Solidaritet som avskräckning mot cyber- och påverkansoperationer

Inträdesanförande i KKrVA avd VI den 13 oktober 2021 av Patrik Oksanen

Résumé

Cyberattacks and influence operations could severely hurt the targeted society, especially when one considers long term effects of the operations. But compared with activities conducted in the physical realm these attacks are not viewed as severe and do not lead to the same severe response from the attacked. This means that the attacker can continue its attacks without facing any real consequences. In his entrance speech to the Academy, Patrik Oksanen, argues for the need of using solidarity between likeminded countries in order to build a deterrence in this field. Solidarity means together applying consequences for the attacker. This does not mean this is the only means of building societal resilience to withstand attacks but should be viewed as one of several tools that are needed to be developed as soon as possible. Countermeasures from other countries, showing solidarity with the attacked partner, could range from public naming and shaming simultaneously with more conventional measures such as sanctions against individuals and companies that enable the attacks. This article argues that the solidarity pact should be developed first in the smaller Nordic-Baltic (NB8) family and then be open for other democracies to join.

OM RYSKA SPECIALFÖRBAND med vapen i hand hade stormat norska stortinget i augusti 2020 så hade Sveriges svar varit givet. Sedan 2009 års inriktningsproposition för försvaret, som innehöll försvarsberedningens solidaritetsförklaring, har Sverige sagt att:

> Sverige kommer inte att förhålla sig passivt om en katastrof eller ett angrepp skulle drabba ett annat medlemsland (i EU) eller nordiskt land. Vi förväntar oss att dessa länder agerar på samma sätt om Sverige drabbas.[1]

De politiska reaktionerna hade också varit omfattande, för att inte tala om konsekvenserna. Natos artikel 5 hade troligen utlösts som en följd av angreppet.

I verkligheten stormade faktiskt ryska specialförband norska Stortinget i augusti 2020, men det skedde utan vapen. Den ryska militära underrättelsetjänstens operatörer var heller inte på plats i Oslo när de genomförde angreppet. De satt i Ryssland och tillhörde enligt medieuppgifter GRU:s enhet 26165. Samma enhet har pekats ut för cyberangrepp mot tyska förbundsdagen och Demokraternas e-post i USA 2016.

Det osynliga angreppet

En statsaktörs angrepp på den norska lagstiftande församlingen är ett angrepp mot demokratins hjärta, och syftet kan förstås som att underminera demokratin, förminska landets suveränitet och därigenom förmågan

att självständigt fatta sina beslut. Genom att angreppet skedde i cyberdomänen och inte var synlig för blotta ögat så ser vi det inte. Händelsen förblir abstrakt för de allra flesta.

Den norska regeringen gick den 13 oktober 2020 ut med ett pressmeddelande: ”Basert på det informasjonsgrunnlaget regjeringen besitter, er det vår vurdering at Russland står bak denne aktiviteten.” Jämfört med hur lång tid det brukar ta från ett cyberangrepp till attribuering var den norska handläggningen berömvärd och exceptionellt snabb.

Norges utrikesminister Ine Eriksen Søreide kommenterade för NRK angreppet med ”ei veldig alvorleg hending, og at det er viktig å halde Russland ansvarleg for angrepet. Å gå ut offentleg og legge skulda på Russland er ein del av ansvarleggjeringa.”[2] Dagen efter uttalade sig statsminister Erna Solberg: ”det er viktig at Noreg reagerer tydeleg når me opplever at andre land handlar feil”.[3]

Ett land uttalade öppet sitt stöd för Norge efter angreppet. Det var inte Sverige med sin solidaritetsdeklaration. Det var inte Danmark som Norge både delar Nordiskt Råd och Nato med. Det var inte USA. Det enda landet som reagerade officiellt på det ryska angreppet var ett land som själv sedan 2014 är i ett hybridkrig med Ryssland, där skalan går från militärt våld till falska twitterkonton. Ukrainas utrikesminister Dmytro Kuleba krävde att Ryssland måste hållas ansvarig för angreppet, samt i uttalandet påpekade han att ”Euroatlantisk solidaritet och ömsesidigt stöd är nyckeln för att möta utmaningar från hybridkriget”.[4]

Det norska fallet från 2020 illustrerar problembilden, att det tas ut en för låg kostnad av angriparen.

Så länge som det är riskfritt, utan konsekvenser och den totala kostnadskalkylen är låg kommer angreppen att fortsätta.

I krig – nu

Exemplet ovan handlade om Norge, men när det gäller cyber- och påverkansdomänen är det inte någon överdrift att konstatera att Sverige (och många andra demokratiska länder) redan idag befinner sig i strid med främmande makter, vare sig vi själva vill erkänna det eller inte.

