp.

Fenomen i cybermiljön utvecklas och blir allt snabbare allt mer mångformiga som en del av den tekniska utvecklingen och i och med att resurserna och färdigheterna för aktörerna i cybermiljön ökar. Under de närmaste åren kan till exempel kvantdatorernas stora datorkapacitet och den automation som artificiell intelligens erbjuder bidra till att cyberattackerna är allt mer avancerade, mer objektsanpassade, formbara i realtid och svårare att upptäcka och bekämpa.

Cyberhoten har ökat och blivit allt mångformigare till följd av digitaliseringen i samhällena, den tekniska utvecklingen och aktörernas ökade kapacitet. Detta har avspeglats som ökad allvarlig cyberbrottslighet och nya hot mot den nationella säkerheten och försvaret.

2.2 Cyberhot från stater

Cyberhot mot Finland från andra stater kan handla om cyberspionage till exempel i syfte att inhämta icke-offentliga uppgifter om Finlands kritiska infrastruktur, utrikes- och säkerhetspolitiska beslutsfattande, statsförvaltningen eller försvaret. Information som söks genom cyberspionage mot Finland, och metoderna för att söka information, kan i kombination med offentliga uppgifter även möjliggöra cyberpåverkan mot Finland i ett senare skede, till exempel för att störa funktionen i vitala informationsnät eller styrsystem, förhindra användningen av sådana nät eller system eller destruera sådana nät eller system. Dessutom bedriver olika stater cyberspionage mot högteknikföretags produktutvecklingsinformation och universitets och andra forskningsinstituts forskningsdata. Ofta betecknas statliga aktörer i cybermiljön eller spår som statliga aktörer har lämnat i cybermiljön som avancerade ihållande hot (Advanced Persistent Threat, APT).

Ofta är det mycket svårt att upptäcka cyberspionage. Metoderna utvecklas avsiktligen så att kommersiella informationssäkerhetsprodukter och informationssäkerhetssystem inte kan upptäcka dem. I praktiken går det att genom cyberspionage samla in alla slags data som finns i informationssystem, det vill säga handlingar, e-postmeddelande och användardata. Dessutom kan olika rum till exempel avlyssnas och olovligt observeras med inbyggda mikrofoner och kameror i datorer och andra anordningar. Vid spionage är fördelar med cybermetoderna, jämfört med andra metoder, bland annat att priset är lågt, risken är liten och det är lätt att förneka verksamhetens ursprung. Cyberspionage kan även bedrivas mot personlig utrustning utöver organisationers informationssystem. Cyberspionaget stöds med andra metoder, såsom personbaserad underrättelseinhämtning och underrättelseinhämtning ur öppna källor.

Utöver cyberspionaget utvecklar statliga aktörer sina cyberresurser som en del av den militära kapaciteten och kapaciteten för hybridpåverkan, men kan också förvärva resurser som behövs från marknadsaktörer, brottslingar eller andra lämpliga aktörer. Dessutom kan statliga aktörer vid behov lägga ut cyberverksamhet på kriminella grupper, vilket kan syfta till att hemlighålla och förneka den statlig aktör som står bakom verksamheten. Kriminella cybergrupper kan anlitas vid dataintrång i syfte att inhämta information som en statlig aktör är intresserad av eller för till exempel överbelastningsangrepp i syfte att störa och utöva informationspåverkan. I verksamheten kan syftet även vara att använda så kallade insider, det vill säga personer som har en laglig åtkomst till önskat informationssystem. En insider kan agera för en främmande stats eller brottslingars räkning eller för att orsaka skada för den organisation som insidern företräder, till exempel på grund av hämnd eller av ideologiska skäl.

Cybermiljön har blivit en separat militär verksamhetsmiljö. Redan på Natotoppmötet i Warszawa 2016 konstaterade Nato att cybermiljön var en likadan militär verksamhetsmiljö som de mer konventionella miljöerna, nämligen land, hav, luft och rymd. På likadant sätt som de konventionella verksamhetsmiljöerna kan cyberoperationer användas som metoder för krigsföring eller för att förbereda krigsföring. I detta syfte är det även möjligt att genom cyberoperationer till exempel inhämta information om industriautomationssystem i den kritiska infrastrukturen i den stat som är föremål för operationen. Cyberoperationerna kan genomföras som fristående operationer eller i kombination med andra operationer som specialtruppoperationer, underrättelse, elektronisk krigsföring och särskilt informationsoperationer. Cyberoperationer kan genomföras under tröskeln för användning av militärt våld redan under normala förhållanden, vilket delvis har gjort gränsdragningen mellan fred och krig suddigare. Vid sidan av informationspåverkan kan de vara en metod för hybridpåverkan för statliga aktörer i syfte att bidra till att nå egna mål redan under fredstid.

Förutom att cyberoperationer riktas till Finland är det möjligt att man försöker utnyttja informationsnätinfrastrukturen i Finland i en cyberverksamhet som bedrivs mot en tredje part.

2.3 Allvarlig cyberbrottslighet

Cyberbrottslingar kan försöka vinna ekonomisk fördel eller rykte och respekt som framgångsrika dataintrång eventuellt medför. Det är inte bara enskilda medborgare och företag utan även kritiska samhällsaktörer som kan bli offer. Objekt för cyberbrottslighet som riskerar den nationella säkerheten kan till exempel vara viktiga tjänsteproducenter inom hälso- och sjukvården eller energiaktörer som är kritiska med tanke på försörjningsberedskapen. Angrepp med utpressningsprogram mot företag kan i värsta fall även ha globala konsekvenser för tillgången till råvaror eller komponenter, eller så kan ett dataintrång riktas till en stor grupp medborgare och deras känsliga personuppgifter. Dessutom är det möjligt att genom allvarlig cyberbrottslighet förbereda och skapa en grund för omfattande åtgärder mot samhället, till exempel genom att inhämta information eller skaffa åtkomst till informationssystem.

I sin verksamhet använder kriminella cybergrupper till exempel nätfiske, dataintrång, överbelastningsangrepp och utpressningsprogram. Cyberbrottslingar väljer ofta sina objekt av opportunistiska skäl och utifrån en nyttokostnadsanalys och försöker då minimera användningen av de resurser som behövs för dataintrånget och maximera vinsterna. Cyberbrottslingar som har god it-kompetens säljer sin kompetens även som en tjänst (Cybercrime as a Service, CaaS), som inte enbart kan utnyttjas av cyberbrottslingar utan även av statliga aktörer. Den senaste tidens kriser har visat att åtgärder som skickliga

individer på egen hand har vidtagit även kan drabba andra stater. Då kan det hända att åtgärderna antingen tendentiöst eller felaktigt tolkas som att en annan stat har genomfört dem.

3 Internationell omvärld

3.1 Folkrätt

Folkrätten skapar allmänna ramar för staternas verksamhet, även i cybermiljön. Denna utgångspunkt har antagits i bred utsträckning, bland annat i rapporter från FN:s grupp av regeringsexperter (2013 och 2015) och i rapporten 2021 från generalförsamlingens öppna arbetsgrupp. Olika stater har dock olika syner på hur folkrätten gäller cybermiljön och hur reglerna ska tolkas. Mellanstatliga förhandlingar om hur folkrätten ska tolkas i cybermiljön fortsätter inom ramen för FN.

I ställningstagandet 2020 sammanställde utrikesministeriet Finlands ståndpunkter på hur folkrätten tolkas i cybermiljön. Finlands ståndpunkter utgår i regel från behov av att

1. fastställa att Finland även kan reagera på kränkningar av sin politiska självständighet eller sin territoriella integritet, när kränkningarna sker i cybermiljön,
2. fastställa att alla stater har en rättslig förpliktelse att även undvika gränsöverskridande allvarliga skador i cybermiljön och
3. motarbeta sådana tolkningar av folkrätten som innebär betydande risker för eskalering av aggressiv cyberverksamhet.

Ståndpunkterna rör bland annat statens suveränitet, förpliktelse att vidta åtgärder för att förebygga gränsöverskridande skador, statens ansvar och situationer där militärt våld används.

Enligt den allmänna principen för folkrätten åtnjuter varje suverän stat territoriell integritet och politiskt oberoende i förhållande till andra stater. Suveräniteten skyddar såväl statens territorium och luftrum som cyberinfrastrukturen och de informationssystem inom statens territorium som stöder sig på cyberinfrastrukturen. Den senaste tiden har det föreslagits att suveränitet endast skulle vara en princip från vilken det inte är möjligt att härleda rättsliga påföljder i cybermiljön. Finland har inte samma syn. Enligt etablerad praxis har kränkningar av territoriell integritet och av politiskt oberoende betraktats som kränkningar av suveränitet och som rättsstridiga gärningar.

Om vi godtog att regeln inte gäller i cybermiljön, skulle staters cyberstörningar i andra staters nät bli oreglerade även i situationer där störningarna har skadliga konsekvenser. I så fall skulle det vara förbjudet att, utöver cyberattacker som kan jämställas med

användning av våld eller med väpnade angrepp, ingripa i en stats interna ärenden (olaglig intervention) vilket är avgränsat till vissa frågor och dessutom kräver syfte att tvinga, vilket är svårt att bevisa.

Finland anser att obehöriga intrång i informationsnät och informationssystem som stöder sig på cyberinfrastrukturen i en annan stats territorium kan kränka statens suveränitet. Frågan ska bedömas från fall till fall med beaktande av cyberintrångets art och konsekvenser, såsom materiella skador, störningar i anläggningars funktion, ändring av data eller förstöring av data.

Obehörigt cyberintrång kan också anses vara en kränkning av suveräniteten för den stat mot vilken intrånget görs, när föremålet för intrånget är uppgifter eller tjänster som är nödvändiga för att sköta statens centrala uppgifter. Dessutom kan cyberoperationer mot objekt som skyddas av den suveräna immuniteten (krigsfartyg, statens fartyg som enbart används för offentlig verksamhet eller okommersiell verksamhet, statens luftfartyg) anses vara kränkningar av suveränitet. Finland anser att en kränkning av suveränitet är en internationellt sett rättsstridig gärning som ger upphov till statens ansvar.

Finland har även antagit tillämpningen av omsorgsplikten i cybermiljön. Det är fråga om en etablerad princip i folkrätten, en princip om att staten är skyldig att förhindra användning av sitt territorium på ett sätt som kränker statens rättigheter. Det är förbjudet att medvetet tillåta cyberoperationer inom statens territorium eller under bevakning av staten, om operationen orsakar andra stater skadliga konsekvenser. Trots att en stat ska visa en ändamålsenlig omsorgsplikt när staten bevakar sitt territorium, är staten inte befriad från skyldighet att uppfylla andra internationella förpliktelser, till exempel skyldighet att tillgodose de mänskliga rättigheterna.

Det är endast stater som kan kränka suveränitet, men den omsorgsplikt som bygger på suveränitet gäller också privata åtgärder inom en stats territorium. Allvarliga skador på andra stater till följd av privata cyberåtgärder kan ge upphov till statens internationella ansvar, men endast om staten har underlåtit att fullgöra sin omsorgsplikt.

Det saknas internationella särskilda regler om staters åtgärder i cybermiljön och därför tillämpas de allmänna reglerna om statsansvar på sådana åtgärder. Statsansvaret har betydelse, framför allt vid reflektion om vilka de potentiella motåtgärderna enligt folkrätten ska kunna vara vid internationellt sett rättsstridiga gärningar. Motåtgärderna vid gärningar som strider mot folkrätten bör uppfylla vissa rättsliga kriterier. De ska vara proportionella och syfta till att få den stat som har agerat rättsstridigt att uppfylla sina förpliktelser. Motåtgärden behöver dock inte motsvara den ursprungliga rättsstridiga gärningen. Det är med andra ord möjligt att bekämpa cyberoperationer med många olika metoder som inte är begränsade till bara cyberverksamhet.

Enligt artikel 2.4 i Förenta Nationernas stadga (FN-stadgan) skola alla medlemmar i sina internationella förbindelser avhålla sig från hot om eller bruk av våld. Denna regel är även en vedertagen norm för internationell sedvanerätt. Den naturliga rätten till individuellt eller kollektivt självförsvar i händelse av ett väpnat angrepp har antagits i den internationella sedvanerätten och i artikel 51 i stadgan. Ett väpnat angrepp eller hot om sådant berättigar till användning av våld i självförsvarssyfte för att avvärja angreppet och undanröja det omedelbara hotet.

Än så länge saknas en etablerad definition av när en cyberattack motsvarar sådant bruk av våld som avses i artikel 2.4 i FN-stadgan eller ett sådant väpnat angrepp som avses artikel 51. Enligt rådande tolkning bör en cyberoperation vara sådan att den orsakar likadana konsekvenser som en väpnad användning av våld för att den ska kunna jämställas med en väpnad användning av våld. Även hot om en cyberattack ska eventuellt kunna bryta mot förbudet att använda våld, om hotet är tillräckligt tydligt och riktat mot en annan stat.

