Björn Weigel

DIGITALISERINGENS BAKSIDA

CYBERHOTETS KOMPONENTER OCH KONSEKVENSER

Björn Weigel

Digitaliseringens baksida

-

Cyberhotets komponenter
och konsekvenser

Utgiven av Frivärld
Sättning och och omslag: Henrik Sundbom
Tryck: F4 Print
ISBN: 978-91-7703-177-2
www.frivarld.se

Innehåll

Förord 4
Upprinnelsen 6

DEL I 8
Cyberkriminalitet 9
Cyberkriminaliteten ökar *14*
Ekonomiskt cyberspionage 16
Överföring av rikedomar *17*
Motreaktion *22*
En ny fas? *24*
Politisk krigföring 2.0 26
”Inget är sant och allting är möjligt” – igen *27*
Arenan vidgas *31*
Trycket ökar *33*

DEL II 36
Konsekvenser 37
Samhällskontraktet försvagas, tilliten sjunker *38*
Tull på ekonomiskt välstånd *41*
Folkstyret utmanas av den starkes rätt *43*

DEL III 46
Åtgärder 47
Värna samhällets integritet *49*
Anpassa åtgärder *50*
Värna balansen i det ekonomiska maskinrummet *52*

Slutligen 54
Referenslista: 56

Förord

Snart påverkas alla delar av samhället i någon utsträckning av internet och dess effekter. Samtidigt står det klart att utvecklingen, bortom innovationer och välstånd, också fört med sig nya hot och sårbarheter. Digitaliseringen har en baksida.

Cyberhotet diskuteras ofta på helt olika sätt beroende på sammanhang. Antingen avhandlas de nya sårbarheterna i tekniska termer – någonting som blir svårbegripligt för alla som befinner sig utanför tech-kretsen. Eller så talas det om nya säkerhetspolitiska hotbilder, men bortom de försvarspolitiska seminarierna uppfattas samhällsfaran som diffus. Näringslivet är kanske den sektor som har mest erfarenhet av digitaliseringens baksida. Men av rädsla för att exponera svagheter, omsorg för kunderna eller av hänsyn till det interna säkerhetsarbetet är näringslivets företrädare ofta förtegna om hur de drabbas av cyberangrepp.

Sårbarheterna spänner över många samhällssektorer, men präglas till stor del av gemensamma nämnare. Ändå tenderar diskussionen om cyberhotet att vara fragmenterad. Frågan avhandlas antingen som en teknisk angelägenhet, ett ekonomiskt problem för näringslivet eller som ett militärt hot. Det övergripande samtalet om hur digitaliseringens baksida berör samhället som helhet har lyst med sin frånvaro.

I ”**Digitaliseringens baksida – cyberhotets komponenter och konsekvenser**” tar **Björn Weigel** ett brett grepp om cyberhotet. Skriften beskriver hur cyberkriminalitet, ekonomiskt cyberspionage och politisk krigföring växer och får spelrum i takt med digitaliseringens framfart. Weigel analy-

serar också vilka implikationer cyberhotet i dess olika former får för det liberaldemokratiska samhället som helhet, samt vilka åtgärder som bör vidtas för att för att mildra dess konsekvenser.

Teknikutvecklingen och framväxten av nya innovationer har varit svårslagna välståndsskapare. Samtidigt innebär ny utveckling nya sårbarheter. Så var fallet under tidigare tekniska revolutioner, och så är fallet när digitaliseringen nu med full kraft sveper över våra samhällen. I en tid då gränslandet mellan ekonomi och säkerhet suddas ut finns anledning att vara särskilt vaksam över hur ny teknik påverkar oss. Endast genom att se och erkänna existensen och omfattningen av cyberhotet kan vi samla oss till att bemöta det.

”Digitaliseringens baksida – cyberhotets komponenter och konsekvenser” öppnar upp för en helhetsförståelse av cyberhotet som samhällsfenomen. Genom att belysa hur nya sårbarheterna spänner över en rad sektorer gör Weigel ett välkommet inlägg i diskussionen om hur samhället som helhet bäst kan rusta sig mot cyberhotet och hantera dess konsekvenser.

Katarina Tracz
Stockholm, December 2018

Upprinnelsen

Internet var stökigt redan som barn.

Uppväxten i skuggan av kalla kriget präglades av surfbrädor och frihetsromantik, av teknikoptimism och entreprenöriella instinkter. Röken från det sena 60-talets hippierörelse dröjde fortfarande kvar. Allt det där satte sina spår.

Det vilade något rebelliskt över internet från allra första början. Poeten John Perry Barlow försökte sätta ord på det i sitt legendariska ”Declaration of the Independence of Cyberspace” på World Economic Forum i Davos i februari 1996. Han riktade sig till världens stater och slog fast att internet är gränslöst: ”Ni bör lämna oss ifred. Ni är inte välkomna hos oss. Ni har ingen suveränitet där vi samlas.”[1]

På den vägen är det. Till en början gick det också riktigt bra, tills det inte gick så bra längre och där befinner vi oss i dag. Det där upproriska finns kvar, men internets poetiska charm är sedan länge borta. Kvar finns en rå verklighet där allt uppkopplat mot internet kan hackas och därmed riskerar att förfaras, från företag till politiska val, självkörande bilar, personliga identiteter och värderingar. Trycket ökar dessutom, cyberhotet är i en uppåtgående trend, inte minst i väst.