Ett sätt att möta angreppen är genom solidaritet mellan likasinnade demokratiska stater. Att utveckla en ny mekanism istället för att använda EU beror dels på att EU-processen är för långsam och dels svårigheterna att nå en överenskommelse på grund av kraven på enhällighet inom utrikesområdet. Ytterligare skäl är att det här är en fråga som är större än EU-länderna, och mekanismen bör vara öppen för alla demokratiska stater att ansluta sig till. I Sveriges närområde handlar det om Norge, Island och Storbritannien.

Det här är inte det enda sättet att möta påverkansoperationer och cyberattacker från främmande makter. Förslaget ska ses som ett verktyg bland många flera, och att det behövs användas tillsammans med motståndskraftsstärkande åtgärder som förbättrad cybersäkerhet och utbildning av allmänhet och beslutsfattare om påverkansoperationer och deras syfte. Samtidigt fungerar solidariska motåtgärder också indirekt som motståndskraftsbyggande, de påminner den egna befolkningen om angriparens mål och metoder vilket bidrar till att bygga förmåga att hantera nästa attack.

Vilket tillstånd råder?

Viljan att kunna påverka sin motståndare är gammal, och går tillbaka till Sun Tzus läror för 2500 år sedan. Koncept kring vilseledning och påverka motståndarens vilja har operationaliserats både av Ryssland

och Kina. Sovjetunionen kom att göra doktrin av Maskirovka, som i Lars Ulfvings bok *Den Stora Maskeraden* – sovjetrysk militär vilseledning beskrivs som döljandets och vilseledandets konst. En tradition som kan spåras tillbaka till mongolväldet som förde med sig Sun Tzus tänkande västerut. Sun Tzu översattes också fyra gånger till ryska under 1800-talet.[5]

I Sun Tzus tänkande, som också är starkt i kinesisk militär tradition, beskrivs överlägsen skicklighet den som gör att fiendens motstånd bryts utan att man behöver strida. Kan man dessutom strida utan att motståndaren förstår det har man en viktig fördel.

Keir Giles på Chatham House påpekade 2016 att Rysslands agerande på informationsarenan tyder på att Ryssland ser sig själv varande i krig.[6] I *The Russian understanding of War* pekar Oscar Jonsson på att Ryssland ser hot från demokratirörelser och ”färgrevolutioner” som regimens största utmaning och att de är underblåsta från väst:

> The borderline between war and peace has been blurred, with the current confrontation already in the blurred area. It is only necessary for one party to see itself in the blurred area of war for the war to exist.[7]

Både Jonsson och Giles argumenterar att synsätten kring konflikten mellan väst och Ryssland är oöverbryggbara och måste hanteras genom denna insikt. Betydelsen av icke militära medel kommer att öka i takt med gränserna mellan krig och fred suddas ut ytterligare:

> This understanding underlies why Russia is more determined, more willing to take risks, and more proactive than a complacent West believing itself to be in a period of peace.[8]

Segra utan strid

Kina kom under Mao att använda sig av Sun Tzus lärdomar. I en rapport från US Army Command and General Staff College beskrivs det kinesiska kommunistpartiets påverkansarbete i inbördeskriget som mycket effektivt.

Mao hade ett koncept med tre faser i påverkansoperationerna som utgick från uppbyggnad i hemlighet i den första, i den andra som kan beskrivas som den strategiska jämviktsfasen gick man över till öppna operationer för att slutligen besegra motståndaren i den tredje. I den strategiska jämviktsfasen låg även tydlig prioritering på informationens infrastruktur.[9] Den som kontrollerar infrastruktur kan också kontrollera budskap. I dagens avancerade teknologiska samhälle uppvisar Kina stort intresse för informationsinfrastruktur. Det här gäller såväl 5G-utbyggnad som medieägande och arbetet att såväl legalt som illegalt skaffa sig en stor mängd data.

Folkets befrielsearmé (PLA) ser sig som en förlängning av kommunistpartiet och har åtminstone sedan 1963 haft riktlinjer för politisk påverkan mot utlandet. Det har bestått av att påverka allmän opinion, använda sig av psykologiska operationer och använda sig av juridiken i krigföringen. Syftet är att splittra motståndarens aktiviteter och hindra fiendens försök att skapa oenighet i Kina.[10]

Det som skapar helt nya möjligheter i att uppvisa överlägsen skicklighet i att segra utan strid i våra dagar är den digitala sfären. Den digitala utvecklingen har gått fort sedan den första moderna sökmotorn Alta Vista lanserades 1995.