Det är i bred utsträckning godtagbart att en målstat får vidta cyberåtgärder eller olika motåtgärder, inklusive militära metoder, mot en cyberoperation som kan jämställas med ett väpnat angrepp. I alla situationer ska åtgärderna i självförsvarssyfte vara förenliga med rättsliga regler såsom krav på nödvändighet och proportionalitet enligt FN-stadgan och den internationella sedvanerätten.

I cybermiljön gäller det inte enbart att iaktta ovannämnda regler i folkrätten utan även till exempel att följa krigets lagar och uppfylla skyldigheten att tillgodose de mänskliga rättigheterna. Krigets lagar är endast tillämpliga på cyberoperationer, om cyberoperationer är en del av en väpnad konflikt eller en orsak att inleda en väpnad konflikt.

När det gäller straffrätt är Europarådets Budapestkonvention av den 23 november 2011 det enda internationella fördraget om just it-brottslighet. Även länder som inte är medlemmar av Europarådet kan ansluta sig till konventionen. Dessutom pågår förhandlingar om FN:s konvention om it-brottslighet, och Finland deltar också i förhandlingarna som en del av Europeiska unionen. Under våren 2023 antar Europeiska unionen EU:s förslag till förordning om europeiska utlämnandeorder och bevarandeorder för elektroniska bevis i straffrättsliga förfaranden (den så kallade e-Evidence-förordningen). Dessutom har it-säkerhetsdirektivet (NIS2) antagits och för närvarande genomförs direktivet nationellt. Även ePrivacy, ett direktiv om integritet och elektronisk kommunikation, omarbetas och förslaget till dataakt och det andra tilläggsprotokollet till Budapestkonventionen om it-brottslighet bereds.

3.2 Cybersäkerhet som en del av utrikes- och säkerhetspolitiken

Den utrikes- och säkerhetspolitiska lägesöversikten våren 2022 behandlade hur förändringarna i den utrikes- och säkerhetspolitiska omvärlden återspeglades i cybermiljön. Lägesöversikten kartlade cyberhotmiljön i Finland och urvalet av metoder för att stärka Finlands cyberresurser såväl på nationell nivå som genom internationellt samarbete.

Internationellt samarbete är viktigt för EU:s och Finlands cybersäkerhet och cyberförsvar. Det ligger i Finlands intresse att ha ett nära samarbete med internationella aktörer multilateralt, regionalt och bilateralt. Detta omfattar såväl ett tekniskt samarbete och utveckling av internationella normer och standarder som en politisk dialog. Rysslands invasion av Ukraina har också påverkat det internationella samarbetet, bland annat i FN, och gjort att den värdebaserade polariseringen har ökat ytterligare. Framöver förväntas samarbetet bedrivas i allt mer avgränsade sammansättningar utifrån en gemensamt delad värdegrund, demokrati och ett människorättsbaserat och regelbaserat förhållningssätt. Till följd av det aktuella läget har EU slutit sina led, även i frågor som gäller cybersäkerhet. En gemensam strategi för cybersäkerhet har tagits fram till stöd för det politiska beslutsfattandet och det är viktigt att foga strategin till den övergripande strategiska lägesbilden.

Eftersom parterna i det regelbaserade systemet inte har nått något brett samförstånd och inte heller tagit fram en fungerande mekanism för att hantera fientliga statliga aktörers angrepp i cybermiljön, har det aktuella internationella och politiska läget gjort att samarbetet mellan likasinnade länder har blivit allt närmare när det gäller att hantera cyberhot och stärka cyberresiliens.

Finland har varit aktivt i EU vid utvecklingen av cyberdiplomatin. EU-rådets slutsatser om gemensamma diplomatiska åtgärder för att skydda sig mot cyberhot från tredjeländer antogs 2017. ”Verktygslådan för cyberdiplomati” omfattar tredjeland-cyberdialoger, åtgärder för att förebygga cyberattacker och restriktiva åtgärder (sanktioner). I de restriktiva åtgärderna ingår förbud att resa till EU och frysning av personers och sammanslutningars tillgångar. De första sanktionerna infördes 2020. De diplomatiska metoder som har använts är också demarscher mot tredjeländer och uttalanden. Verktygslådan vidareutvecklas och stärks.

EU:s cybersäkerhetsstrategi, som Europeiska unionen och Europeiska utrikestjänsten antog i december 2020, stärker EU:s diplomatiska verksamhet för att bekämpa cyberattacker. EU:s cyberdialoger med flera aktörer är en viktig del av cyberdiplomatin och arbetet med att stärka cyberresiliensen och främjar även EU:s standardiseringar.

EU:s politik för cyberförsvar utvecklas vid sidan av cyberdiplomatin. Syftet är att förbättra kapaciteten för EU:s cyberförsvarsförmåga och att effektivisera samordningen och samarbetet mellan försvarets cybergemenskaper och civila cybergemenskaper.

Debatter om cybermiljön förs inte enbart inom EU utan även bland annat inom FN, Europeiska säkerhets- och samarbetsorganisationen OSSE, Europarådet, Organisationen för ekonomiskt samarbete och utveckling (Organization for Economic Co-operation and Development, OECD) och Nato. FN:s generalförsamling har tagit de första stegen mot en global process som granskar en ansvarstagande statlig aktör (Program of Action to advance responsible State behaviour in the use of ICT in the context of international security). I FN och de regionala organisationerna som OSSE ligger fokus på att öka förtroendet genom att ge information om cyberattacker och cyberpåverkan och på att stärka cyberkapaciteten.

Via processen för Finlands Natomedlemskap skapar deltagandet i försvarsalliansens cyberförsvar en ny nivå för Finlands cyberförsvar och arbetet med att stärka cyberresiliensen. EU:s och Natos cyberresurser stärks på ett samordnat sätt.

I Finlands cyberdiplomati har dialogerna med länder som sett till värdegrunden är likasinnade blivit allt närmare. Samarbetet fördjupas i olika grupper och bilaterala dialoger med relevanta partnerländer.

3.3 Utrikes- och säkerhetspolitisk reaktion

Beslut om reaktion på fientlig statlig cyberverksamhet mot Finland fattas i etablerade utrikes- och säkerhetspolitiska processer. Utrikesministeriet bereder ärendet och sammanställer informationen som har varit tillgänglig i olika källor. Riktlinjer för Finlands reaktion dras vid behov upp på ett gemensam möte mellan det utrikes- och säkerhetspolitiska ministerutskottet och republikens president. Utrikes- och säkerhetspolitisk reaktion handlar om att identifiera den part – ofta en stat – som är ansvarig för fientlig cyberverksamhet och om respons eller reaktion på verksamheten genom olika metoder. Förfarandet kallas attribution.

I detta avseende ska attributionen skiljas från tillräknande av rättsligt ansvar. Om statliga organ eller sådana privata grupper eller personer som agerar för ett statligt organs räkning kan identifieras som cyberoperatörer som kränker en stats internationella förpliktelser, har staten ett internationellt ansvar för cyberoperationerna. Huruvida en stat tillräknas internationellt ansvar bedöms enligt etablerade rättsliga kriterier.

Attribution, det vill säga ansvarsgörande eller tillräknande, är ett flerdimensionellt begrepp. När begreppet används för fientlig statlig cyberverksamhet (cyberspionage och cyberpåverkan), avses å ena sidan processen för att identifiera en ansvarig statlig part och å ena sidan en offentlig attribution som har utförts som motåtgärd utifrån processen.

I den offentliga debatten associeras ordet attribution i första hand till offentligt fördömande av fientlig cyberverksamhet. Å ena sidan kan dock attribution betyda ett urval av motåtgärder som vidtas av en stat som har blivit föremål för fientlig cyberverksamhet och å andra sidan även en analys- och beslutsprocess som motiverar ovannämnda motåtgärder.

Attributionen omfattar flera processer som är åtskilda från varandra. Varje process har ett tydligt ändamål och å andra sidan delvis överlappande processer som förser varandra med såväl information som sina respektive metoder. Enkelt uttryckt innebär attributionen insamling och analys av fakta, en teknisk och rättslig utvärdering, beslutsfattande och till slut information om beslutet till olika parter. Attributionsförmåga är en av de viktigaste nationella resurserna för att trygga den nationella säkerheten och för att stödja det utrikes- och säkerhetspolitiska beslutsfattande som rör cybermiljön.

I en övergripande attributionsprocess behövs förmåga att utnyttja all attributionsrelaterad information, som tillhandahålls av bland annat underrättelse-, cybersäkerhets- och förundersökningsmyndigheterna som en del av sina lagstadgade uppgifter. Andra organisationer inom den offentliga förvaltningen och privata företag tillhandahåller också nödvändig information som en del av sina uppgifter och utför utredningsarbete i olika fall.

Offentlig attribution som motåtgärd är en del av en övergripande utrikes- och säkerhetspolitisk bedömning och av ett beslutsfattande som sker utifrån en ändamålsenlighetsprövning. Därför kan den inte vara automatik som bygger på i förväg fastställda kriterier. Det är också bra att komma ihåg att offentlig attribution är bara ett av de tillgängliga alternativen att reagera bland de övriga utrikes- och säkerhetspolitiska metoderna. Det är möjligt att i den utrikes- och säkerhetspolitiska attributionen inkludera olika ekonomiska och politiska motåtgärder, som vidtas antingen ensam eller som en del av det internationella samfundet. På så sätt är det möjligt att höja tröskeln för fientlig verksamhet i cybermiljön.

Formen, metoden och tidpunkten för reaktionen på fientlig statlig cyberverksamhet är alla val som ska göras utifrån en övergripande utrikes- och säkerhetspolitisk bedömning och med beaktande av bland annat följande faktorer:

a. Föremålet för fientlig statlig verksamhet, verksamhetens omfattning, allvarlighetsgraden för verksamhetens påföljder, verksamhetens intensitet

och motivet till verksamheten i relation till Finlands övergripande säkerhet och utrikes- och säkerhetspolitiska relationer,

b. den utrikes- och säkerhetspolitiska målbild som eftersträvas på längre sikt, särskilt ansvarsfullt statsbeteende och stärkande av det regelbaserade förhållningssättet i cybermiljön,
c. offentlig attribution, framför allt en gemensam attribution i samarbete med likasinnade partnerländer, skapar också avskräckning och upprätthåller den genom att öka de politiska respektive diplomatiska kostnaderna för fientlig cyberverksamhet (anseende- och legitimitetsskador).

Att fördöma cyberattacker och cyberspionage i offentligheten är en viktig del av arbetet med att stärka EU:s och de europeiska staternas säkerhet och, på nationell nivå, arbetet med att förbättra Finlands cybersäkerhet. Målet är att synliggöra fientliga gärningar och kapaciteten att upptäcka dem och att eventuellt indicera färdigheten att vidta motåtgärder. Meddelanden och motåtgärder som understryker EU:s sammanhållning och den internationella solidariteten har stor betydelse för syftet att skapa effektiv avskräckning mot fientlig cyberverksamhet.

Inom Europeiska unionen har varje medlemsland en suverän rätt att besluta om attribution. EU:s roll som samordnare är viktig, även om varje medlemsland enligt EU:s principer har frihet att välja sina metoder och förhållningssätt när det gäller attribution. EU utarbetar diplomatiska svar baserat på beslut från Europeiska unionens råd. När rådet har fastslagit att ett externt hot föreligger, kan processen framskrida. Rådet måste vara enhälligt och efter beslutet kan fysiska personer, juridiska personer och andra aktörer upptas på en sanktionslista. EU:s verktygslåda omfattar flera åtgärder som kan aktiveras från fall till fall. Medlemsländerna kan också begära att vissa åtgärder aktiveras. Nivån på motåtgärderna fastställs av EU:s statschefer och regeringar i överensstämmelse med folkrätten.

4 Nuläge för bekämpningen av cyberhot i Finland

Händelser som riskerar säkerheten i cybermiljön kan samtidigt vara informationssäkerhetshot, brott och hot som riskerar den nationella säkerheten och försvaret och som har utrikes- och säkerhetspolitiska konsekvenser. Därför har flera myndigheter ansvar för att utreda incidenterna (se tabell 1). De har alla sina respektive uppgifter som en annan myndighets åtgärder inte kan ersätta. Cybersäkerhetscentret vid Transport- och kommunikationsverket samordnar hanteringen av informationssäkerhetsincidenter, polisen ansvarar för förundersökningen, underrättelsemyndigheterna tillhandahåller information för det utrikes- och säkerhetspolitiska beslutsfattandet och Försvarsmakten ansvarar för säkerheten i försvarssystemet.