Det talas om digitaliseringens fördelar, men digitaliseringens baksida glöms ofta bort. Denna skrift har tre syften. Det första syftet är att diskutera cyberhotet i väst, som i denna skrift består av tre delar; cyberkriminalitet, ekonomiskt cyberspionage och politisk krigföring 2.0. De är alla tre negativa kraf-

1 Internet Hall of Fame (2018).

ter som digitaliseringen släppt lös i väst, de växer i takt med digitaliseringen, står nära auktoritära ideal, och samhället och näringslivet kontrollerar dem inte speciellt väl. De tas heller inte alltid på tillräckligt stort allvar av beslutsfattare. Cyberhotet diskuteras i del I.

Skriftens andra syfte är att diskutera cyberhotets konsekvenser som är mer långtgående för samhället och näringslivet än många kanske tror: samhällskontraktet försvagas och tilliten sjunker. Cyberhotet avkräver i praktiken en tull på ekonomiskt välstånd och innebär att folkstyret utmanas av den starkes rätt. Lite mer än tjugo år efter Barlows självständighetsförklaring i Davos står det klart att auktoritära krafter inte lämnar oss i fred utan snarare ökar sina försök att sätta sin egen prägel på världen via nätet. Cyberhotet är på god väg att utvecklas till en förtroendefråga för vårt samhällssystem. Det talas om att den liberala världsordningen är i kris – cyberhotet bidrar till att förvärra krisen. Allt detta diskuteras i skriftens del II.

I den tredje delen diskuteras vad mer som kan göras för att temperera cyberhotet. Två grundantaganden diskuteras, därefter tre förslag på insatsområden. Dessa är att värna samhällets integritet, att anpassa åtgärder och att värna balansen i det ekonomiska maskinrummet.

DEL I

Cyberkriminalitet

Längst upp på Mark Zuckerbergs och James Comeys datorer sitter en liten bit tejp och under tejpen hittas en webbkamera.[2] Bakom lager av säkerhet som brandväggar och antivirussystem nekar Facebooks grundare och FBI:s förutvarande chef cyberspioner insyn med enkla medel. Tejpen sitter där den sitter eftersom datorn är uppkopplad mot internet, som Erik Schmidt, tidigare vd för Google konstaterade, ”är det första som mänskligheten byggt [och] som mänskligheten inte förstår, det största experimentet i anarki som vi någonsin har haft”.[3] I ett anarkiskt tillstånd är det möjligt att två av världens säkraste webbkameror hackas.

Internet är många saker, bland annat en passande miljö för cyberkriminella. Cyberkriminalitet är när aktörer bereder sig otillåten tillgång till datorer och digitala nätverk, och cyberkriminella inkluderar bland annat vissa stater, missnöjda anställda, studenter, terrorister, opportunister och yrkeskriminella. De är alla del av en kriminell värld på nätet som få har kännedom om eller någonsin frivilligt skulle besöka. Men det spelar ingen roll, den världen kommer i stället till oss. Om vi önskade bygga den perfekta plattformen för kriminalitet, då har vi lyckats med internet. Detta har cyberkriminella sedan länge klurat ut.

För lite mer än vad det kostar att tanka en svensk familjebil kan vem som helst köpa duglig hack-kod och begå brott på nätet. Femtonhundra kronor räcker långt och tekniska

2 Titcomb (2016).

3 Taylor (2010).

kvalifikationer behövs nästan inte.[4] Att bereda sig otillåten tillgång till datorer och digitala nätverk kan vara enklare än många föreställer sig. Det kan räcka med att trycka på en knapp i användargränssnittet i ett hackerprogram: På egen hand hittar programmet mål, bryter sig in i system och återrapporterar. Avsändaren behöver inte ens veta vem som drabbats eller hur mycket skada som gjorts.

Cyberkriminella siktar ofta in sig mot företag. DDoS-attacker (”Distributed Denial of Service”) som överbelastar företag med anrop skickade från hackade datorer är ett exempel. Kryptering av hackade datafiler är ett annat. Sommaren 2017 drabbades redarbolaget A.P. Möller Maersk av en krypteringsattack. Skadorna uppgick till cirka två miljarder svenska kronor. Bolaget tvingades återinstallera 4 000 servrar och 45 000 datorer, samt hantera delar av verksamheten manuellt. Som bolagets vd uttryckte saken: ”Tänk dig ett företag där ett fartyg med 20 000 containrar kommer in i en hamn var femtonde minut, och i tio dagar har du ingen IT.”[5] Allt fler företagare känner igen sig. Enligt Cisco:s tidigare vd John Chambers finns bara ”två typer av företag: de som blivit hackade och de som inte vet att de har blivit hackade”.[6] Och om vi får tro FBI:s tidigare chef Robert Mueller sammanfaller ”även de … [med] en kategori: företag som blivit hackade och som kommer att bli hackade igen.”[7]

Cyberkriminalitet sträcker sig emellertid bortom näringslivet. Ingen och ingenting uppkopplat mot nätet undgår ris-

4 McKinsey (2017).
5 Cimpanu (2018).
6 Chambers (2015).
7 Mueller (2012); Kerravala (2015).

ken att drabbas av cyberkriminalitet, något som även gäller kritiska samhällsfunktioner. Den 12 maj 2017 drabbades Englands sjukvårdssystem (NHS) av en krypteringsattack. Plötsligt eldhärjades sjukvårdssystemets digitala infrastruktur med krypteringskod. För de drabbade kunde det lika gärna ha handlat om en faktisk brand när provsvar försenades, akutmottagningar fick stänga och ambulanser tvingades vända. Nära tjugo tusen patientbesök fick ställas in dagarna efter attacken.[8]

Cyberkriminella får inte alltid utdelning, men det spelar mindre roll. När det gäller utpressning på nätet till exempel, som ofta är syftet med DDoS-attacker och kryptering av hackade datafiler, betalar offren med ojämn tillförlitlighet, och kraven är dessutom ofta modesta. Men attackeras tillräckligt många blir avkastningen värd mödan, och antalet måltavlor är stort.