De digitala storbolagen som Google och Facebook har förändrat både samhället och hur opinionsbildningen fungerar. I utredningen ”Det demokratiska samtalet i en digital tid” (2020:56) konstateras att 1993

skedde en procent av det globala informationsutbytet över internet, mot strax över 50 procent vid millennieskiftet och 97 procent 2007.[11]

Med digitaliseringen som grund har kostnaderna för att bedriva påverkansarbete sjunkit kraftigt. Mycket talar för att effekterna som kan uppnås också är mycket bättre än under det analoga samhället. Snabbheten samt faktorer som tid och rum minskar i betydelse är andra påtagliga effekter.

Sociala mediers algoritmer förstärker detta.

Falskt versus sant

Amerikanska sajten Buzzfeed visade exempelvis att falska historier fick mer spridning än sanna historier på Facebook under de tre sista månaderna för presidentvalet i USA 2016. Det mest notervärda är att skiftet skedde precis före valet. I februari-april, hade de 20 toppartiklarna i etablerad press cirka 12 miljoner i Facebookengagemang, alltså delningar, likes och kommentarer, mot de falska nyheternas tre miljoner.

Från augusti till valdagen vann de falska nyheterna med 8,7 mot 7,3 miljoner. De två mest spridda falska historierna handlade om att Hillary Clinton sålt vapen till Islamiska staten och ett påstående om att påven ställt sig bakom Donald Trump som presidentkandidat.[12] De falska nyheterna gynnade helt klart Trump, bara en av de tjugo mest delade falska historierna kan sägas ha varit negativ mot Trumpkampanjen.

När det gäller Twitter visade en studie som publicerades i tidskriften *Science* från MIT att falska nyheter hade bättre förutsättningar att spridas än sanna. Det var 70 procent högre sannolikhet för en falsk nyhet att retweetas än en sann. Det tog också sex gånger så lång tid för en sann historia att nå 1 500 personer som en falsk. Forskarnas slutsatser var att en falsk historia överraskar mer än en sann och därför spreds snabbare.[13]

WHO var tidigt ute och klassade informationsspridningen om Covid-19 som en infodemi, med en stor mängd falska historier kring viruset. Nu när vi är inne i vaccinationsfasen konstaterar flera forskare att det motstånd vi ser till stor del kan förklaras av sociala medier. Medieforskaren Whitney Philips argumenterar i boken *You are here* att vi behöver se sociala medier som ger spridning åt desinformation som företaget som släpper ut föroreningar.[14]

Oavsett hur vi väljer att se på sociala medieföretagen så är de centrala i att ge spridning åt desinformation. När Ryssland byggt upp det ekosystem, som bland annat har beskrivits av USA:s utrikesdepartementet i rapporten *Pillars of Russia's Disinformation and Propaganda Ecosyst*, så är sociala medier centrala för att skapa kraften i räckvidden.

I rapporten beskrivs hur det här ekosystemet fungerar med inslag av cyberoperationer, trollkonton, botar, proxysidor, statsmedier och regeringsutspel.[15] Till det ryska ekosystemet ser vi även hur ett symbiotiskt förhållningssätt till andra aktörer, som Kina utvecklas.[16] I det ryska ekosystemet så spelar också cyberangreppen en central roll för att skapa desinformation och påverka debatten.

Penetration, spridning och falsarier

Själva företeelsen, att ta sig in i andras datasystem, oavsett motivet bakom, är något som ökar stadigt. I januari 2017 sade FRA att man upptäckte 10 000 aktiviteter varje månad från statliga utländska angripare mot svenska mål. 2019 konstaterade FRA att det hade ökat, men ville inte längre ange en siffra.[17] Ett budskap som upprepats efter det; angreppen fortsätter att öka. En annan

indikation på ökningen vittnar företaget Truesec om, som gör dataforensiska undersökningar. I september 2021 konstaterade företaget att man hade närmast tredubblat uppdragen jämfört med året innan.[18]

Dessutom är det inte bara statsaktörer utan även kriminella aktörer som är verksamma. Dessa kriminella grupper kan verka med olika regeringars goda minne, och från tid till annan arbeta på uppdrag av staten, vilket gör det ännu svårare att särskilja vem som är vad i cyberdomänen och med säkerhet tillskriva en aktör ansvaret för angreppet. Samtidigt är kostnaden för samhället stora. Bara för svenska företaget beräknades 2020 kostnaden för cyberangrepp landa på cirka 20 miljarder kronor.[19]

I framtiden kan vi förvänta oss ännu kraftfullare verktyg, både för att penetrera datasystem och för att genomföra spridandet av desinformation. Till exempel genom att skrapa stora mängder med information, kombinerat med AI, så kan man framställa information som i sig inte behöver vara helt fel, men väl anpassat efter syfte. Därefter kan man i praktiken överrösta ett målområde med sådana berättelser helt eller delvist automatiserat och därigenom ta utrymme för debatt kring exempelvis att uppmärksamma hot från främmande makt.