I framtagningen av cybersäkerhet deltar även en stor grupp andra myndigheter och offentliga och privata aktörer som teleoperatörer. De har särskilda lagstadgade skyldigheter och rättigheter som fastställs i lagen om tjänster inom elektronisk kommunikation (917/2014, nedan kallad TEKL). Lagen fastställer dock en del begränsningar, bland annat för utlämnande av uppgifter och för framtagning och användning av lägesbilder.

4.1 Cybersäkerhetsmyndigheter och deras lagstadgade uppgifter

Till följd av cyberhot som riktas till Finland inleds samtidigt åtgärder både av de organisationer som har drabbats av incidenten och av flera operativa myndigheter som alla har en särskild uppgift i helheten för att utreda fallet och begränsa skadorna. En del av organisationerna har även en uppgift vid beredningen av ett eventuellt påföljdsförfarande (en straffprocess eller en utrikes- och säkerhetspolitisk attribution). De relevanta myndigheternas uppgifter sammanfattas i tabellen nedan och myndigheternas cybersäkerhetsuppgifter beskrivs nedan mer ingående.

Tabell 1. De relevanta cybersäkerhetsmyndigheternas uppgifter och roller

	Informationssäkerhet i den utsatta organisationen	Valtori	Traficom	Förundersöknings-myndigheterna	Underrättelsemyndigheterna	Försvarsmakten
Händelse	Informationssäkerhets-incident i organisationen	Informationssäkerhets-incident i statens gemensamma tjänster eller informationsnät	Informations-säkerhetsincident	Brott, försök till brott och förberedelse till brott	Hot mot den nationella säkerheten eller försvaret	Beväpnat angrepp eller motsvarande externt hot
Befogenhets-bestämmelser	TEKL 272 §	TEKL 272 § Lag om verksamheten i den offentliga förvalt-ningens säkerhetsnät Lag om anordnande av statens gemensamma in-formations- och kommu-nikationstekniska tjänster	TEKL 172, 244 a, 273 och 316 §	10 kap. i tvångs-medelslagen och 5 kap. i polislagen (polisen och Skyddspolisen) Lag om militär disciplin och brottsbekämpning inom försvarsmakten (FM)	5 kap. i polislagen (Skyddspolisen) Lag om militär underrättelseverksamhet (myndigheterna med ansvar för militär underrättelseverksamhet)	4 § i lagen om försvarsmakten TEKL 272 §
Mål	Utredning av en teknisk incident som påverkar organisationen (teknisk informationssäkerhet) och/eller kartläggning och begränsning av skador (administrativ informationssäkerhet)	Utredning av en teknisk incident i statens gemensamma tjänster eller säkerhetsnät	Utredning av en teknisk incident som påverkar Finland	Utredning av parterna och fakta i händelsen i en straffprocess	Utredning av skadorna och tillhanda-hållande av information till andra sä-kerhetsmyndigheter (Skyddspolisen) eller Försvarsmakten (myndigheterna med ansvar för militär underrättelse-verksamhet) och till statens högsta ledning (båda)	Militärt försvar av Finland och tryggande av landets suveränitet

	Informationssäkerhet i den utsatta organisationen	Valtori	Traficom	Förundersöknings-myndigheterna	Underrättelsemyndigheterna	Försvarsmakten
Viktiga frågor	Hur förebyggs incidenterna framöver genom teknik?	Hur förebyggs incidenterna framöver genom teknik?	Hur förebyggs incidenterna framöver genom teknik? Finns det andra drabbade objekt? Hur identifieras incidenterna framöver?	Misstänkt brott, omständigheter under vilka brottet har begåtts, skada som har orsakats genom brottet och vinning som har nåtts genom brottet?	Vilken part som gjort gärningen, hur förebyggs incidenterna framöver, vilka skador, vilka intressen, vilken betydelse för Finlands intressen? Hur sker identifiering? Bedömning av fortsättningen av den fientliga verksamheten.	Vilka intressen? Vilka konsekvenser? Hur sker avvärjning? Bör man bidra till att avbryta verksamheten? Är det fråga om ett beväpnat angrepp eller påverkan på lägre nivå?
Åtgärder, aktörer	Informationssäkerhetsåtgärder, organisationens ledning	Informationssäkerhetsåtgärder, Valtoris ledning och kunder som berörs av incidenten	Informationssäkerhetsåtgärder, Traficom, KM eller SR beroende på innehållet i beslutet	Straffprocess, polisen, åklagaren, domstolen	Åtgärder för att bekämpa eller en utrikes- och säkerhetspolitisk process, part som beslutet förutsätter	Motåtgärder, påverkan under ett beväpnat angrepp, utrikes- och säkerhetspolitiska beslut och beslut i frågor kring militärkommandon

Statens center för informations- och kommunikationsteknik Valtori har till uppgift att med stöd av lagen om anordnande av statens gemensamma informations- och kommunikationstekniska tjänster (1226/2013, nedan kallad TORI-lagen) tillhandahålla staten gemensamma bastekniktjänster och informationssystemtjänster, som de statliga ämbetsverken och inrättningarna i princip är skyldiga att använda. Valtori ska se till att verksamheten och tjänsteproduktionen fortsätter så störningsfritt som möjligt vid störningar under normala förhållanden samt under undantagsförhållanden.

Bestämmelser om verksamheten i myndigheternas säkerhetsnät finns i lagen om verksamheten i den offentliga förvaltningens säkerhetsnät (10/2015, nedan kallad TUVE-lagen). Säkerhetsnätet möjliggör dagligt arbete såväl i operativ verksamhet som i administrativa uppgifter. Nät- och infrastrukturtjänster för säkerhetsnätet tillhandahålls med ensamrätt av statsägda **Suomen Erillisverkot Oy**. Bolaget tillhandahåller också informations- och kommunikationstekniska tjänster för myndighetsradionätet och för myndigheternas tidskritiska mobilkommunikation via bredband i enlighet med TUVE-lagen. Statens center för informations- och kommunikationsteknik Valtori tillhandahåller med ensamrätt informations- och kommunikationstekniska tjänster och integrationstjänster för säkerhetsnätet. TUVE-lagen fastställer att den som tillhandahåller tjänster för säkerhetsnätet inom sitt uppgiftsområde ska svara för att de krav på säkerhet, aktionsberedskap, annan beredskap och kontinuitet som gäller säkerhetsnätet uppfylls under normala förhållanden och vid störningar under normala förhållanden samt under undantagsförhållanden. Tjänsterna för säkerhetsnätet är viktiga vid förmedling av information som byts ut mellan myndigheter, även vid störningar som orsakas av kränkningar av informationssäkerheten.

Transport- och kommunikationsverket utvecklar och övervakar driftsäkerheten och säkerheten i informationsnät och informationstjänster samt utreder kränkningar av informationssäkerheten och hot om kränkning av informationssäkerheten mot nättjänster, kommunikationstjänster, mervärdestjänster och informationssystem. Cybersäkerhetscentret samlar in data om händelser i informationsnät, vidarebefordrar dem till olika aktörer, tar fram en nationell kombinerad lägesbild av cybersäkerheten och delar ut lägesbilden. Cybersäkerhetscentrets kunder kan använda information om lägesbilden när de ordnar och prioriterar sin beredskap. När Cybersäkerhetscentret sammanställer lägesbilden, anlitar centret Traficoms hela transport- och kommunikationssektor, säkerhetsmyndigheterna för nationella källor, såsom nätverk av organisationer som är kritiska med tanke på försörjningsberedskapen, och även sina officiella samarbetsnätverk eller internationella samarbetsnätverk som baserar sig på frivillighet och ömsesidigt förtroende.

Cybersäkerhetscentret har även tagit fram ett centraliserat system (HAVARO) som upptäcker allvarliga informationssäkerhetshot för att skydda aktörer som är viktigast med tanke på samhällets övergripande säkerhet. Cybersäkerhetscentret tillhandahåller även

statsförvaltningen en motsvarande tjänst, GovHAVARO, som upptäcker informationssäkerhetshot. Dessutom är Cybersäkerhetscentret informationssäkerhetsmyndighet i säkerhetsfrågor som gäller elektronisk dataöverföring och databehandling av säkerhetsklassificerat material.

Polisens uppgift är att trygga rätts- och samhällsordningen, skydda den nationella säkerheten, upprätthålla allmän ordning och säkerhet samt att förebygga, avslöja och utreda brott och föra brott till åtalsprövning. Polisen ska dessutom sköta andra uppgifter som uttryckligen föreskrivs i lag samt inom ramen för sina uppgifter ge var och en den hjälp som han eller hon behöver. Polisen utreder brott i informationsnät och försöker även förebygga eventuella framtida brott utifrån den information som polisen har fått. Polisen uppdaterar den nationella lägesbilden av brott i informationsnät.

Skyddspolisens uppgift är att förebygga och bekämpa de allra allvarligaste hoten gentemot den nationella säkerheten, såsom terrorism och främmande staters olagliga underrättelseverksamhet inklusive cyberspionage mot Finland. Skyddspolisen har till uppgift att upptäcka, förhindra och avslöja sådan verksamhet, sådana förehavanden och sådana brott som kan hota statsskicket och samhällsordningen eller Finlands inre eller yttre säkerhet. Skyddspolisen utför civil underrättelseinhämtning, bland annat för att utreda bakgrunden och motiven till cyberattacker på nätet för att skydda den nationella säkerheten, stödja den högsta statsledningens beslutsfattande – även i attributionsprocessen – och för att andra myndigheter ska kunna utföra de lagstadgade uppgifterna kring den nationella säkerheten.

Syftet **med den militära underrättelseinhämtningen** är att till stöd för den högsta statsledningens beslutsfattande och för att ge en förvarning inhämta och behandla information om militär verksamhet som riktar sig mot Finland eller som är av betydelse med tanke på Finlands säkerhetsmiljö för att Försvarsmakten ska kunna utföra sina uppgifter. De militära underrättelsemyndigheterna kan inhämta information om verksamhet som till sin art är militär och om verksamhet som bedrivs av en främmande stat eller om någon annan verksamhet som allvarligt hotar det finska försvaret eller som äventyrar samhällets vitala funktioner. Verksamhet som är föremål för militär underrättelseinhämtning kan även bedrivas i cybermiljön.

Till **Försvarsmaktens** uppgifter hör bland annat det militära försvaret av Finland, stödjande av andra myndigheter och givande av internationellt bistånd, samverkan och annan internationell verksamhet. Det militära försvaret av Finland innefattar övervakning av landområdena, vattenområdena och luftrummet samt tryggande av den territoriella integriteten, tryggande av befolkningens livsbetingelser, de grundläggande fri- och rättigheterna och statsledningens handlingsfrihet samt försvar av den lagliga samhällsordningen. Försvarsmaktens uppgifter kan anses innefatta även cybermiljön.

Försvarsmakten tryggar Finlands territorium, befolkningens livsbetingelser och statsledningens handlingsfrihet samt försvarar den lagliga samhällsordningen vid behov med militära maktmedel när ett väpnat angrepp eller ett motsvarande yttre hot riktas mot Finland. De militära maktmedlen ska vara förenliga med internationella förpliktelser som är bindande för Finland. Med militära maktmedel avses användning av militärpersoners personliga vapen och kraftfullare vapenmakt.

Försvarsmakten är också territorialövervakningsmyndighet. Dessutom ansvarar Försvarsmakten för den militära underrättelseverksamheten enligt beskrivningen ovan.

Till **Statsrådets kanslis** ansvarsområde hör statsrådets gemensamma lägesbild, beredskap och säkerhet samt den allmänna samordningen av hanteringen av störningssituationer. För att stödja republikens presidents och statsrådets beslutsfattande och verksamhet ska statsrådets lägescentral samla in och analysera information om säkerhetssituationen och sådana störningar och hot om störningar som äventyrar samhällets vitala funktioner, sköta och koordinera förvaltningsövergripande uppgifter som hänför sig till upprätthållande, sammanställande, samordnande och förmedlande av en lägesbild och sprida den samordnade informationen till republikens president, statsrådet och andra myndigheter.

Statsrådets lägescentral tar fram information om säkerhetshändelser i realtid och skapar en lägesbild som har sammanställts utifrån uppgifter från de behöriga myndigheterna. Lägescentralen kombinerar information från olika myndigheter och andra källor och rapporterar utgående från den till statsledningen och olika myndigheter.

Till **utrikesministeriets** ansvarområde hör bland annat utrikes- och säkerhetspolitisk beredning och verkställighet, meddelanden om utrikespolitiskt betydelsefulla ståndpunkter till andra stater och internationella organisationer, utveckling av folkrätten och andra frågor som rör folkrätten. Med stöd av lagen om internationella förpliktelser som gäller informationssäkerhet (588/2004) ska utrikesministeriet som Finlands nationella säkerhetsmyndighet även uppfylla internationella förpliktelser som gäller informationssäkerhet. I cyberfrågor omfattar utrikesministeriets ansvarsområde cyberdiplomati, folkrättslig utveckling av cybermiljön, frågor som rör fördrag, handelsekonomiska relationer och främjande av Finlands intressen via beskickningsnätverket. Utrikesministeriet har en central roll i beredningen av attributionen. Beredningen sker ofta i samarbete med Finlands internationella partnerländer.