Internet underlättar för den som är kriminell och försvårar för den som har något att försvara. Cyberinbrott är till exempel ofta svårupptäckta; vanligen avslöjas de långt efter att de inträffat. Stora värden kan stjälas på bara några sekunder och ta år att upptäcka. Nio av tio intrång är över på en minut eller mindre medan två tredjedelar i bästa fall upptäcks först efter flera månader.[9] När en bankrånarliga med sannolika kopplingar till bland annat Ryssland och Ukraina avslöjades för några år sedan – operation Carbanak – hade ligan under två års tid ostört rånat banker i trettio länder på upp till 8 miljarder kronor.[10]

8 Morse (2017).
9 Verizon (2018).
10 Kaspersky (2015).

Det var länge sedan cybersäkerhet främst handlade om att förhindra intrång, hackare kan nämligen ofta ta sig in i system om de bara vill. Nu handlar cybersäkerhet mer om att hindra aktörer från att ta med sig någonting ut från system de olovligen tagit sig in i, men även detta är svårt. Cyberbankrånare släpar inte säckar med pengar från sprängda bankvalv till väntande flyktbilar. I fallet Carbanak rånades bankomater och bankkonton obemärkt och utan att rånarna behövde sätta sin fot vid någon av offrens bankkontor. När femtio miljoner Facebook-användarkonton hackades i september 2018 krävdes inga lastpallar för att lyfta ut stöldgodset. Om en akt motsvarat ett fysiskt A4-ark när kreditföretaget Equifax hackades på över 145 miljoner personuppgifter i september 2017 skulle stöldgodset ha vägt 725 ton eller motsvarat cirka fyrahundra personbilar.

Ingen kommer undan med denna omfattning av brott i den fysiska världen, men i den digitala världen är volymfrågan ointressant. Det tog två månader innan Equifax annonserade intrånget, vilket trots allt var snabbare än när Yahoo hackades på alla sina tre miljarder användarkonton (det dröjde fyra år innan omfattningen uppdagades).[11] Men svårare än att upptäcka intrång, eller att hindra hackare från att få med sig något, är att hitta de skyldiga.

Kryptovalutor som Bitcoin, som ofta används vid utpressning, kan hanteras anonymt. Nätverk och plattformar som Onion Router (TOR), Freenet eller I2P döljer identiteter. Vissa länder skyddar cyberkriminella i utbyte mot tjänster. Därtill är internets storlek ett skydd, och då inte bara dess

11 Hatmaker (2015).

sökbara del. Google hanterar dagligen över sex miljarder sökningar på nätet, men den del av nätet som sökprogrammen hanterar och som är indexerad utgör endast en bråkdel av totalvolymen. The Deep Web – som innehåller data som sökprogrammen inte hittar – bedöms vara kanske femhundra gånger större mätt i datavolym än det sökbara internet.[12]

Internet är ett passande habitat för cyberkriminella likaså eftersom det är uppbyggt efter användarvänlighet, inte säkerhet. När internet utvecklades var datorkraft dyr och det fanns incitament till att dela kostnader och information – säkerhet var inte prioriterat. Den grundarkitektur som då skapades lever till stor del kvar. Nätet är säkerhetsmässigt poröst. När ny hård- och mjukvara tillförs ökar exempelvis risken för att det ska uppstå säkerhetsbrister. Företagets datasystem riskerar att kompromitteras när någon ska installera en ny skrivare på nätverket, likaså om någon kopplar upp sina trådlösa hörlurar. Cyberförsvaret ligger ofta steget efter. En studie av 40 virusprogram designade för att upptäcka och avstyra virus som testades mot 82 aktiva virus visade att virusprogrammen var närmast verkningslösa och släppte igenom 95 procent av alla aktiva virus.[13]

Men den kanske viktigaste anledningen till varför internet är en idealisk plattform för kriminella är att den erbjuder möjligheter att exploatera mänskliga svagheter. Enligt James Clapper, tidigare chef för USA:s underrättelsegemenskap, inleds upp till nittio procent av alla försök till nätintrång med en metod som innefattar manipulation och att lura

12 Europol (2017); Choudhury et al (2017).

13 Goodman (2015) s 31.

användare.[14] Cyberkriminella utnyttjar oaktsamhet eller nyfikenhet där användare exempelvis öppnar dokument med skadlig programkod eller använder planterade och smittade USB-stickor.

Med allt detta i åtanke är det lätt att förstå varför Zuckerberg och Comey är noga med tejpen – de vet att cybersäkerhet är en kapplöpning mellan vem som upptäcker svagheter först.