När det gäller rörlig bild suddar Deep Fake teknologin ut gränserna för vad vi egentligen kan lita på när vi ser en film. Deep Fake skulle kunna innebära att statsministern dyker upp med en video i ett skymningsläge före kriget och meddelar att mobiliseringen ska upphöra och att svenska styrkor ska lägga ned sina vapen. Problemet för svenskt vidkommande är bara att statsministern aldrig sagt något sådant, utan att allt är producerat med hjälp av artificiell intelligens någon annanstans i världen. Ett annat exempel är att medieföretags sidor kan hackas så att de skriver det som den som ligger bakom attacken önskar.

Angrepp för att påverka

Allt det här gör att motmedel behöver utvecklas och konceptualiseras. Här spelar avskräckning en roll. Dagens uteblivna konsekvenser av angrepp får inte främmande makt att avstå från att fortsätta.

Fallet med det norska stortinget är bara en i raden av många, det finns betydligt fler från de senaste åren, där rysk underrättelsetjänst riktat angrepp mot västliga institutioner för att bedriva påverkan.

Det mest kända och välskrivna är förstås angreppet på det amerikanska presidentvalet 2016, men några fler närliggande fall, som åtminstone borde ha föranlett en diskussion kring gemensamt agerande när de upptäcktes, är värda att notera.

Ghostwriter är namnet på den ryska kampanjen som pågått åtminstone sedan 2017. Ghostwriter har beskrivits som att ett stort antal parlamentsledamöter, regeringsföreträdare samt journalister och civilsamhället i EU har attackerats i påverkanskampanjer genom cyberinbrott som gett hackarna tillgång till datasystem och personliga konton.[20] Detta har kombinerats med aktiviteter som att distribuera desinformation via falska artiklar och falska mediepersonligheter. Till exempel fabricerades en intervju med en amerikansk general som påstods kritisera baltiska och polska allierade.[21] En av de aktiviteter som Ghostwriter tillskrivs är att attackera tyska förbundsdagen.

I mars 2021 gick tyska myndigheter ut och berättade att sju förbundsdagsledamöter och 31 ledamöter vid regionala parlament utsatts för intrångsförsök. Samtidigt var det ett relativt snabbt utpekande jämfört med tidigare attacker. 2015 utsattes Tyskland för ett större angrepp, något den

tyska regeringen först fem år senare pekade ut Ryssland för.[22]

Även om Ryssland indirekt pekats ut av underrättelsekällor långt tidigare så var det först i maj 2020 som den tyska regeringen talade officiellt om attacken. Förbundskansler Angela Merkel sade att det fanns ”hårda bevis” för Rysslands ansvar för den attack som kallades för skandalös. Bland de drabbade kontona fanns Merkels egna parlaments konto. Stölden ska ha omfattat 16 gigabytes, det motsvarar omkring 320 000 A4-sidor. Förbundskanslern fördömde attacken, men det fick inga praktiska konsekvenser där och då.

Fallet med Riksidrottsförbundet

Sverige har också drabbats. I december 2017 till maj 2018 var GRU:s operatörer från enhet 26165 (alltså samma som i fallet med stortinget) inne i Riksidrottsförbundets system. Syftet var att kompromettera svenskt antidopningsarbete som en del i en större kampanj att relativisera rysk dopning på andra länders bekostnad.

Dokumenten som hämtades ut från Riksidrottsförbundet användes sedan av ryska statsmedier i en välregisserad kampanj för att skapa misstro mot svenska idrottare.[23] Svensk medierapportering hade påtagligt svårt att värja sig från angreppet i maj 2018 när GRU lade ut listor med läkemedelsdispenser och interna mejl från anställda på Riksidrottsförbundet

Därför blev inte nyheten att ryska militära underrättelsetjänsten GRU har stormat Riksidrottsförbundet utan istället hette det att ”ryska hackare” varit inne i Riksidrottsförbundets system. Det pratades i termer om ”starka krafter”. Sveriges Radio rapporterade att uppgifterna presenterats på ”en tidigare omdebatterad rysk sida”. *Expressens* sportredaktion kallade det för ”en rysk hackergrupp, som tidigare har fått uppmärksamhet”. I *Expressens* rapportering hamnar Riksidrottsförbundets antidopningsansvariga direkt i försvarsställning: ”Illa – men vi har ingenting att dölja”. Och ”det är inte okej att släppa den här typen av uppgifter”.