Politikåtgärder inom olika förvaltningsområden styrs av flera ministerier. Kommunikationsministeriet bereder allmänna politikåtgärder som rör cybersäkerhet, och tjänsten som statens cybersäkerhetsdirektör är också förlagd till kommunikationsministeriet. Statens cybersäkerhetsdirektör leder och samordnar den nationella utvecklingen, planeringen och beredskapen i fråga om cybersäkerheten och är statsledningens rådgivare i ärenden som

gäller cybersäkerhet. Inrikesministeriet leder politikåtgärder för bekämpning av cyberbrottslighet och för civil underrättelseinhämtning. Försvarsministeriets uppgift är att ta fram politikåtgärder för cyberförsvar och militär underrättelseinhämtning. Dessutom är finansministeriets uppgift att utveckla cybersäkerheten inom den offentliga sektorn. I cyberverksamheten deltar utöver ovannämnda myndigheter även andra myndigheter, bland annat de tillsynsmyndigheter som avses i EU:s direktiv om säkerhet i nätverks- och informationssystem (det så kallade NIS-direktivet). Med tanke på samhällets kritiska funktioner är Försörjningsberedskapscentralen en central aktör.

5 Bedömning av nuläget och utvecklingsbehov

I den fysiska världen har myndigheterna vanligen tydliga uppgifter i hanteringen av hotfulla situationer, och ansvarsområdena och samarbetsskyldigheterna mellan olika myndigheter har fastställts. När det gäller cybermiljön saknar Finlands lag tillräckligt omfattande bestämmelser om samordningen och samarbetet mellan myndigheter på olika nivåer. Lagstiftningen beaktar inte heller i tillräcklig omfattning cybermiljöns särdrag vid hantering av cyberhot och vid informationsutbyte. Arbetet med att skydda cybermiljön är fördelat på flera förvaltningsområden, och cybermiljön har inte som en helhet utpekats och kan inte heller utpekas som ett enda förvaltningsområdes uppgift. Reaktion på hot förutsätter ett nära samarbete mellan olika förvaltningsområden såväl på strategisk nivå som på operativ nivå. Genom att göra samarbetet allt närmare är det möjligt att säkerställa att en lämplig myndighet genomför åtgärder i rätt tid, men inte äventyrar en annan myndighets uppgifter, och å andra sidan att bästa kompetens finns tillgänglig i verksamheten.

I nuläget har myndigheterna inte tillräckliga verksamhetsförutsättningar för en effektiv beredskap för och bekämpning av allvarliga cyberhot som äventyrar den nationella cybersäkerheten och försvaret. Inom följande sju viktiga delområden identifierades behov av utvecklingsåtgärder för att förbättra verksamhetsförutsättningarna: den strategiska målbilden för cybersäkerheten, samarbete och myndighetsprocesser, lägesbild, informationsutbyte, påverkan och motåtgärder, informationsinhämtning och skydd av myndighetsnätverk.

5.1 Den strategiska målbilden

Cybersäkerheten och de nationella målen och strukturerna för cybersäkerheten har utvecklats baserat på de nationella strategierna och de utvecklingsprogram som har tagits fram utifrån strategierna. Cybersäkerhetsstrategin är en del av säkerhetsstrategin för samhället och av verkställigheten av EU:s cybersäkerhetsstrategi. Den målbild som fastställs i strategierna har dock inte nåtts i alla avseenden. Till följd av att säkerheten och den operativa miljön i Finland och Europa har förändrats i grunden behövs en ny bedömning av målbilden och de strategiska nationella riktlinjerna för cybersäkerheten

även sett till Natomedlemskapet. I den övergripande bilden ligger allt större fokus på kopplingen av den nationella säkerheten, försvaret och cybersäkerheten till utrikes- och säkerhetspolitiken.

Dessutom kommer det att uppstå behov av att omarbeta den nationella cybersäkerhetsstrategin, när EU:s cybersäkerhetsdirektiv (NIS2) och CER-direktivet om kritiska infrastrukturers motståndskraft genomförs. Enligt NIS2-direktivet ska varje medlemsstat anta en nationell strategi för cybersäkerhet som anger strategiska mål, resurser som behövs för att nå målen och relevanta politiska och reglerande åtgärder, i syfte att uppnå och upprätthålla en hög cybersäkerhetsnivå, med beaktande av en nationell riskbedömning och samarbete mellan offentlig och privat sektor.

Cyberförsvar är ett försvarsområde inom cybersäkerheten och består av underrättelseverksamhetens kapacitet, påverkanskapacitet och skyddskapacitet samt av olika stödfunktioner. Det framtida Natomedlemskapet ger upphov till behov av att definiera cyberförsvaret som en del av den nationella cybersäkerheten och skapar samtidigt en parallell struktur för det samarbete som drivs inom ramen för EU. Detta förutsätter en nationell handlingsmodell som samordnar framförandet av ståndpunkter till EU och Nato.

En specificerad nationell målbild krävs särskilt för att fastställa hur en nationell reaktion på en fientlig verksamhet sker, i vilken process arten av åtgärderna definieras, vilka de befogenheter som behövs utöver de nuvarande är och vem befogenheterna tilldelas. Om frågorna ovan klarlades, skulle det i sin tur styra utvecklingen av samarbetet mellan myndigheterna, utnyttjandet av bästa kompetenser för att förbättra den nationella säkerheten och bedömningen av behovet av att ändra lagstiftningen.

Utvecklingsförslag

Den nationella målbilden ska fastställas i en ny cybersäkerhetsstrategi. Strategin ska beakta förändringar i säkerhetsmiljön, uppfylla kraven i EU-lagstiftningen och fastställa mål för det samarbete som drivs inom ramen för EU och Nato. I målbilden bör påverkan på förhållanden och fientlig verksamhet i cybermiljön vara allt mer övergripande, vilket bör ligga i linje med riktlinjerna för utvecklingen av EU:s cyberförsvar och Natos cyberförsvar och förutsätta en cyberförsvarsdoktrin.

Betydelsen av teknik ökar i geopolitiken, vilket också påverkar målen för och genomförandet av den nationella cybersäkerheten. Därför bör målbilden beakta den tekniska utvecklingen, fastställa därtill hörande val och utvärdera konsekvenserna för försörjningsberedskapen.

5.2 Samarbete och myndighetsprocesser

Vid cyberincidenter är samarbete mellan myndigheter nödvändigt, eftersom flera myndigheter är skyldiga att utreda fallet inom ramen för sin respektive uppgift. Samarbetet ska beakta arten av olika cyberhot och de befogenhets- och samarbetskrav som bekämpningen av cyberhot förutsätter. Skräddarsydda operationer som främmande staters underrättelsetjänster och arméer driver med stora resurser förutsätter andra lösningar än vad bekämpningen av vanliga dagliga hot kräver. Ett proaktivt samarbete spelar en viktig roll i uppdateringen av den kontinuerliga lägesbilden och lägesuppfattningen och samtidigt i identifieringen av betydelsefulla fall genom att kombinera information från olika myndigheter. I regel deltar även en företrädare för den utsatta organisationen, eftersom det i praktiken inte är möjligt att utreda en cyberincident och begränsa konsekvenser utan åtgärder från underhållet av det utsatta systemet. En betydande utmaning är dock att behörigheten i olika dimensioner av ett fenomen tillhör olika myndigheter. Med anledning av den egna grundläggande uppgiften och behörigheten upplevs samarbetet mellan myndigheter och behovet av samarbete på olika sätt och olika myndigheter har olika förväntningar på samarbetet.

Till följd av att det internationella läget hade tillspetsats tillsattes en samordningsgrupp på ministernivå i statsrådet den 16 maj 2022. Gruppen skulle stödja samarbetet i cybersäkerhetsfrågor och framtagningen av en lägesbild. Samarbetsgruppen har utökat växelverkan mellan olika förvaltningsområden betydligt och bidragit till den gemensamma lägesuppfattningen på strategisk nivå i statsrådet. Dessutom har olika cybersäkerhetsmyndigheter etablerade ömsesidiga samarbetsformer på sakkunnignivå. Den beslutsnivå som finns mellan den strategiska nivån och sakkunnignivån har däremot inga officiella strukturer som har tillsatts till uppgiften och som sammanträder regelbundet.

En av samarbetsformerna mellan myndigheter är också handräckning. Vanligen har Försvarsmakten och polisen kunnat ge handräckning. Vid kränkningar av informationssäkerheten har Transport- och kommunikationsverket kunnat ge andra myndigheter sakkunnighjälp som handräckning. På grund av gällande bestämmelser om handräckning kan dock till exempel Transport- och kommunikationsverket inte ta emot handräckning från andra myndigheter. Lagstiftningen om handräckning behöver därför ses över och kompletteras i fråga om cybermiljön.

Vid sidan av behovet av att intensifiera samarbetet mellan myndigheter finns det skäl att beakta att många kritiska funktioner i samhället ägs av den privata sektorn och variationerna i dessa aktörers cybersäkerhetskapacitet är stora. Vid behov biträder Cybersäkerhetscentrets CERT-verksamhet (Computer Emergency Response Team) i det första skedet aktörer vid utredningen av kränkningar av informationssäkerheten, men mer omfattande utredningsåtgärder och fortsatta åtgärder genomförs till exempel med hjälp av den privata sektorns tjänster. Med anledning av resurser eller befogenheter kan alla myndigheter i nuläget inte ge tillräckligt stöd för att de aktörer och företag som är kritiska med tanke på samhällets funktion och försörjningsberedskapen ska kunna bereda sig på och återhämta sig efter allvarliga störningar som orsakas av cyberincidenter. Framför allt i sofistikerade cyberattacker kan nuläget, där alla myndigheters kompetens och kapacitet inte finns tillgänglig, leda till att det inte är möjligt att i tillräcklig omfattning begränsa konsekvenserna av en allvarlig attack för samhällets funktion eller att tillräckligt fort återhämta sig efter allvarliga attacker.

I nuläget är det dessutom på grund av komplicerade leveranskedjor svårt att identifiera kritiska kunder och deras tjänsteleverantörer. Om de inte har identifierats i förväg, vidtar Transport- och kommunikationsverket eller andra myndigheter inte nödvändigtvis sådana åtgärder som läget kräver och byter till exempel inte ut information med andra myndigheter. En närmare beskrivning av kritiska kunder och tjänsteleverantörer skulle avsevärt främja Transport- och kommunikationsverkets och de övriga myndigheternas funktionsförmåga och samarbete.

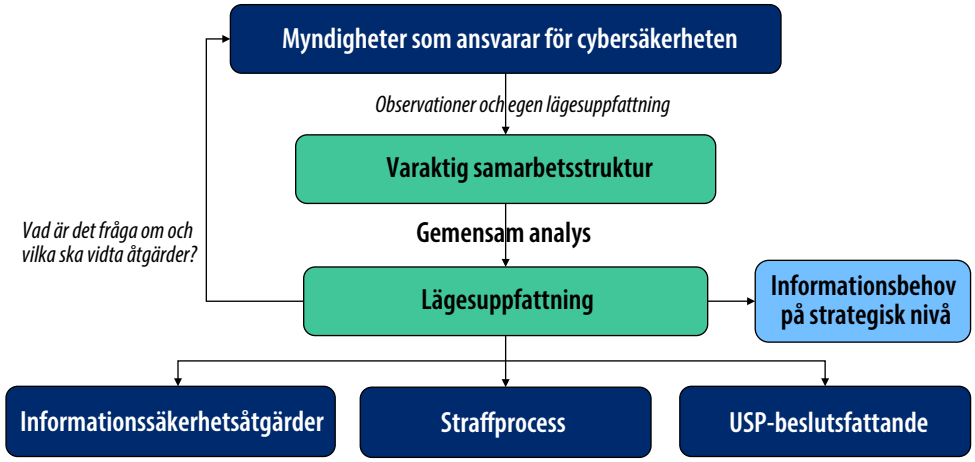
Utvecklingsförslag

En varaktig samarbetsstruktur för den ovan beskrivna ämbetsverksnivån mellan statsrådsnivån och den tekniska sakkunnignivån bör tas fram för samarbetet mellan myndigheterna. Samarbetsstrukturen bör tillsättas för uppgiften och den bör sammanträda regelbundet. I samarbetsstrukturen bör myndigheterna i samverkan analysera lägesdata som de har samlat in ur sina egna källor, och nå enligt principerna på bild 1 en gemensam lägesuppfattning som underlag för beslutsfattande och fortsatta åtgärder från myndigheter som är behöriga vid varje enskilt tillfälle. Det finns skillnader mellan förvaltningsområdenas strukturer, vilket förutsätter identifiering av de olika förvaltningsområdenas horisontella nivåer i det fortsatta arbetet.