Cyberkriminaliteten ökar

Nära 90 procent av ansvariga för informationssäkerhet i amerikanska och brittiska företag oroar sig för växande cyberhot, enligt en undersökning av RiskIQ från 2018.[15] Antalet skadliga program för mobiltelefoner ökade med 54 procent 2017 enligt säkerhetsföretaget Symantec som också bedömer att så kallad ”cryptojacking”, att otillåtet använda andras datorer för att generera kryptovalutor som Bitcoin, ökade med 8 500 procent samma år.[16] Mellan 2016 och 2017 ökade företagens kostnader för cyberbrott i exempelvis England med 21 procent och i Tyskland med 42 procent enligt en studie av Accenture (där fem år och flera länder jämfördes och där ökningstakten i procent var som störst i slutet av perioden).[17] Cyberkriminalitet är enligt de flesta bedömare i en uppåtgående trend.

Med tanke på att det snart finns ännu fler möjligheter för cyberkriminella att olagligt tjäna pengar är det också rimligt att vänta sig att trenden fortsätter. Bara under de senaste två

14 Clapper (2018) s 286.
15 Ismail (2018).
16 Symantec (2018).
17 Richards, et al. (2017).

åren genererades nittio procent av all data som finns och tillväxttakten ser inte ut att mattas av.[18] Fysiska ting kopplas upp mot nätet, en utveckling som benämns ”Internet of Things” (IoT). Ungefär 55 miljarder enheter kopplas upp fram till år 2025 enligt experter, en uppgång från 9 miljarder enheter 2017.[19] Kylskåpet, femåringens leksaksgitarr, babymonitorn och jobbets kaffeapparat kommer snart att kopplas upp om de inte redan är det och exponeras därmed för cyberkriminalitet. En tredjedel av alla framgångsrika IT-attacker riktade mot företag i framtiden kommer att ske via utrustning som företagen inte ens känner till är uppkopplade, förutspår analysföretaget Gartner.[20]

Därtill utvecklas bättre och billig teknik som döljer bedrägeriförsök. Skillnaden suddas till exempel ut mellan verkliga och fabricerade ljudfiler, och mellan falska och äkta rörliga bilder, med så kallade *deep fakes* – högkvalitativ falsk information framställd med hjälp av artificiell intelligens (AI). AI ändrar förutsättningarna för cyberkriminalitet. AI kan hacka dygnet runt utan mänsklig handpåläggning. Även cybersäkerhet automatiseras. Redan består cirka 30 procent av företagens cyberförsvar av AI.[21]

Kvantdatorer kan automatisera intrång med större kraft och knäcka de flesta krypteringar om de utvecklas så som många experter bedömer. Utvecklingen kan revolutionera frågan om cybersäkerhet och bland annat påverka utvecklingen inom förarlös teknik. Tänk bara på drönare. Redan använder över

18 Marr (2018).
19 Newman (2018).
20 Hegarty, Ferreira & Grahn (2018).
21 Cisco (2018).

nittio länder militära drönare. Vad händer om kryptering inte längre skyddar dem mot intrång? Vad händer med förarlösa bilar, gräsklippare, bussar, budbilar och mycket annat när de kan kommas åt av hackare?

Klart är att alla de egenskaper som gör internet till en passande miljö för cyberkriminella även underlättar för det som utgör cyberhotets andra del: ekonomiskt cyberspionage.

Ekonomiskt cyberspionage

Pressmeddelanden från Myndigheten för samhällsskydd och beredskap (MSB) får normalt inte så mycket uppmärksamhet, men bulletinen den elfte april 2017 passerade långtifrån obemärkt. ”Omfattande internationella cyberangrepp”, angav meddelandet, hade riktats mot svenska intressen. Oron spred sig snabbt; vem hade angripit och varför, hur länge hade det pågått, vilka var konsekvenserna och varför kallades operationen för Cloud Hopper?[22]

Ekonomiskt cyberspionage är den andra kraften som digitaliseringen har släppt lös och den inbegriper cyberstöld upplyft till statsstrategi. Ekonomiskt cyberspionage inträffar när stater via egna resurser eller med hjälp av inhyrda kapaciteter via datorer och digitala nätverk spionerar på och stjäl information och teknik från andra länders företag och organisationer. Syftet är främst att gynna det egna näringslivet, eller att gynna den egna statens strategiska och kommersiella intressen. Ekonomiskt cyberspionage riktas ofta mot tekniskt och ekonomiskt utvecklade länder och företag i väst.

22 PwC (2017).

Överföring av rikedomar

Spioneri på och stöld av information och teknik från andra länders företag och organisationer uppfanns inte med internet, men nätet ändrar förutsättningarna för sådana aktiviteter och redan 2012 varnade chefen för amerikanska National Security Agency (NSA) att cyberbrott mot amerikanska företag utgjorde den ”största överföringen av rikedomar genom historien”.[23]

Ekonomiskt cyberspionage, som operation Cloud Hopper, är förknippat med juridiska oklarheter, delvis saknas internationella regelverk. Likväl existerar ett globalt regelverk och system kring handel och konkurrens som världens länder enats om. Systemet är inte perfekt, men dess parter har ändå följt regelverket någorlunda väl. Naturligtvis förekommer regelbrott från exempelvis stater som otillbörligen gynnar det inhemska näringslivet.

De internationella handelsregelverken har skapat en situation som kunde ha varit bättre, men också betydligt sämre – i den fysiska världen vill säga. I den digitala världen är läget mer kaotiskt. Ekonomiskt cyberspionage hade i den fysiska världen inneburit omfattande brott mot internationella överenskommelser beträffande handel och konkurrens.