Det här misslyckandet för svenska medier och för Riksidrottsförbundet sker trots att det var uppenbart var uppgifterna kom ifrån. ”Den ryska hackergruppen” Fancy Bear var sedan länge identifierade som rysk militär underrättelsetjänst. Den kunskapen fanns öppet och publicerat sedan tidigare. Riksidrottsförbundets ordförande Björn Eriksson kunde inte heller förmå sig säga exakt vem som låg bakom. Istället beskrevs det som ”väl finansierade krafter” och att syftet är att skapa bilden av att alla fuskar. ”Det är så man jobbar med ”falska nyheter”, man slänger ur sig påståenden och försöker säga att i mörkret är alla katter grå”.[24]

2021 är alltså är utredningen klar, riksåklagare konstaterar att chansen att lagföra individer från ryska militära underrättelsetjänsten är för små och lägger ned förundersökningen. I ett pressmeddelande motiverade åklagaren Mats Ljungqvist beslutet:

> Mot bakgrund av att aktörerna agerar för en främmande makt, i detta fall Ryssland, gör vi bedömningen att förutsättningar för lagföring utomlands eller utlämning till Sverige saknas av de personer som misstänks ligga bakom intrånget.

Därigenom blev det ingen riktig konsekvens för attacken mot Riksidrottsförbundet. Åklagaren kunde ha gått till Interpol och efterlyst de misstänkta operatörerna. Om det varit omöjligt att namnge inblandade GRU-officerare genom utbytet av underrättelseinformation skulle ett åtal kunna rikta

sig högre upp i befälskedjan till den öppna delen av GRU.

Sveriges regeringen valde att reagera på händelsen genom att i samband med det nedlagda åtalet kalla upp den ryska ambassadören Viktor Tatarintsev till UD.

Lama reaktioner

Förutom bristande cybersäkerhet illustrerar både de tyska exemplen och Riksidrottsförbundets problem som oförmåga att tala klartext vilket gör att logiken bakom informationsattacken inte bryts. Lägg sedan till långa reaktionstider och bristen på konsekvenser för angriparen.

Detta sker trots att diskussionen om en avskräckande cyberpolitik funnits i flera i år. EU antog 2017 ett ramverk för ”Joint EU Diplomatic Response to Malicious Cyber Activities”. Ramverket tillåter EU och dess medlemstater att använda alla verktyg som EU:s gemensamma utrikes- och säkerhetspolitik erbjuder.

2020 fattade EU ett första beslut om sanktioner mot sex personer och tre organisationer från Kina och Ryssland som pekats ut som ansvariga för olika cyberattacker, som den mot OPCW (Organisationen för förbud mot kemiska vapen) och de attacker som är kända som WannaCry, NotPetya och Operation Cloud Hopper. Sanktionerna innebar reseförbud och frusna tillgångar. Det riktade sig dock inte emot Folkrepubliken Kina eller Ryska federationen som statssubjekt.[25]

I september 2021 kom Europeiska unionens höga representant för utrikes frågor och säkerhetspolitik Joseph Borell att hota Ryssland med sanktioner efter just tidigare nämnda Ghostwriter. I ett uttalande skrev Borell:

> Such activities are unacceptable as they seek to threaten our integrity and security, democratic values and principles and the core functioning of our democracies.

Ryssland uppmanades att upphöra med aktiviteterna omedelbart och Borell öppnade dörren för sanktioner mot Ryssland i uttalandet.

Hoten från cyberattacker och hybridkrig lyftes i den nordiska kretsen genom rapporten ”Nordic Foreign and Security Policy 2020” beställd av Nordiska ministerrådet. Rapportören Björn Bjarnason hade ett särskilt uppdrag i dessa frågor samt att titta på ”strengthening and reforming multilateralism and the rules-based international order.”[26]

I rapporten pekar Bjarnason på betydelsen att exponera skadliga informationsaktiviteter:

> However, closer collaboration between the Nordics should also entail standing together when Nordic countries or companies are threatened or attacked. This requires the willingness to expose malign and coercive information activities of states or other actors as well as safeguarding and publicly supporting both Nordic research communities and independent media.[27]

Och i en debatt i sommaren 2021 på Nordiska rådets digitala temasession gick Bjarnasson ännu längre och uttryckte sig tydligare om behovet av avskräckning:

> Cyberförsvarets avskräckande kraft ökar om man kan räkna med solidaritet mellan grannländer. Det har effekt om man möter kritik från fem länder i stället för från ett land.[28]

För att summera läget

- Cyberangreppen mot Sverige ökar från statsaktörer.
- Den tekniska medieinfrastrukturen gör det enklare än tidigare att sprida des-

information och genomföra påverkansoperationer.

- Demokratiska institutioner hos våra närmaste grannländer har attackerats.
- Frågan om angrepp från statsaktörer är uppe på politisk dagordning i EU och Nordiska Rådet, men ännu har det inte omvandlats i den konkreta solidaritetshandlingar.