En gemensam lägesuppfattning förbättrar förutsättningarna att identifiera allvarliga cyberhot och gör det möjligt att förmedla mer övergripande information till en strategisk nivå och andra samhällsaktörer. Utöver den varaktiga strukturen bör olika myndigheter säkerställa det egna deltagandet i befintliga och verksamma grupper för samarbete och informationsutbyte. Detta skapar förutsättningar för att bättre använda den information

som byts i grupperna. Samarbetsstrukturen ska inte ersätta myndigheternas lagstadgade uppgifter i olika processer. Den kan dock se till att all information som behövs finns tillgänglig i varje process och att lägesuppfattningen är mer övergripande.

Figur 1. Princip för myndighetssamarbetet



Baserat på den gemensamma lägesuppfattning som nås i samarbetsstrukturen är det möjligt att samordna och utvärdera nödvändiga myndighetsåtgärder eller rekommendationer till andra aktörer, oberoende av om det är fråga om informationssäkerhetsåtgärder, ärenden som ingår i straffprocessen eller stödet för det utrikes- och säkerhetspolitiska beslutsfattandet. Den etablerade samarbetsstrukturen, som möjliggör ett effektivt samarbete mellan myndigheter, kräver beskrivning och precisering av processerna och kan även förutsätta ändringar i lagstiftningen. Samarbetsstrukturen bör även beakta att informationsspridningen är tillräcklig inom förvaltningsområdena.

Myndigheterna bör kunna ge mer omfattande stöd till samhällets kritiska aktörer för att minska konsekvenserna av attacker mot kritiska aktörer. Detta förutsätter definition av kritiska aktörer och specificering av aktörerna enligt bransch. De kritiska aktörerna är också beroende av sina egna tjänsteleverantörer och därför bör de beaktas i granskningen.

Med tanke på handräckning behöver bestämmelserna om handräckning utökas så att handräckning är möjlig mellan olika myndigheter så som regeringen redan har föreslagit i sin proposition RP 243/2022 rd, som har förfallit i riksdagen.

5.3 Lägesbild

För att en lägesbild av cybersäkerheten ska kunna tas fram förutsätts en tillräcklig kapacitet att upptäcka hot mot cybermiljön. För närvarande sker observationsprocessen i olika myndigheter på olika sätt och i det syfte som myndighetens lagstadgade uppgift förutsätter. Dessutom strävar informationssäkerhetsunderhållet för varje informationssystem efter att upptäcka avvikelser i informationssystemet. Transport- och kommunikationsverket tar fram en nationell lägesbild av cybersäkerheten med hjälp av olika källor.

För att sköta sina uppgifter tar myndigheterna även för tillfället fram lägesbilder på olika nivåer, för olika användningsändamål och med olika innehåll. I Finland har myndigheternas sakkunniga tagit fram och delat ut tekniska lägesbilder under lång tid och även strategiska lägesbilder av cybersäkerheten sedan sommaren 2022. Den samordningsgrupp som nämns ovan har inrättats på ministernivå för att utöka informationsunderlaget för den strategiska lägesbilden och för att effektivisera utdelningen av information. Dessutom stöder gruppen samarbetet i cybersäkerhetsfrågor. Gruppens verksamhet bygger på samordnandet inom ramen för de befogenheter som har fastställts för myndigheterna genom lagstiftning. De behöriga myndigheterna har dock ingen kombinerad och analyserad lägesbild som de samordnar sinsemellan.

Enligt riktlinjerna i statsrådets försvarsredogörelse ska man kunna övervaka alla domäner. Med övervakning avses inte inhämtning av information om medborgares konfidentiella kommunikation. Med övervakning avses däremot framför allt framtagning och en mer systematisk sammanställning av en bättre cyberlägesbild samt möjliggörande av informationsflöden som påverkar lägesbilden, i syfte att särskilt nå en gemensam lägesuppfattning om statliga aktörers eller andra aktörers verksamhet som riskerar den nationella säkerheten i Finlands cybermiljö. En lägesbild av cyberförsvaret utgör en del av myndigheternas gemensamma lägesuppfattning. Det förutsätts informationsutbyte, befogenheter och nationella samarbetsstrukturer mellan myndigheter för att förbättra cyberlägesbilden av försvarssystemet och för att förebygga och bekämpa cyberhot.

I anknytning till framtagningen av en cyberlägesbild är det bra att beakta att en polisanmälan i nuläget görs efter eget övervägande av företag som har drabbats av en kränkning av informationssäkerheten. Aktörer som omfattas av NIS-direktivet, till exempel relevanta aktörer och tjänsteleverantörer som är kritiska för försörjningsberedskapen, är inte heller skyldiga att göra en polisanmälan i sådana situationer. NIS-aktörer gör en anmälan till den myndighet som utövar tillsyn över den aktuella sektorn, och tillsynsmyndigheten rapporterar fallen till Transport- och kommunikationsverket. Dessutom kan Transport- och kommunikationsverket få vetskap om fallen genom frivilliga anmälningar.

I nuläget kan dock Cybersäkerhetscentret vid Transport- och kommunikationsverket inte ens vid allvarliga informationssäkerhetskränkningar som hotar den nationella säkerheten eller försvaret automatiskt informera andra myndigheter utan ett uttryckligt samtycke av anmälaren.

Utvecklingsförslag

När det gäller observationsverksamheten i cybermiljön behöver informationsinsamlingen systematiseras så att det är möjligt att nå en mer omfattande lägesuppfattning om allvarliga hot som riktas mot Finland. I fråga om observationsverksamheten gäller det visserligen att behålla balansen så att myndigheterna inte heller i fortsättningen onödigt begränsar integritetsskyddet och konfidentialiteten vid kommunikation. Detta har framför allt betydelse vid bedömningen av observationen av cyberhot. Å andra sidan är det semantiska innehållet i meddelanden inte föremål vid observation av allvarliga hot och vid teknisk styrning av kritiska infrastrukturer, utan föremålet är till exempel en skadeprogramkod som får det utsatta systemet att fungera på det sätt som skadeprogrammet avser. En främmande stats fientliga verksamhet anses inte heller åtnjuta integritetsskydd och konfidentialitet vid kommunikation. Information som byts ut och behandlas i den strategiska lägesbilden handlar oftast inte heller om personuppgifter och andra uppgifter som omfattas av skyddet av de grundläggande rättigheterna, till skillnad från en situation där teknisk lägesbildinformation byts ut.

En effektivare observationsverksamhet i cybermiljön samt framtagning och analys av en förvaltningsövergripande lägesbild förutsätter tillräckliga rättigheter att lämna ut och få information, möjligheter för berörda myndigheter att byta ut information och mer omfattande och förpliktande anmälningsskyldigheter för drabbade aktörer. Detta förutsätter ändringar i lagstiftningen. Men vid sidan av en eventuell ny reglering bör möjligheterna att byta ut information även ses över utifrån den nuvarande regleringen och de olika myndigheternas uppgifter och behov av information i den förändrade säkerhetsmiljön. Hänsyn ska även tas till den pågående lagberedningen i syfte att införliva skyldigheterna i NIS2-direktivet i nationell lagstiftning, där utökning av anmälningsskyldigheten är en av de frågor som behandlas. Dessutom bör utvidgningen av anmälningsskyldigheten på nationell nivå granskas så att anmälningsskyldigheten även ska gälla sektorer som inte omfattas av direktivets tillämpningsområde, exempelvis försvaret och säkerhetssektorn. Detta kan förutsätta att såväl anmälningsskyldigheten som lagstiftningen utvidgas till sektorer som är relevanta med tanke på den nationella säkerheten och försvaret.

När bestämmelserna om utlämnande av uppgifter utvärderas, är det viktigt att utvärderingen utgår från behov eller nödvändighet som bygger på skötseln av myndighetsuppgifter och att utvärderingen är proportionell och tillräckligt noggrant specificerad. Vid utlämnande av uppgifter bör hänsyn även tas till en myndighets oavhängiga möjlighet att lämna ut till en behörig myndighet utan en uttrycklig begäran.

Framtagningen av en lägesbild mellan myndigheter bör betraktas som ett kontinuum och processen bör beskrivas och etableras. Utveckling av gemensamma processer för framtagning av lägesbilder ska kunna inledas genom att man fastslår befintliga processer och samarbetsgrupper och gör en noggrannare beskrivning av processernas och gruppernas uppgifter och målen för verksamheten. De olika myndigheterna bör inte enbart ha en delad uppfattning om hur lägesbilder tas fram och vilka de ansvariga parterna är utan också om olika lägesbilder. Detta förutsätter enhetliga specifikationer av lägesbilder och överenskommelse om vilken terminologi som används. Till exempel kan Transport- och kommunikationsverket eventuellt vara den part som samordnar de gemensamma lägesbildsprocesserna och insamlingen och analysen av data.

Framtagningen av en delad lägesbild förutsätter likväl ett närmare samarbete mellan myndigheter på den ledningsnivå som ansvarar för de praktiska åtgärderna. En del myndighetsfunktioner har lagt märke till att lägesbilden av cybersäkerheten lätt förblir en teknisk beskrivning. Då tas ärenden inte upp i den högsta ledningens diskussioner och inte heller på en ändamålsenlig beslutsnivå.

Lägesinformation om allvarliga cyberhot bör kunna delas till myndigheternas ledning och statsledningen, men allt effektivare, på ett ändamålsenligt sätt även till de företag som är kritiska med tanke på försörjningsberedskapen, kommunerna och välfärdsområdena med beaktande av säkerhetsklassificeringen av informationen. Detta skulle stödja organisationernas beredskap och stärka kapaciteten att agera snabbt och effektivt vid störningar. Samtidigt som myndigheternas rättighet att få information och organisationernas relaterade skyldigheter preciseras i lagstiftningen, bör det säkerställas att lagstiftningen inte innefattar hinder för myndigheter som är relevanta med tanke på cybersäkerheten att lämna information om cyberlägesbilden till ovannämnda parter eller hinder för parterna att ta emot informationen.

5.4 Informationsutbyte

Informationsutbytet mellan myndigheter på sakkunnignivå är i stort sett etablerat och varit aktivt inom ramen för lagstiftningen sedan början av 2000-talet. Som exempel på samarbetet kan nämnas Transport- och kommunikationsverkets nätverkssamarbete som

möjliggör ett relativt omfattande informationsutbyte. Informationsutbytet har delvis en reaktiv karaktär, vilket inte alltid möjliggör en tillräckligt aktiv beredskap mot cyberhot, avvärjande av cyberhot och beredning av användningen av befogenheter.

Samarbetet och informationsutbytet bör dock vara intensivare, särskilt när det gäller att observera hotmiljön, för att skador till följd av verksamhet som är fientlig med tanke på den nationella säkerheten och försvaret i Finland ska kunna förebyggas på ett effektivt sätt. Informationsutbytet påverkas av olika myndigheters bristfälliga kännedom om varandras uppgiftsfält, behov av information eller om sambandet mellan information och en annan myndighets uppgift. Dessutom kan de ömsesidiga beroendeförhållandena i cybermiljön leda till sådana oväntade konsekvenser för en annan myndighets uppgifter som inte har kunnat identifieras i konsekvensbedömningen i första instans.

Trots att samarbetet i myndighetsnätverket fungerar är det inte helt klart om alla nödvändiga parter deltar i det samarbete som gäller informationsutbyte. Som exempel på detta kan nämnas att underrättelsemyndigheternas och Cybersäkerhetscentrets förutsättningar att byta information i syfte att utvärdera cyberincidenter är bra, men den operativa cyberförsvarsaktören inom Försvarsmakten och polisen uteblir från informationsutbytet på grund av gällande lagstiftning. Å andra sidan kan Transport- och kommunikationsverket med anledning av lagstiftningen inte lämna ut alla uppgifter som behövs, till exempel till underrättelsemyndigheterna, utan tillstånd av den som har varit föremål för kränkning av informationssäkerheten.

Myndigheternas behörighet, olika uppgifter och användningsändamål med information utgör i nuläget en begränsning för att byta mer detaljerad information om cyberhot. Begränsningarna kan anses bygga på skyddet för privatlivet, konfidentialiteten vid kommunikation och frågor kring rättssäkerheten.

Kravet på lagstiftningen är att den ska vara tydlig för att det är klart vilken information myndigheterna kan byta och enligt vilka förutsättningar, i vilken utsträckning och i vilka situationer. När det gäller att byta personuppgifter ska användningsändamålet med uppgifterna beaktas, framför allt när det gäller gränsområdet mellan den allmänna dataskyddsförordningen och dataskyddslagstiftningen i brottmål Myndigheternas verksamhet vid praktisk tillämpning av lagar försvåras även av att flera olika författningsgrunder är tillämpliga på behandling av uppgifter som betraktas som personuppgifter. Det är viktigt att lagstiftningen är tydlig och begriplig, även med tanke på enskilda tjänsteinnehavares rättssäkerhet.