Ingen kan veta säkert hur stort problemet är. Det ligger i sakens natur att förövare hemlighåller intrång. Alla kostnader som upptäcks rapporteras inte och gränsdragning är föremål för debatt. Tankesmedjan Center for Strategic and International Studies (CSIS) beräknar att kostnaden för cyberbrott

23 Rogin (2012).

uppgår till närmare 600 miljarder dollar, motsvarade cirka 0,8 procent av den globala bruttonationalprodukten (BNP) 2016 (detta jämfört med cirka 0,62 procent 2014).[24] Siffran ligger nära den internationella försäkringsförmedlaren Aon:s bedömning om cirka 550 miljarder dollar i skador från cyberbrottslighet 2017.[25] Cybersecurity Ventures bedömer att de totala kostnaderna för cyberbrott når sex biljoner dollar 2021 – vilket därmed skulle göra cyberbrottslighet lönsammare än den globala illegala droghandeln.[26]

Men ekonomiskt cyberspionage handlar om mer än pengar. Ekonomiskt cyberspionage riktas mot de mest framgångsrika företagen, de värdefullaste teknologierna och mot verksamheter med stor ekonomisk, militär och social potential. Ekonomiskt cyberspionage fokuserar på företag som kan bygga bättre samhällen i framtiden. Om de blir bestulna har samhället svårare att dra nytta av fördelar som medföljer ny teknik och fördjupade kunskaper. Därför är det oroväckande med uppgifter som att exempelvis 65 procent av industri- och teknologiföretagen i Tyskland, vilka tillhör Europas mest avancerade teknikföretag, hackades bara under 2016 enligt en studie av försäkringsbolaget Hiscox.[27] I värsta fall tvingas några av dessa företag bort från marknaden av konkurrenter som säljer stulen teknologi till lägre pris eftersom dessa konkurrenter drar nytta av att inte behöva ta hänsyn till utvecklingskostnader. Inte konstigt att cirka sextio procent av de verkställande direktörerna i en

24 CSIS (2018).
25 The Economist (2018).
26 Morgan (oktober 2017).
27 Hiscox (2017).

annan studie från 2017 ansåg att cyberhot var ett ”going concern” för företagstillväxten.[28]

Företagen är mer utsatta i dag än tidigare eftersom de är mer exponerade tack vare digitaliseringen. Det är länge sedan materiella tillgångar, det vill säga fysiska tillgångar som maskiner och produktionsanläggningar, utgjorde merparten av företagens marknadsvärde. Marknadsvärdet består i dag i stället främst av immateriella tillgångar, som patenträtter, kundregister, affärsmodeller, datorprogram, avtal, forskningsresultat, arbetsprocesser och liknande. År 1975 representerade dessa värden mindre än tjugo procent av det totala marknadsvärdet för bolag listade på kreditvärderingsinstitutet Standard & Poor’s index över börsnoterade stora företag i USA (S&P 500). År 2015 hade andelen ökat och uppgick till cirka 84 procent av det totala marknadsvärdet, 19,8 biljoner dollar.[29] I utvecklade företag och länder är immateriella värden i dag synonymt med stora strategiska värden, vilket inte har undgått opportunistiska stater som därigenom ser en chans att minska gapet till ledande tekniknationer. Detta leder oss tillbaka till Operation Cloud Hopper.

Säkerhetsföretag och underrättelseorganisationer i flera länder, däribland Sverige, genomförde omfattande kartläggningsarbete och kriminaltekniska analyser för att avslöja vad som sedermera blev känt som Operation Cloud Hopper. Det tog sin tid. Hackarna dolde sina spår väl. Gruppen APT10, även känd som ”Red Apollo”,[30] tillskrevs ansvar. Och akro-

28 PwC blogs (2017).

29 The Economist (2018).

30 APT10, a.k.a. Stone Panda, menuPass, CVNX.

nymen ”APT” som står för ”advanced persistent threat” beskriver tillvägagångssättet. Attacken var både avancerad och beständig, och vissa experter tror att den pågår än. Den krävde omfattande förberedelser inklusive kartläggning av tänkta mål, deras arbetsförhållanden, anställdas privata relationer och annat för att göra operationen framgångsrik.

Operationen genomfördes genom bland annat så kallad ”spear phishing” – en metod som liknar att fiska abborre (ryska hackergruppen Fancy Bear använde metoden med framgång mot Hillary Clintons kampanjordförande John Podesta). Hackaren kastar förvisso inte ut agnade fiskekrokar, men däremot agnade email och väntar sedan på napp. Det kan räcka med att endast en person nappar och öppnar ett agnat mail för att en organisation ska hackas. Den som nappat märker ofta ingenting, men väl inne bakom brandväggar och virusdetektionssystem stjäls information, kommunikation avlyssnas och plattformen kan sedan användas som språngbräda mot ytterligare mål. I fallet Cloud Hopper angreps serviceföretag som erbjöd vad kunderna trodde var säkra molntjänster. Väl inne kunde hackarna hoppa runt bland företagen som använde molntjänsterna – därav namnet.

Experter bedömer att APT10 är verksamma från Kina, men ännu är inte detektivarbetet för att kartlägga alla detaljer kring det massiva angreppet färdigt.[31] Nyligen framkom uppgifter om att det kan finnas en koppling mellan hackergruppen och ministeriet för statens säkerhet i Tianjin, Kinas

31 PwC (2017).

motsvarighet till amerikanska NSA.[32] Sommaren 2018 slog ett säkerhetsföretag som uppgav att de följt hackergruppen i nästan tio år larm och påstod att APT10 precis försökt hacka japanska medieföretag.[33] Det återstår att se om berättelsen fortsätter. Kina eller kinesiska aktörer har dock aldrig erkänt skuld i relation till Cloud Hopper.