I en tid när konfliktintensiteten i världen ökar, och aktörer som Ryssland och Kina ser på användandet av icke militära medel som en naturlig del för att främja sina intressen behöver Sverige ställa sig frågan hur solidaritetsdeklarationen och säkerhetspolitiken ska anpassas till den nya verkligheten.

Det enkla svaret är att titta på vad Sverige säger sig vilja göra generellt och utgå från det när cyberområdet inkluderas i säkerhetspolitiken. 2009 års överenskommelse i försvarsberedningen, som också slogs fast i inriktningspropositionen samma år är i detta bärande:

> Sverige kommer inte att förhålla sig passivt om en katastrof eller ett angrepp skulle drabba ett annat medlemsland (i EU) eller nordiskt land. Vi förväntar oss att dessa länder agerar på samma sätt om Sverige drabbas.

Samarbete är grunden för Sveriges breda säkerhet, och sträcker sig från naturliga katastrofer som översvämningar och skogsbränder till militära konflikter:

> Vi ska kunna och vilja hjälpa varandra i händelse av olyckor, kriser eller konflikter och med relevanta förmågor. Regeringen delar Försvarsberedningens slutsats att Sverige mot denna bakgrund bör ha förmåga att både ta emot och ge militärt stöd. Regeringen anser att dagens hot mot fred och säkerhet avvärjs bäst i gemenskap och samverkan med andra länder och organisationer. Effektivt multilateralt samarbete är därför ett grundelement i svensk säkerhetspolitik.

Eftersom cyber- och påverkansoperationer inte är reglerade i internationella konventioner så har västvärlden haft svårt att agera samfällt. När det gäller solidariskt agerande har det framför allt krävt fysiska och konkreta visuella överträdelser för att andra länder ska agera.

Således ledde den ryska militära underrättelsetjänsten GRU:s förgiftning av avhopparen Sergej Skripal och hans dotter Julia med det kemiska stridsmedlet novitjuk 4 mars 2018 i Salisbury till massutvisningar av ryska diplomater, som enligt utvisningsbeslut pekades ut som underrättelseofficerare.

I en samordnad insats kom USA att utvisa 60 diplomater. I EU-familjen utvisade Tyskland, Frankrike och Polen fyra diplomater vardera, Litauen och Tjeckien tre vardera, Danmark, Italien och Rumänien två medan en diplomat utvisades från Estland, Lettland, Kroatien, Finland, Ungern, Sverige och Rumänien. Utanför EU utvisade Ukraina 13 diplomater, Albanien två diplomater, Kanada fyra diplomater (samt att tre ryska diplomatansökningar avvisades) och Australien två diplomater.[29]

När Tjeckien våren 2021 gick ut och berättade att man kommit fram till att Ryssland var ansvarig för sprängningen av ett ammunitionsförråd 2014 blev reaktionen inte lika omfattande. Förutom att Tjeckien först utvisade 20 ryska diplomater, därefter 63, agerade bara ett fåtal länder i solidaritet.[30] Estland, Lettland, Litauen, Slovakien och Rumänien agerade till förmån för tjeckerna och utvisade ryska diplomater. Sverige däremot lös med sin frånvaro.[31]

Det som sker i cyberdomänen är i högsta grad verkligt med verkliga effekter på vår förmåga. Det behöver leda till slutsatser som ändrar angriparens kalkyl. Idag är kostnaden alltför låg för angriparen att genomfö-

ra ett cyberangrepp. Långsamhet i attribuering, brist på solidaritet och avsaknad av en strategi för att ta ut en kostnad gör det attraktivt för angriparen att fortsätta, förutom att det är en billig metod med potentiellt omfattande resultat.

Det skulle inte behöva vara så här. I Solidaritetsdeklarationen har Sverige en lagd grund i form av viljeinriktning, moralisk kompass och strategisk analys för ett instrument som skulle kunna utvecklas här och nu. Steg för steg skulle detta instrument kunna sätta en internationell och multilateral standard som fler ansluter sig till.

I stället för att vänta på att EU skulle komma fram till något liknande, som också riskerar att i praktiken bli ineffektivt då alla 27 länder måste vara överens på utrikesområdet för att fatta beslut om gemensamma åtgärder, kan Sverige bygga ett solidaritetsprotokoll med konsekvenser som kan tas i bruk omedelbart. I bästa fall får det EU att följa efter så småningom.

Det här kan göras steg för steg

Det första och mest närliggande steget är samarbetet mellan Sverige och Finland. Det borde vara en enkel sak att komma överens med Helsingfors om, och som sedan gemensamt agera i Nordiska Rådet för en bredare nordisk uppgörelse. Ett nästa steg är att utöka kretsen till de baltiska länderna.