Såsom redan konstaterats ovan använder myndigheterna många olika tjänster som tillhandahålls av privata företag, och på så sätt stöder sig myndigheterna på företagens infrastrukturer. I avtal som ingås med privata aktörer kan aktörerna eventuellt uppmanas att ge information till berörda myndigheter inom ramen för gällande lagstiftning.

Utvecklingsförslag

Genom att utveckla de befintliga modellerna för informationsutbyte är det möjligt att undvika åtminstone lösningar som mestadels är överlappande. En omläggning av verksamheten i proaktiv riktning förutsätter dock nya modeller och strukturer samt granskning av lagstiftning.

Lagstiftningen om informationsutbyte behöver förtydligas, eftersom gällande lagstiftning inte kan anses möjliggöra ett tillräckligt informationsutbyte i tillräckligt bred utsträckning mellan flera myndigheter som är relevanta med tanke på bekämpning av cyberhot. Därför bör myndigheternas verksamhetsförutsättningar och informationsutbyte granskas som en helhet på ett nytt sätt för att myndigheterna vid allvarliga cyberhot ska ha tillgång till effektiva metoder som kan vidtas och genomföras snabbt. Utvidgningen av informationsutbytet förutsätter att lagstiftningen förses med en definition av tydliga förutsättningar för informationsutbyte och med en definition av parter som deltar i informationsutbyte. Å andra sidan förutsätter utvidgningen att grunderna för befintliga begränsningar för informationsutbytet utvärderas och eventuella ändringar av befogenheterna för informationsutbyte beaktas. Detta kan garantera att informationsutbytet mellan olika organisationer sker tydligare och är bundet till vissa tjänsteuppgifter som har fastställts för aktörerna på förhand och som omfattar ansvar vid informationsutbytet. Detta kan garantera att informationsutbytet fortsätter även om en viss person avgår från organisationen och å andra sidan att informationen blir tillgänglig för organisationen. En tydlig lagstiftning skulle även öka rättssäkerheten i myndigheternas verksamhet, göra enskilda händelser mer spårbara och förtydliga enskilda tjänstemäns ansvar.

Regeringens proposition RP 243/2022 rd föreslog förbättringar av myndigheternas möjligheter att byta information vid informationssäkerhetskränkningar som är allvarliga för samhällets funktion. Riksdagen hann dock inte slutföra behandlingen av propositionen före valet och därför finns det fortfarande behov av en sådan lagstiftning som avsågs i propositionen.

Informationsutbytet bör vara dubbelriktad, men även balanserad, bundet till användningsändamålet och baserat på rätten att få information och på intresset av att byta information mellan parter som behöver den. Det bästa resultatet för informationsutbytet kan uppskattas bli nått i en situation där lagstiftningen gör det möjligt att övergå från tänkande baserat på informationsbehov (need to know) till tänkande baserat på

behov av att dela information (need to share). Det innebär att tillhandahållaren eller innehavaren av information på eget initiativ kan identifiera och ge informationen till en behörig myndighet. Detta förutsätter en bedömning av i vilken utsträckning ett behovsbaserat informationsutbyte är möjligt med tanke på de grundläggande rättigheterna, särskilt när det exempelvis gäller förmedlingsuppgifter.

Inom de ramar som lagstiftningen fastställer förutsätter ett effektivt utbyte av relevant information att den part som delar information identifierar vilken information den som behöver information eventuellt behöver. En tydlig lagstiftning förutsätter en granskning av processerna för informationsutbyte, en specificering av en myndighets kärnverksamhet i cybermiljön och kännedom om myndigheternas informationsbehov. Specificeringen bör ske separat för varje organisation, och varje organisation bör specificera sina databehandlingsprocesser.

Förhållandet mellan behovet av att skydda information och vikten av att dela information bör beaktas vid informationsutbytet. Begränsningar som den ursprungliga informationslämnaren kan fastställa för databehandlingen ska kunna beaktas vid lagstiftningen. På så sätt är det möjligt att behandla information konfidentiellt och att bevara förtroendet mellan olika aktörer samt nödvändiga rättsmedel. Ett exempel på en sådan begränsning kan eventuellt vara att information som har lämnats ut inte får användas som bevis i en straffprocess.

Den så kallade brandväggsregleringen i lagstiftningen om underrättelseverksamhet kan tas upp som en särskild fråga om metoder för underrättelseinhämtning med tanke på bekämpningen av cyberbrottslighet och lägesbilden av cyberbrottslighet. Brandväggsregleringen ger möjlighet att i vissa lagstadgade situationer i syfte att bekämpa brott lämna ut information som har skaffats genom metoder för underrättelseinhämtning. Brandväggsregleringen bör ses över så att den även gör det möjligt att lämna ut tillräcklig information till brottsbekämpningsmyndigheterna i syfte att förebygga cyberhot.

Den befintliga brandväggsregleringen och andra liknande begränsningar bör utvecklas så att det är möjligt att fastställa begränsningar för användning av information i straffrättsliga processer, men så att förundersökningsmyndigheten ändå kan använda informationen bland annat vid upprätthållande av den allmänna ordningen och säkerheten eller vid förebyggande och bekämpning av fientlig verksamhet från en annan stat. I sådana situationer kan dock undantag från förbudet att använda underrättelseinformation till exempel utgöras av situationer där informationen kan anses vara till fördel för den åtalade. Brandväggsregleringen bör dock alltid tillåta delning av information om statliga aktörer för att avvärja hot, eftersom en straffprocess i praktiken inte inleds mot en statlig aktör.

För att det ska vara möjligt att använda information i olika myndighetsfunktioner i syfte att utreda och förebygga omfattande helheter, är det viktigt att användningen av information som har tagits emot till exempel inte har begränsats till bara en utredning av ett enskilt fall eller en enskild kränkning.

För att ett effektivt informationsutbyte mellan myndigheter ska vara möjligt behövs det för hantering av cyberhot också ett myndighetsgemensamt system för utbyte av information i hög säkerhetsklass.

Med tanke på den övergripande cybersäkerheten i samhällets kritiska funktioner är det likväl viktigt att det är möjligt att med beaktande av säkerhetsklassificeringen av informationen dela information om informationssäkerhetsincidenter och avvikelser på ett effektivare sätt än i dag, även till de företag som är kritiska med tanke på försörjningsberedskapen, välfärdsområdena, kommunerna och de kommunägda tjänsteleverantörerna.

Bättre hänsyn till informationsutbytet i avtalsvillkor förutsätter samarbete mellan myndigheter när det gäller att fastställa avtalsvillkor och avtalsprocesser. I denna fråga uppdaterar informationshanteringsnämnden för närvarande kraven på informationssäkerhet vid upphandling. I samband med uppdateringen kan myndigheterna bland annat lyfta fram sina behov vad gäller cybersäkerheten. Dessutom kan det med beaktande av gällande lagstiftning förutsättas att privata aktörer gör en första anmälan till Transport- och kommunikationsverket och till den myndighet som är avtalspartner.

Vid upphandling bör upphandlaren också alltid utreda om upphandlingen kan göras som försvarsupphandling eller säkerhetsupphandling, varvid förutsättningarna att ställa kvalitetskriterier är mycket bättre än vid vanlig upphandling.

5.5 Påverkan och motåtgärder

Cyberpåverkan kan anses avse åtgärder som genomförs i eller via informationssystem eller informationsnät och som påverkar informationssystem eller enheter som ansluts till program, informationsnät eller informationssystem eller data, utrustning, deras funktion eller personer i informationsnät eller informationssystem. Syftet med cyberpåverkan är att förhindra, avbryta, begränsa, eliminera, försvaga eller störa objektets verksamhet eller att förstöra, manipulera eller vilseleda kapaciteten för den som är föremål för påverkan att bedriva sin verksamhet.

Bekämpningen av cyberattacker och cyberpåverkan förutsätter kapacitet att vidta motåtgärder för att minska eller helt förhindra konsekvenser av attackerarens fientliga åtgärder. Genom motåtgärder höjs tröskeln att göra attacker och vid behov försämras attackerarens verksamhetsförutsättningar redan före egentliga attacker. Motåtgärderna bör kunna dimensioneras i förhållande till de förväntade eller realiserade konsekvenserna av fientlig verksamhet.

Verksamhet som riktas till en teknisk miljö hanteras genom informationssäkerhetsåtgärder i den egna informationstekniska miljön. Om det samtidigt är fråga om ett brott, används också de brottsbekämpningsmetoder som behövs. Om en fientlig verksamhet handlar om en verksamhet som bedrivs av en stat, är möjliga motåtgärder sådana utrikes- och säkerhetspolitiska åtgärder som skyddar den nationella säkerheten och som efter prövning från fall till fall kan omfatta allt från diplomatiska metoder till militära metoder.

Transport- och kommunikationsverket kan vidta nödvändiga informationssäkerhets-åtgärder för att upptäcka, förhindra och utreda betydande informationssäkerhets-kränkningar som med hjälp av fi-domännamn riktas mot allmänna kommunikationsnät eller kommunikationstjänster eller användare av dem samt för att göra sådana kränkningar föremål för förundersökning. Åtgärderna kan bland annat omfatta åtgärder för att förhindra eller begränsa trafik som riktas till ett domännamn och för att dirigera trafiken till ett domännamn till ett annat domännamn. Dessutom har Transport- och kommunikationsverket rätt att i enskilda fall besluta om korrigerande åtgärder på tele-kommunikationsutrustning som orsakar betydande skada samt om att utrustningen ska kopplas bort från det allmänna kommunikationsnätet. Cybersäkerhetscentret vid Transport- och kommunikationsverket har även rätt att ålägga ägaren eller någon annan innehavare av kommunikationsnätet koppla bort telekommunikationsutrustningen från de kritiska delarna av sitt nät, om den nationella säkerheten och försvaret äventyras.

För att förebygga skador och följder av brott kan polisen beslagta fysiska enheter, med teleövervakningsbefogenhet avbryta datatrafiken för en viss tid och bestämma att distributionen av webbmeddelanden med olagligt innehåll ska avbrytas. Genom åtgär-derna kan polisen eventuellt påverka och ingripa i enskilda enheter eller program och i information som enheten eller programmet innehåller, men inte i en systematisk brottslig verksamhet i en nätverksmiljö som en helhet. Även om befogenheterna är tillämpliga, stämmer deras begreppsapparat och de situationer där befogenheterna enligt motive-ringen tillämpas inte överens med kraven på dagens cybermiljö. När gällande lag om polisens befogenheter stiftades, kunde särdragen och mångfalden i den utvecklande cybermiljön inte beaktas och identifieras i den omfattningen att lagstiftningen ens i tolkningspraxis motsvarar nuläget.

Situationen är en annan, om en enhet eller ett program som en stat har använt för cyberspionage eller cyberpåverkan finns utomlands. I princip försöker man ingripa i sådana situationer genom internationell rättshjälp, internationella samarbetsnätverk eller till exempel genom ovan beskrivna diplomatiska metoder. Om ursprungslandet inte vill ingripa i den skadliga verksamheten eller enligt sin tolkning inte har behörighet och en praktisk möjlighet att ingripa, är de finska myndigheternas möjligheter att agera begränsade. Myndigheterna kan inte använda sina befogenheter i en annan stats territorium. Ett undantag utgörs av underrättelsemyndigheterna, som också kan tillämpa underrättelsemetoder för att inhämta information i länder utanför Finland.

Om skador till följd av ett brott kommer fram i andra länder än i Finland och Finland har varit land via vilket skadlig verksamhet i cybermiljön har bedrivits, kan Finland som stat även anses ha omsorgsplikt enligt reglerna i folkrätten. Det innebär att Finland inte i sitt territorium kan tillåta verksamhet som orsakar betydande skada för andra staters rättigheter.

Inom Försvarsmaktens cyberförsvar bygger befogenheten att avbryta fientlig cyberpåverkan framför allt på fastställandet av användning av militärt våld. Sett till folkrätten har användning av militärt våld och användning av vapenmakt i cybermiljön inte kunnat definieras på ett heltäckande och enhetligt sätt. När det gäller Försvarsmakten är det dessutom oklart vad befogenhetsgrunden för att avbryta cyberpåverkan avser i fråga om cyberpåverkan som nationellt står under definitionen av tröskeln för ett väpnat angrepp. Lagstiftningen om Försvarsmakten kan också anses innehålla brister i fråga om att bereda åtgärder som syftar till att förhindra eller avbryta cyberspionage och cyberpåverkan samt i fråga om skydd av egen verksamhet och rekognoscering som har ett direkt samband med avbrytande av fientlig cyberpåverkan.