Men att länder spionerar via nätet är välkänt, likaså att inflytelserika länder med internationella ambitioner som USA, Kina och Ryssland satsar stora resurser på cyberspionerі. Amerikanska försvarsdepartementet pekar ut Kina tillsammans med Ryssland som strategiska hot inom cyber.[34] Nyligen anklagade amerikanska myndigheter kinesiska aktörer för stöld av militära hemligheter från Naval Undersea Warfare Center. 614 gigabyte data uppgavs stulna, inklusive hemliga ritningar av framtida amerikanska ubåtsrobotar.[35] År 2015 avslöjades ett intrång där förövarna kom över miljontals ansökningar om säkerhetsklassning i amerikansk federal tjänst som innehöll hemliga personuppgifter, intervjuer, namn på referenter och information om familjemedlemmar. Även kopior av 5,6 miljoner fingeravtryck kom i orätta händer. Enligt säkerhetstjänster hackades uppgifterna av aktörer från Kina och skulle kunna användas i militärt syfte.[36]

Militärt spionage är en sak, medan omfattande internationellt ekonomiskt cyberspionage är något annat, och gällande det sistnämnda återkommer ofta samma aktörer i experter-

32 Kozy (2018).
33 Matsuda, et al. (2018).
34 Department of Defense (2018).
35 Nakashima, & Sonne (2018).
36 Clapper (2018) s 295.

nas rapporter. Den amerikanska IPC-kommissionen konstaterade att Kina ”förblir världens främsta förbrytare” inom immateriella rättigheter.[37] Representanter från Afrikanska unionen befarade 2017 att deras högkvarter i Addis Ababa, Etiopien, som byggts av ett statligt kinesiskt företag, hade hackats och information skickats till servrar i Shanghai nattetid över flera år. Kina nekar till detta.[38] En studie i *Military Cyber Affairs* från hösten 2018 hävdade att det kinesiska företaget China Telecom via internets basinfrastruktur olovligen kopierat internettrafik från tio platser i Nordamerika (via ”distributed points of presence”, PoP), en handling som ansågs ha börjat tidigt på 2000-talet. Studien hävdade att bland annat datatrafik från Sverige och Norge till en nyhetsorganisation i Nordamerika hade kopierats under 6 veckor i april och maj 2017.[39] Experten Mark Anderson, grundare av och vd för Strategic News Service (SNS), går så långt att han påstår att en stor del av Kinas tillväxt under de senaste åren går att förklara med hänvisning till ekonomiskt cyberspionage och att så mycket som kanske hälften av landets BNP kan komma från ekonomiskt cyberspionage och andra stölder.[40]

Exemplen kan fortsätta radas upp. Larmrapporterna avlöser varandra. Om rapporterna stämmer – och stater i Väst tar till sig av innehållet – torde det komma en motreaktion. Kanske är det den vi nu ser?

37 IP Commission Report (2017).
38 Aglionby et al. (2018).
39 Demchak & Shavitt (2018).
40 Anderson (2017).

Motreaktion

Hösten 2015 annonserade Kinesiska kommunistpartiets generalsekreterare Xi Jinping och dåvarande amerikanske presidenten Barack Obama ett ömsesidigt ställningstagande mot ekonomiskt cyberspionage. Därmed skulle ekonomiskt cyberspionage minska mellan Kina och USA. Det råder delade meningar om överenskommelsens effekter. Visserligen noterade experter i USA en minskning i aktiviteter omedelbart efter överenskommelsen, men snart uppstod tvivel om att det kanske snarare handlat om skärpta metoder och större precision i hackandet. Hur som helst var överenskommelsen ett tydligt diplomatiskt tecken på att USA nått en gräns för vad landet var berett att tolerera. Fler reaktioner från USA skulle följa. Några sentida exempel:

- I juli 2018 införde USA tullavgifter på kinesiska varor. Bedömningen var att ekonomiskt cyberspionage är en av flera bakomliggande orsaker till vad som alltmer liknar en handelskonflikt mellan Kina och USA.

- FBI:s chef avrådde 2018 från att använda kinesiska mobiltelefoner och från att bereda kinesiska telekomföretag inflytande över telekominfrastruktur.[41]

- I november 2017 åtalades tre kinesiska medborgare i USA för bland annat datorhackning, stöld av företagshemligheter och identitetsstöld.[42]

Politiska reaktioner med hänvisning till cybersäkerhet och Kina har även kommit från andra länder, inklusive England,

41 Salinas (2018).

42 NCSC (2018) s 7.

Tyskland och Australien. Augusti 2018 kom uppgifter att Japan överväger restriktioner mot kinesiska Huawei Technologies Co. och ZTE Corp.[43] Alltmer uppmärksamhet riktas mot att Kina donerat datorutrustning till över 35 länder – övervägande utvecklingsländer som förefaller vara strategiskt viktiga för Kina – efter oro att utrustningen skulle kunna ge Kina makten att spionera på användarna.[44] Politiskt hörs oftare och allt skarpare uttalanden riktade mot Kina. I representanthusets utrikesutskott sommaren 2018 dundrade ordföranden: ”Ingen nation på jorden har gynnats mer från efterkrigstidens världsordning än Kina … Trots sina framgångar vill Kina inte spela enligt reglerna ... Kina utnyttjar sårbarheterna i det globala systemet … för att vinna strategiska fördelar. Kina har ingen avsikt att bli en jämlik partner i världssamfundet. De gör detta (vinner fördelar) genom att fuska. Precis som Kinesiska kommunistpartiet inte vill ha rivaler hemma, vill de ha ett globalt system som säkerställer deras egen dominans.”[45]

En ny fas?