Med NB8-samarbetet som grund kan andra likasinnade demokratier kunna ansluta sig steg för steg, det gäller både EU-medlemmar och länder utanför EU som Storbritannien men även icke europeiska länder som Kanada, Japan, Sydkorea, Taiwan, Australien, och Nya Zeeland. Med NB8 finns också en tyngd att driva frågorna framåt inom ramen för EU-samarbetet, samt inom Nato. En solidaritetsmekanism skulle kunna ha en bred paljett av åtgärder. Från den lägsta nivån med uttalat stöd från regeringsföreträdare, via utvisningar av diplomater till sanktioner.

Hur mekanismen med åtgärder ska se ut är något som får arbetas fram längs vägen för att hitta proportionella och adekvata nivåer. Det kommer också antagligen behöva prövas skarpt i samband med verkliga händelser. Det är dock viktigt att understryka att det som behöver komma på plats är en vilja att agera tillsammans och kontaktvägar för hur den kontakten ska ske när ett land som utsatts för angrepp ber om hjälp. Den kollektiva reaktionen behöver upplevas som kännbar, och därigenom avskräckande, för angriparen och uppfattas som proportionerlig och legitim hos vår egen befolkning.

Nästa gång den ryska militära underrättelsetjänsten stormar en lagstiftande församling i Norden med ett angrepp mot demokratins hjärta så kan inte det samfällda svaret från de närmaste vännerna vara tystnad och att vi låter den angripne stå ensam.

Så länge Sverige har solidaritetsdeklarationen så förpliktigar orden:

> Sverige kommer inte att förhålla sig passivt om en katastrof eller ett angrepp skulle drabba ett annat medlemsland (i EU) eller nordiskt land. Vi förväntar oss att dessa länder agerar på samma sätt om Sverige drabbas.[32]

Detta behöver bli vår säkerhetspolitiska lärdom av det som skedde i Stortinget i augusti 2020.

Cyberdomänen existerar inte i ett vakuum utan påverkar vår verklighet. Verktygen för att genomföra den här typen av angrepp kommer bara att fortsätta att utvecklas, därför behöver olika motmedel, som att ta ut en kostnad för angreppen, komma på plats redan idag.

Författaren är redaktör och ledamot av KKrVA.

Noter

1. Tolgfors, Sten: ”Sveriges Säkerhetspolitiska doktrin – Från neutralitet till Natooption”, *Frivärld,* 2021.
2. ”Viktig å halde Russland ansvarleg”, *NRK,* 2020-10-13, *https://www.nrk.no/nyheter/_-viktig-a-halde-russland-ansvarleg-1.15199356,* (2022-02-12).
3. ”Viktig at Noreg seier frå”, *NRK,* 2020-10-14, *https://www.nrk.no/nyheter/_-viktig-at-noreg-seier-fra-1.15200033,* (2022-02-12).
4. ”Ukraine's MFA calls for Russia's responsibility for cyberattack on Norway”, *112 UA,* 2020-10-15, *https://112.international/politics/ukraines-mfa-calls-for-russias-responsibility-for-cyberattack-on-norway-55606.html,* (2022-02-12).
5. Ulfving, Lars: *Den stora maskeraden – sovjetrysk militär vilseledning,* Försvarshögskolan, Stockholm 2000.
6. Giles, Keir: *Confronting the West: Continuity and Innovation in Moscows Exercise of Power,* Chatham House, 2016-03-21, *https://www.chathamhouse.org/2016/03/russias-new-tools-confronting-west-continuity-and-innovation-moscows-exercise-power,* (2022-02-12).
7. Jonsson, Oscar: *The Russian Understanding of War,* Georgetown University Press, Washington DC 2019, s 157.
8. Ibid, s 159.
9. Mildren, Jr, Ronald D: *The Effectiveness of Mao's Influence Operations at the Beginning of the Chinese Civil War,* Army Command and General Staff College, Fort Leavenworth 2014.
10. Mattis, Peter: ”China's 'Three Warfares'”, *Perspective, War on the Rocks,* 2018-01-30, *https://warontherocks.com/2018/01/chinas-three-warfares-perspective/,* (2022-02-12).
11. *Det demokratiska samtalet i en digital tid – Så stärker vi motståndskraften mot desinformation, propaganda och näthat,* betänkande av kommittén Nationell satsning på medie och informationskunnighet och det demokratiska samtalet, SOU 2020:56, Stockholm 2020, s 59.
12. Silverman, Craig: ”This Analysis Shows How Viral Fake Election News Stories Outperformed Real News On Facebook”, *Buzzfeed,* 2016-11-16, *https://www.buzzfeednews.com/article/craigsilverman/viral-fake-election-news-outperformed-real-news-on-facebook,* (2022-02-12).
13. ”Falska nyheter sprids mer och snabbare”, *Ny Teknik (TT),* 2018-03-09, *https://www.nyteknik.se/digitalisering/falska-nyheter-spridsmer-och-snabbare-6903233,* (2022-02-12).
14. ”Internetforskare: Facebook har bidragit till vaccinmotståndet”, *Dagens Nyheter,* 2021-10-01, *https://www.dn.se/ekonomi/internetforskare-facebook-har-bidragit-till-vaccinmotstandet/,* (2022-02-12).
15. *Pillars of Russia's Disinformation and Propaganda Ecosystem,* GEC Special Report, US State Department 2020, s 5.
16. Oksanen, Patrik och Sundbom, Henrik: ”Desinformation i skuggan av coronakrisen”, *Frivärld,* Stockholm 2020.
17. Olsson, Jonas: ”FRA: Cyberangreppen mot Sverige ökar”, *SVT,* 2019-01-05, uppdaterad 2019-01-15, *https://www.svt.se/nyheter/fra-cyberangreppen-mot-sverige-okar,* (2022-02-12).
18. Augustin, Johan: ”Cyberangreppen ökar mot svenska bolag under pandemien”, *Dagens PS,* 2021-09-21, *https://www.dagensps.se/foretagare/cyberangreppen-okar-mot-svenska-bolag-under-pandemin/,* (2022-02-12).
19. Sellebråten, Marlène: ”Så mycket kostar ransomware svenska företag”, *Realtid,* 2021-06-17, *https://www.realtid.se/sa-mycket-kostar-ransomware-svenska-foretag,* (2022-02-12).
20. Cotovio, Vasco: ”Russia accused of ”Ghostwriter” cyberattacks ahead of German election”, *CNN,* 2021-09-24, *https://edition.cnn.com/2021/09/24/europe/russia-accused-ghostwriter-cyberattacks-german-election-intl/index.html*, (2022-02-12).
21. Jeong, Andrew: ”E.U. tells Russia not to carry out cyberattacks as Germany heads for Sunday election”, *Washington Post,* 2021-09-25, *https://www.washingtonpost.com/world/2021/09/25/germany-election-russia-cyber-attack/,* (2022-02-12).
22. ”Russian hackers target German parliament again – Der Spiegel”, *Reuters,* 2021-03-26, *https://www.reuters.com/article/us-germany-politics-cyber-idUSKBN2BI272*, (2022-02-12).