Utvecklingsförslag

För att sköta sina lagstadgade uppgifter bör olika myndigheter ha rätt att inom de ramar som folkrätten fastställer förhindra och avbryta fientlig cyberverksamhet som utgör ett allvarligt hot mot den nationella säkerheten och försvaret i Finland. Dessutom bör myndigheter ha en mer flexibel möjlighet att delta i gemensamma insatser med myndigheter i andra stater för att avbryta olaglig verksamhet. De delaktiga myndigheterna bör även ha rätt att tillämpa de metoder som behövs i det nämnda syftet.

Polislagen bör förses med bestämmelser om rättigheter och befogenheter som behövs för att förhindra och avbryta funktionen i enheter eller program som används för systematiskt och uppsåtligt cyberspionage eller för fientlig cyberpåverkan som undergräver den nationella säkerheten i Finland. Syftet med åtgärden bör vara att förhindra eller avbryta ett hotande eller pågående brott eller en annan farlig gärning eller händelse. Polisen bör

även ha rätt att ta kontroll över dirigeringsadresser som har använts i skadeorsakande verksamhet, det vill säga webbadresser till kommandoservrar. Med befogenheten är det möjligt att allt bättre utreda brott som till exempel har samband med uppbyggande av botnät. Dessutom är det möjligt att förebygga nya brott och skador som en kriminell aktör med hög sannolikhet kommer att orsaka med hjälp av sin kommandoserver och det fjärrstyrda nät som aktören har byggt upp. På så sätt kan myndigheterna också bättre få information om skadelidande målsägande.

Författningsgrunden för Försvarsmaktens cyberförsvar bör förtydligas genom lagstiftning om Försvarsmaktens cyberförsvar. Det skulle skapa allt bättre förutsättningar att integrera cyberförsvaret i det nära samarbetet mellan olika sektorer, myndigheter och övrigt samhälle. Befogenhetsgrunden för att avbryta fientlig cyberverksamhet och inhämta information i samband med avbrytandet samt för att skydda den egna verksamheten bör utfärdas så att Försvarsmaktens kapacitet också kan användas, om tröskeln att använda militärt våld, enligt gällande tolkningspraxis i folkrätten, inte anses bli överskriden.

Tillräckliga verksamhetsförutsättningar och möjligheter i olika beredskapsförhållanden bör säkerställas för cyberförsvaret vid bekämpning av olika hot i samarbete med andra myndigheter och aktörer, så att Försvarsmakten vid behov kan bistå andra myndigheter med sin kapacitet.

5.6 Inhämtning av information om allvarliga cyberhot

Den information som har erhållits genom informationsinhämtning i cybermiljön har en mycket stor betydelse för den övergripande säkerheten i samhället. Den informationen utgör en viktig källa för myndigheternas och statsledningens cybersäkerhetsbilder och uppfattning om cyberläget. Den utgör också viktiga indata för sådan informationssäkerhetsverksamhet och annan verksamhet, inbegripet HAVARO och underrättelseinhämtning avseende datatrafik, som upptäcker cyberkränkningar av kritiska informationsnät och viktiga kritiska samhällsaktörer och som skyddar näten och aktörerna mot cyberkränkningar. Den information om hot och statliga aktörer bakom hoten som har erhållits genom informationsinhämtning i cybermiljön är också en förutsättning för attribution och stopp för fientlig verksamhet genom motåtgärder.

Information om allvarliga cyberhot inhämtas från Cybersäkerhetscentrets HAVARO-system som bygger på frivillighet. Dessutom kan informationsinhämtningen i cybermiljön ske i form av civil och militär underrättelseinhämtning eller inom ramen för förundersökning för att utreda cyberbrott eller inom ramen för åtgärder för att förebygga och avslöja brott. Därför är det ytterst viktigt att lagstiftningen motsvarar de faktiska behoven och möjliggör en tillräckligt effektiv informationsinhämtning i cybermiljön, men med beaktande av de

krav som har samband med begränsning av de grundläggande rättigheterna. Befogenheterna att inhämta information i cybermiljön ska även i verkligheten göra det möjligt att utreda statliga aktörer som ligger bakom cyberhot, aktörernas motiv samt skador och risker som aktörernas verksamhet orsakar, och att förbättra skyddet.

Myndigheternas informationsinhämtning i cybermiljön riktar sig vanligen till olika tekniska enheter, teleterminaler och informationssystem samt datatrafiken mellan dem. Tillämpningen av metoder riktas på grundval av att en viss enhet eller ett visst system utifrån observationer används vid cyberspionage eller någon annan fientlig verksamhet mot Finland. En central utmaning och ett hinder för en effektiv informationsinhämtning i cybermiljön är dock att myndigheten i det tillståndskrav som den ska lägga fram för domstolen måste lämna identifieringsuppgifter om den enhet som är föremål för informationsinhämtning. Lösningen fungerar inte i fråga om cyberspionage och cyberpåverkan från en stat eller utredning av brott. Orsaken är att, när domstolen har godtagit den första tekniska enheten som föremål för åtgärd, visar det sig att det bakom enheten finns tiotals eller till och med hundratals andra enheter som en främmande stat använder i kedjan för spionage eller fientlig påverkan mot Finland. Uppkopplingar och kedjor mellan enheter som en stat använder i fientlig cyberverksamhet uppkommer och försvinner mycket snabbt. Därför är det i nuläget inte möjligt att hos domstol ansöka om tillstånd till underrättelseinhämtning som riktas till dem inom tillgänglig tidsram. Av detta följer att kedjor som enskilda enheter bildar inte kan identifieras och informationsinhämtningen blir resultatlös.

Som en särskild observation av metoder för underrättelseinhämtning kan nämnas en sådan behandling av tekniska data som är relevant med tanke på riktandet av underrättelseinhämtning avseende datatrafik och som är bunden till en kortvarig tidsperiod. Data som har inhämtats utifrån behandlingen kan inte heller användas för att skapa sökvillkor som används vid ordinarie underrättelseinhämtning avseende datatrafik. Identifieringen och övervakningen av cyberhot försvåras i sin tur av en begränsande bestämmelse i gällande lagstiftning. Bestämmelsen tillåter endast tagning av kortvariga prov på en del av ett informationsnät. Begränsningen försämrar möjligheterna att upptäcka ändringar av dirigering och att i datatrafiken identifiera nya föremål för underrättelseinhämtning, såsom cyberhot.

I Finland innehas informationsnätstrukturen av privata företag. Därför är de företagens medverkan nödvändig för att använda vissa underrättelseinhämtningsmetoder och informationsinhämtningsbefogenheter som har föreskrivits för myndigheter. Av den anledningen föreskriver polislagen om skyldighet för teleföretag att biträda myndigheter genom göra de kopplingar i ett telenät som behövs för teleavlyssning och teleövervakning samt genom att tillhandahålla polismyndigheten de uppgifter och redskap samt den personal som behövs för utförande av teleavlyssningen. Med teleföretag avses företag

som tillhandahåller nättjänster eller kommunikationstjänster till en användargrupp som inte har begränsats på förhand. Information om de teleföretag som är verksamma i Finland har samlats in i Transport- och kommunikationsverkets televerksamhetsregister. Enligt polislagen har ett teleföretag rätt att få ersättning för att företaget har biträtt myndigheter. Motsvarande skyldigheter vid militär underrättelseverksamhet föreskrivs i lagen om militär underrättelseverksamhet.

TEKL föreskriver om skyldigheter för teleföretag när det gäller att utföra och möjliggöra teleavlyssning och teleövervakning. Enligt TEKL ska allmänna kommunikationsnät och kommunikationstjänster samt kommunikationsnät och kommunikationstjänster som ansluts till dem planeras, byggas och underhållas så att teleavlyssning och teleövervakning kan utföras samt begäranden som gäller myndigheters rätt att få information kan tillgodoses i enlighet med vad som föreskrivs särskilt. TEKL föreskriver om krav på att biträda myndigheter i anslutning till funktionella kvalitetskrav och tekniska krav på teleavlyssning och teleövervakning. Dessutom föreskriver TEKL om skyldighet för teleföretag att till myndigheter lämna ut information som är relevant för teleavlyssning och teleövervakning och som myndigheten enligt vad som föreskrivs särskilt har rätt att få.

Som metoder har teleavlyssning och teleövervakning en stor betydelse för inhämtningen av information om statliga cyberhot. Med tanke på metodernas praktiska användbarhet är det dock ett betydande och nästan dagligt problem att skyldigheten att biträda och rätten att få ersättning för att biträda, som det framgår ovan, har föreskrivits enbart för konventionella teleföretag. I dagens samhälle är gruppen av kommunikationsförmedlare betydligt större och mer heterogen. Vid bekämpning av statliga cyberhot ska till exempel företag som tillhandahåller datahalltjänster ha en mycket viktig roll i att biträda vid teleavlyssning och teleövervakning och en allt större roll i och med att kommunikationstekniken vidareutvecklas. De omfattas emellertid inte av skyldigheten att biträda myndigheter i att utföra teleavlyssning och teleövervakning och inte heller av rätten att få ersättning för att vidta biträdande åtgärder.

Utvecklingsförslag

Myndigheternas kapacitet att upptäcka, identifiera och vid behov specificera fientlig statlig eller brottslig verksamhet i cybermiljön bör utvecklas för att skadlig verksamhet ska kunna förhindras, konsekvenserna minimeras och fortsatta åtgärder för att hantera skadlig verksamhet utvärderas. Detta förutsätter framför allt att befogenheterna att inhämta information och metoderna för underrättelseinhämtning utvecklas så att de är förenliga med de krav som verksamhetsmiljön i dag och den förväntade utvecklingen ställer.

De olika myndigheternas befogenheter att inhämta information bör vara mer oberoende av teknik för att den ytterligare information som behövs om obehörig verksamhet ska kunna inhämtas i syfte att ingripa i verksamheten.

Specifikationerna och uppgifterna för underrättelseinhämtning och informationsinhämtning i cybermiljön bör preciseras vid sidan av uppdateringen av befogenheterna att inhämta information. För att alla relevanta cybersäkerhetsmyndigheter ska ha en allt tydligare befogenhetsgrund för informationsinhämtning, bör lagstiftningen förses med allt tydligare bestämmelser om strategisk underrättelseverksamhet med befogenheter till militär eller civil underrättelseinhämtning i cybermiljön i anslutning till olika myndigheters uppgifter och om Försvarsmaktens underrättelseverksamhet som har samband med cyberpåverkan.

När myndigheternas rättigheter att få information och metoderna för att inhämta information utvärderas, ska hänsyn i allmänhet även tas till de krav som beror på de grundläggande fri- och rättigheterna och de mänskliga rättigheterna. När man till exempel försöker observera en statlig aktörs skadliga datatrafik, behandlas vanligen också annan datatrafik. Enligt gällande tolkning åtnjuter skadeprogrammen och de statliga aktörerna inte likadant integritetsskydd som till exempel kommunikationen mellan privatpersoner. Att åtskilja en statlig aktörs datatrafik och å andra sidan att göra en attribution är inte alltid så okomplicerat att det ska kunna genomföras ända från början. Förhållandet mellan dem och till exempel konfidentialiteten vid kommunikation och genomförandet av rättsmedel bör därför utvärderas i samband med lagändringarna. Även garantierna för rättssäkerhet och betydelsen av tillsynen över myndigheternas verksamhet betonas när ändringar som rör informationsinhämtningen i cybermiljön bereds.

Kedjekopplingarna av de attacksenheter som används vid cyberspionage och fientlig påverkan mot Finland förändras snabbt, vilket utgör ett problem med att rikta informationsinhämtning. Vid riktandet, som är ett villkor för tillstånd att inhämta information, bör enheterna kunna beaktas som en logisk helhet vid sidan av enskilda teleterminaler, teleadresser och personer.

Tillståndskravet för en metod för underrättelseinhämtning bör till exempel kunna förses med specifik information om den enhet eller programvara eller det system som har märkts ingå i en ovan avsedd helhet. När utgångspunkten för kedjan har specificerats, skulle det redan kunna ge underrättelsemyndigheten rätt att rikta informationsinhämtningen till de enheter och virtuella program och system som för att spionera eller utöva fientlig påverkan kommunicerar eller har bildat en kedja med utgångspunkten.

Information som har inhämtats vid behandlingen av tekniska data om datatrafik har en direkt inverkan på den informationsinhämtning som sker genom underrättelseinhämtning avseende datatrafik och särskilt på riktandet av informationsinhämtningen. Gällande lagstiftning bör utvärderas utifrån erhållna erfarenheter, och när det gäller befogenheten i lagstiftningen bör andra begränsningar än enbart en tidsram övervägas. Dessutom bör insamlade tekniska data kunna utnyttjas bättre än i gällande lagstiftning vid riktande av underrättelseinhämtning till en noggrannare nivå än bara till delar av informationsnät och ändringar i dem.