Frågan är om ekonomiskt cyberspionage kan vara på väg in i en ny fas?

Under lång tid fanns en viss acceptans för ekonomiskt cyberspionage i väst, av tre skäl: Dels eftersom det ansågs gynna fattiga utvecklingsländer som därmed skulle moderniseras och förhoppningsvis också demokratiseras. Men det fanns också ekonomiska motiv och förväntningar om att en väx-

43 Barkin (2018); Negishi (2018).

44 Thomas (2018).

45 Poe (2018).

ande medelklass skulle generera konsumenter i utvecklingsländer som i sin tur skulle efterfråga produkter och tjänster från väst. Dessutom bidrog utvecklingsländer till internationella värdekedjor och utveckling av företag och produkter till nytta i väst. Västvärlden tjänar fortfarande på att utvecklingsländernas ekonomier växer, men acceptansen för ekonomiskt cyberspionage tillhör historien.

Nu är stämningsläget mindre tolerant. Fler röster ger uttryck för att tillräckligt med skadlig programkod spridits, tillräckligt många företagshemligheter försvunnit och tillräckligt många konkurrenter till inhemska företag sålt kopierade produkter till lägre priser. Men det återstår att se om reaktionerna blir skarpare än begränsade sanktioner och politiska markeringar.

Ytterligare ett tecken på att ekonomiskt cyberspionage kan vara på väg in i en ny fas är att en internationell diskussion om gränsdragning intensifieras. Vissa länder skiljer inte på ekonomiska intressen och nationella säkerhetsintressen. Gränsen mellan ekonomiskt cyberspionage och till exempel legitim informationsinhämtning kan vara hårfin. Otillåtet ekonomiskt cyberspionage i ett land kan vara tillåtet i ett annat, teknik kan användas både för militärt och civilt syfte. Gränsen mellan cyberspionage och aggressiv marknadsföring är ibland omärkbar. När har ett övertramp inträffat? Är ett företagsköp att betrakta som kompromitterat om ett av rådgivningsföretagen som hanterat affären har hackats på information om till exempel förhandlingsstrategier i samband med köpet?

Dessutom satsar länder alltmer öppet på att öka sina cyberkapaciteter. Kinas Xi Jinping har deklarerat att landets stra-

tegiska ambition är att bli en ”supermakt i cybersfären”.[46] Landet planerar sex nya cybersäkerhetsuniversitet till år 2027 och genomför program där unga cybertalanger premieras och tränas i tidig ålder. Andra länder genomför liknande satsningar. Är sådana aktiviteter att tolka som legitima försök att stärka den kommersiella förmågan eller bör de betraktas som plantskolor för framtida cyberarméer?[47] Dessa är exempel på frågeställningar i en kokande internationell debatt, som ännu är i sin linda.

Politisk krigföring 2.0

”The ideal subject of totalitarian rule is not the convinced Nazi or the dedicated communist, but people for whom the distinction between fact and fiction, true and false, no longer exists.”

Hanna Arendt

I Sovjetunionens illa fungerande auktoritära planekonomi staplades misslyckanden ovanpå varandra. Butikshyllorna gapade tomma och bilarna liknade skokartonger, men på ett område var Sovjet ledande: i politisk krigföring var ”ondskans imperium”, för att tala med Ronald Reagan, överlägset. Säga vad man vill om dagens PR-konsulter och spinndoktorer, men de är rena amatörer jämfört med sovjettidens beryktade underrättelsetjänst KGB där ”spridning av desinformation [var] … både en livsstil och en konst”[48] enligt tidigare amerikanska utrikesministern Madeleine Albright.

46 Kania et al. (2017).
47 Jing (2017); Risky (2018).
48 Albright (2018) s 164.

Internet innebar en teknikrenässans som vände upp och ned på förutsättningarna för politisk krigföring. Politisk krigföring avser när länder, i syfte att konkurrera med andra länder, använder ”ord, bilder och idéer”, ibland i kombination med visst mått av ”våld, ekonomisk påtryckning, omstörtande verksamhet och diplomati”, utan att agerandet övergår i en krigshandling.[49] Det handlar delvis men inte enbart om kommunikation, och anses ha existerat så länge stater har konkurrerat med varandra. Internet ändrade förutsättningarna för politisk krigföring: tid och rum fick delvis en annan betydelse, landsgränser blev mindre begränsande, angrepp blev billigare medan försvaret kostar mer, angripare kan enklare dölja sina identiteter, antalet tänkbara mål har ökat och slutligen kan det vara svårt att avgöra om en attack pågår. Allt detta kokar ned till att politisk krigföring har ändrat karaktär, till politisk krigföring 2.0.

Politisk krigföring 2.0 är den tredje kraften som digitaliseringen har släppt lös i väst och som växer i takt med digitaliseringen, står nära auktoritära ideal och som samhället och näringslivet inte kontrollerar speciellt väl.