23. ”Upprepade dataintrång del av en större påverkanskampanj”, Säkerhetspolisen, 2021-04-13, *https://www.sakerhetspolisen.se/ovrigt/pressrum/aktuellt/aktuellt/2021-04-13-upprepade-dataintrang-del-av-en-storre-paverkanskampanj.html,* (2022-02-12).
24. Oksanen, Patrik: ”Oroväckande att varken medier eller Riksidrottsförbundet talar klartext om Fancy Bear”, *Hela Hälsingland,* 2018-05-16, *https://www.helahalsingland.se/artikel/oksanen-orovackande-att-varken-medier-eller-riksidrottsforbundet-pratar-klartext-om-fancy-bear,* (2022-02-12).
25. COUNCIL DECISION (CFSP) 2020/1127: ”amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States”, *Official Journal of the European Union,* 2020-07-30, *https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32020D1127&from=EN,* (2022-02-12).
26. Bjarnason, Björn: *Nordic Foreign and Security Policy – Climate Change, Hybrid & Cyber Threats and Challenges to the Multilateral, Rules-Based World Order,* Nordiska Rådet 2020.
27. Ibid, s 18.
28. ”Nordiska rådet kräver starkt samarbete mot cyberhot”, Nordiska Rådet, 2021-07-01, *https://www.norden.org/sv/nyhet/nordiska-radet-kraver-starkt-samarbete-mot-cyberhot,* (2022-02-12).
29. Borger, Julian; Wintour, Patrick och Stewart, Heather: ”Western allies expel scores of Russian diplomats over Skripal attack”, *The Guardian,* 2018-03-27, https://www.theguardian.com/uk-news/2018/mar/26/four-eu-states-set-to-expel-russian-diplomats-over-skripal-attack, (2022-02-12).
30. Janicek, Karel: ”Czechs expel more Russians in dispute over 2014 depot blast”, *Associated Press,* 2021-04-22, *https://apnews.com/article/europe-russia-government-and-politics-5a09d235a24f18dab036459967444cbd,* (2022-02-12).
31. ”Russia expels 7 EU diplomats over ’solidarity’ with Czechs”, *Deutsches Welles,* 2021-04-28, *https://www.dw.com/en/russia-expels-7-eu-diplomats-over-solidarity-with-czechs/a-57360148,* (2022-02-12).
32. Op cit, Tolgfors, Sten, se not 1.