5.7 Skydd för myndighetsnät

Med myndighetsnät avses framför allt det gemensamma kommunikationsnät som har byggts upp för de centrala myndigheterna med ansvar för säkerhet. Ur ett bredare synvinkel kan myndighetsnät även avse centraliserade informations- och kommunikationstekniska tjänster som har byggts upp eller separerats för myndigheterna inom den offentliga förvaltningen. Bestämmelser om myndighetsnät finns i bland annat TUVE-lagen, TORI-lagen och TEKL.

I de myndighetsnät som har separerats för myndigheternas bruk behandlas en stor mängd information som behövs i myndigheternas verksamhet och även information som gäller medborgarna. Skyddet för myndighetsnäten och för den information som behandlas i näten kräver betydande resurser och samarbete mellan leverantörer och användare av gemensamma tjänster i myndighetsnäten, andra myndigheter och företag som tillhanda-håller kommersiella informationssäkerhetstjänster. Hot mot myndighetsnät kan bedömas vara större än hot mot allmänt tillgängliga tjänster. Det finns anledning att anta att statliga aktörer riktar anpassade operationer med stora resurser mot myndighetsnät. Vanligen är det inte möjligt att upptäcka sådana operationer genom att använda kommersiella standardlösningar.

Myndigheternas befogenheter enligt gällande lagstiftning möjliggör endast i begränsad omfattning ett effektivt samarbete och informationsutbyte mellan myndigheterna för att skydda myndighetsnät. Försvarsmakten, polisen, Gränsbevakningsväsendet och Transport- och kommunikationsverket är till exempel enligt TUVE-lagen på begäran av finansministeriet skyldiga att i möjligaste mån ge handräckning i syfte att garantera en störningsfri funktion i säkerhetsnätet. Handräckning har dock alltid en tillfällig oh villkorlig karaktär och utifrån den kan ett kontinuerligt samarbete inte byggas upp. Dessutom är det utan uttrycklig lagstiftning inte möjligt för den som ger handräckning att baserat på handräckning lämna ut eventuella sekretessbelagda uppgifter till den som begär handräckning.

I finansministeriets utredningar om förbättring av skyddet av informationssäkerheten i säkerhetsnätet har ministeriet lyft fram den möjlighet som skulle föreskrivas för Försvarsmakten att delta i tryggandet av cybersäkerheten i säkerhetsnätet. Det bör också noteras att tjänsteleverantörerna av myndighetsnät vid behov fritt kan skaffa informationssäkerhetstjänster från privata tjänsteleverantörer, men inte från andra myndigheter.

I nuläget är ansvaret för skyddet av myndighetsnäten och av den information som behandlas i myndighetsnäten fördelat på tjänsteleverantörerna och de myndigheter som använder tjänsterna. I fråga om dataskydd och informationssäkerhet har ansvaret också fastställts i avtalen om användning av tjänsterna och utifrån den allmänna lagstiftningen om informationssäkerhet. En närmare analys per tjänst bör dock göras när det gäller frågor om fördelningen av ansvaret för dataskyddet och hanteringen av informationssäkerheten för leverantörerna av de gemensamma tjänster som fastställs i TUVE- och TORI-lagarna och å andra sidan för de myndigheter som använder tjänsterna. Valtoris uppgifter är i sin tur också förknippade med frågan om behandling av personuppgifter, som i nuläget är oklar.

Utvecklingsförslag

I en utredning som finansministeriet och Försvarsmakten gjorde 2019 konstaterades det att det skulle vara ändamålsenligt att även föreskriva Försvarsmakten en roll som leverantör av informationssäkerhetstjänster för säkerhetsnätet, en roll som skulle ge Försvarsmakten möjlighet att tillhandahålla de informationssäkerhetstjänster som behövs för att skydda säkerhetsnätet. Uppgifterna skulle bland annat omfatta de åtgärder som beskrivs i TEKL för att genomföra informationssäkerheten i de gemensamma tjänster som tjänsteleverantören av myndighetsnät administrerar och i de enheter som är anslutna till tjänsterna samt, enligt särskild överenskommelse med den berörda myndigheten, i myndighetens informationssystem och enheter. Dessutom skulle uppgifterna omfatta analys av data om kränkningar av och hot mot informationssäkerheten i syfte att skydda säkerhetsnätet och tjänsterna för användare av säkerhetsnätet mot informationssäkerhetshot och i syfte att upprätthålla lägesmedvetenheten om funktionen och informationssäkerheten för tjänsterna i säkerhetsnätet. För att fastställa uppgifterna behövs det även ytterligare bedömningar av bland annat hur de planerade åtgärderna står i relation till de befogenheter som avses i TEKL och om det eventuellt behövs en kompletterande lagstiftning.

I fråga om säkerhetsnätet bör behovet av att i TUVE-lagen separat föreskriva om informationsutbytet mellan leverantörer av tjänster för säkerhetsnätet, användarorganisationer och Försvarsmakten kartläggas, även med beaktande av möjligheten att lämna ut meddelanden som innehåller förmedlingsuppgifter och skadeprogram, eftersom sådana meddelanden inte kan lämnas ut utifrån den allmänna rätten att lämna ut

uppgifter. Vid sidan av utvecklingen av myndigheternas informationsutbyte som behövs för att skydda myndighetsnät ska nödvändiga lagstiftningsmässiga åtgärder inledas för att göra det möjligt att byta information, ta fram en cyberlägesbild och behandla data om hot i syfte att förbättra samarbetet mellan myndigheter och kommersiella företag som tillhandahåller informationssäkerhetstjänster, informationstekniktjänster och kommunikationstekniktjänster.

De skyldigheter och rättigheter att byta information som har samband med hanteringen av informationssäkerheten vid Valtori bör preciseras och föreskrivas genom lagstiftning. Översynen bör även omfatta förverkligande av skydd av konfidentiell kommunikation, skydd av personuppgifter och integritetsskydd samt framför allt precisering av de därtill hörande behandlingsrättigheterna i olika roller i säkerhetsnätverksamheten. Tjänsterna för att hantera informationssäkerheten vid Valtori bör samtidigt preciseras och beskrivas genom servicebeskrivningar.

6 Slutsatser

Utifrån arbetsgruppens utredningsarbete kan utvecklingsåtgärderna nedan förbättra myndigheternas verksamhetsförutsättningar att skydda den nationella cybersäkerheten, bekämpa allvarlig cyberbrottslighet och utveckla cyberförsvaret så att det uppfyller de krav som den avancerande cybermiljön har ställt.

6.1 Utvecklingsåtgärder som ska genomföras i snabb takt

1. En strategisk målbild fastställs
   - Strategin för cybersäkerheten i Finland omarbetas. Strategin fastställer en nationell målbild och beaktar förändringar i säkerhetsmiljön, uppfyller kraven i EU-lagstiftningen och fastställer mål för det samarbete som drivs inom ramen för EU och Nato.
   - En cyberförsvarsdoktrin utarbetas som en del av strategiarbetet.

2. Myndigheternas samarbete och processer förbättras
   - En bestående struktur för myndighetssamarbete skapas på ämbetsverksnivå mellan statsrådsnivå och teknisk sakkunnignivå.
   - Samordnandet av samarbetet mellan myndigheterna förtydligas, informationsutbytet utvecklas och de olika myndighetsprocesserna i cybermiljön beskrivs och etableras.

3. Framtagningen och utdelningen av lägesbilden effektiviseras
   - En myndighetsprocess för kontinuerlig framtagning och utdelning av lägesbild utvecklas och etableras.
   - Anmälning av informationssäkerhetsincidenter fogas bättre till avtalen med privata tjänsteleverantörer.
   - Delningen av information om allvarliga cyberhot, informations-säkerhetsincidenter och avvikelser effektiviseras på ett ändamålsenligt sätt, även till de företag som är kritiska med tanke på försörjningsberedskapen, välfärdsområdena, kommunerna och de kommunägda tjänsteleverantörerna, med beaktande av säkerhetsklassificeringen av informationen.

- Aktörer som tillhandahåller vitala funktioner för samhället, inklusive deras leveranskedjor, identifieras.

4. Informationsutbytet mellan myndigheterna utvecklas i samarbete till en dubbelriktad verksamhet som är bunden till sitt ändamål och bedrivs mellan organisationer inom ramen för gällande lagstiftning.
   - De befintliga verksamhetsmodellerna och processerna vidareutvecklas.
   - En utvärdering görs angående betydelsen av begränsningarna för informationsutbytet mellan myndigheterna i den förändrade säkerhetsmiljön, innehållet i de centrala begreppen i lagar, ramvillkoren för tolkning av begreppen och eventuella behov av ändringar.
   - Ett gemensamt kommunikationssystem som är lämpligt för delning av information i hög säkerhetsklass skapas.

5. Uppdatering av ordlistan om cybersäkerhet inleds.

6.2 Utvecklingsåtgärder som kräver lagändringar

Arbetsgruppen föreslår följande utvecklingsåtgärder som kräver lagändringar:

6. Effektivisering av informationsutbytet i fråga om skyddet för cybermiljön
   - Det rekommenderas att regeringens förfallna proposition (RP 243/2022 rd) för att främja samarbetet mellan myndigheterna vid allvarliga kränkningar av informationssäkerheten överlämnas på nytt.
   - En samordnad framtagning, analys och delning av information från Försvarsmakten, polisen, Skyddspolisen och Transport- och kommunikationsverket möjliggörs i syfte att skapa en gemensam lägesuppfattning.
   - En mer omfattande användning av data från HAVARO kartläggs.
   - En bedömning görs angående behovet av lagändringar som en effektiv verksamhet i den i punkt 2 angivna bestående strukturen för myndighetssamarbete eventuellt kräver.
   - Delningen mellan myndigheterna av information som har lämnats ut med stöd av anmälningar om kränkning av informationssäkerheten förbättras ytterligare.
   - Det utreds om den lagstadgade skyldigheten för konventionella teleföretag att biträda myndigheter mot ersättning kan utvidgas till att omfatta andra betydande tjänsteleverantörer.

7. Utmaningarna med cybermiljön beaktas redan vid den pågående reformen av beredskapslagstiftningen.

8. Förbättring av cybersäkerheten för myndighetsnät och gemensamma tjänster
   - Förutsättningar för att skydda säkerhetsnätet skapas så att myndigheter som är lämpliga för att skydda nätet, såsom Försvarsmakten, kan delta i skyddet.
   - Hänsyn tas även till förbättringen av skyddet för Valtoris TORI-tjänster, och skyldigheterna och rättigheterna att byta information som har samband med hanteringen av informationssäkerheten vid Valtori preciseras.

9. Polisens verksamhetsförutsättningar i cybermiljön
   - Polisens befogenheter och förutsättningar att byta och lämna ut information utvärderas.
   - En bedömning görs angående begränsning av skyldigheten att göra förundersökning och rätten att inte göra förundersökning eller att lägga ned förundersökning i vissa situationer.
   - Förutsättningar skapas för informationslämnaren att fastställa begränsningar för vidareanvändning av information.
   - Hänsyn tas till de förslag i utredningen om kriminalunderrättelseinhämtningen som rör cybermiljön.

10. Försvarsmaktens verksamhetsförutsättningar i cybermiljön
   - Lagar som möjliggör Försvarsmaktens cyberförsvarsuppgifter stiftas, vilket inbegriper tillräckliga befogenheter och förutsättningar att byta och lämna ut information.
   - Försvarsmaktens handräckning och biträde i vissa situationer till aktörer som tillhandahåller vitala funktioner för samhället utvecklas.
   - Hänsyn tas till behovet av lagändringar som Natomedlemskapet och det kollektiva försvaret förutsätter.

11. Underrättelsemyndigheternas verksamhetsförutsättningar i cybermiljön
   - Underrättelsemyndigheternas cyberbefogenheter utvärderas. Som en del av bedömningen skapas förutsättningar att rikta metoder för underrättelseinhämtning till enheter och virtuella system som en helhet.
   - Brandväggsregleringen utvecklas så att tillräcklig information kan ges till brottsbekämpningsmyndigheterna i syfte att skydda den nationella säkerheten.
   - Behandlingen av tekniska data vid underrättelseinhämtningen avseende datatrafik utvecklas.

12. En utvärdering görs angående de lagändringar som behövs för att öka myndigheternas möjlighet att biträda i beredskapen och återhämtningen efter allvarliga störningar till följd av cyberincidenter i företag som är kritiska med tanke på samhällets funktion och försörjningsberedskapen.

SNELLMANSGATAN 1 A, HELSINGFORS
PB 23, 00023 STATSRÅDET
valtioneuvosto.fi/sv/
julkaisut.valtioneuvosto.fi

ISBN: 978-952-383-534-4 PDF
ISSN: 2490-0966 PDF