”Inget är sant och allting är möjligt” [50]– igen

När Rysslands president Boris Jeltsin upplöste KGB 1993 trodde många att det innebar slutet på landets politiska krigföring. I dag vet vi bättre. Agenterna som då försvann har återkommit och bedriver effektivare kampanjer än någonsin. Grunderna i den politiska krigföringen hämtas fortfarande från kalla krigets ”playbook”, kraften hämtas från internet.

49 Smith (1989) s 3.

50 Pomerantsev (2017).

Politisk krigföring 2.0 handlar delvis om demokratiska val, som tydligt illustrerades i det amerikanska presidentvalet 2016. Amerikanska senatens underrättelseutskott slog fast att Ryssland lagt sig i valet och särskilda utredaren Robert Mueller har stämt ryska medborgare, inklusive officerare från ryska militära underrättelsetjänsten GRU.[51] Samtidigt är ryska angrepp mot val i väst inget nytt. Varje amerikanskt presidentval under kalla kriget var måltavla för försök att manipulera utfallet.[52] Men skillnaden mellan tidigare kampanjer och den 2016 var i vilken utsträckning internet blev avgörande.

Demokratiska val hamnar i skottgluggen när auktoritära stater bedriver politisk krigföring 2.0 eftersom val avgör demokratins legitimitet och påverkar allmänhetens tillit till demokratiska institutioner. Ingen vet hur utfallet faktiskt påverkades av 2016 års kampanj men att demokratin i USA fick ta emot rediga törnar är ingen överdrift. Exempelvis har tilliten till regeringen sjunkit drastiskt. Mindre än en tredjedel av befolkningen anser att representanter från regeringen är trovärdiga, en kraftig nedgång från tidigare mätningar.[53] Ett annat exempel är att polariseringen av åsikter mellan demokrater och republikaner når rekordnivåer enligt Pew Research Center.[54]

Men politisk krigföring 2.0 handlar om betydligt mer än enbart val. Nyhetskanalen RT (tidigare Russia Today) startades 2012 och anses av bedömare vara ett redskap för Rysslands politiska kampanjer. Utmärkande för kanalen är hur

51 SSCI (2018); ICA 2017; USA:s justitiedepartement (2018).
52 Clapper (2018) s 314-315.
53 Edelman (2018).
54 Pew (2017).

den verkar i gränslandet mellan den fysiska världen och den digitala. Och det finns fler exempel. Tankesmedjan Atlantic Council visar i rapportserien ”The Kremlin’s Trojan Horses” att Ryssland placerat så kallade politiska trojaner i västerländska demokratier i syfte att destabilisera dem inifrån. Många av dessa trojaner är aktiva inom sociala medier och ligger i framkant när det kommer till att utnyttja nätet.[55] Twitter avslöjade 50 000 automatiska konton kopplade till Kreml med närmare 700 000 följare under det amerikanska presidentvalet 2016.[56] Mycket talar för att aktiviteterna startade långt före valet och fortsätter än i dag. Facebook konstaterade att 126 miljoner amerikaner mottagit material från ryska nättroll mellan 2015 och 2017.[57] Inget vet säkert hur många nättroll eller botar som är verksamma via Facebook i dag.

Bortom de sociala medierna antar den politiska krigföringen 2.0 en rad skepnader. Hackning kan användas för olika politiska syften, några exempel:

- I oktober 2018 grep holländska säkerhetstjänsten officerare från ryska underrättelsetjänsten GRU som försökte hacka Organisationen för förbud mot kemiska vapen (OPCW). Sannolikt var den ryska handlingen kopplad till anklagelser mot Ryssland i samband med giftattacken mot far och dotter Skripal med nervgiftet Novitjok i mars 2018 i Storbritannien.[58]

- De ryska GRU-officerarna kunde beslås med att ha

55 Polyakova, et al. (2016).
56 Rosenberg (2018).
57 Weise (2017).
58 Applebaum (2018b).

hackat utrustning tillhörande världsantidopingbyrån WADA, sannolikt eftersom WADA ansågs drivande bakom att dopinganklagelser resulterade i avstängningar av ryska idrottare, och en uteslutning av Ryssland från att delta i 2018 års olympiska spel.[59]

- Bevis har också hittats för att Ryssland försökt hacka undersökningen bakom nedskjutningen av passagerarplanet MH17 över Ukraina 2014, som tillskrevs den ryska försvarsmakten.[60]

Cyber påverkar i hög grad hur den politiska krigföringen utformas och det har att göra med internet som funktion. Manipulation av sociala medier, snedvridning av traditionella medier och nyhetstjänster samt hackerattacker illustrerar hur cyber har blivit en framstående plattform och ett verktyg i den politiska krigföringen. ”The medium is the message”, konstaterade filosofen och kommunikationsvetaren Marshall McLuhan redan 1967. Få bevingade fraser beskriver cyberhotets politiska dimension bättre. För *funktionen* genom vilken information sprids har stor betydelse, kanske över tid större betydelse än informationen som sådan. Mediet i sig är inte att betrakta som ett neutralt redskap utan ett *budskap*. Internet har blivit ett budskap i det att information sprids på ett annat sätt, och att det i sig haft stora konsekvenser för samhällsutvecklingen. Interaktion mellan mottagare och producent fanns inte tidigare; likaså är uttryckssätt och tidsaspekter ändrade. Internets funktion ändrar förutsättningarna för hur information skapas, sprids och konsumeras.

59 Ibid.

60 News (2018).

Fenomenet är inte nytt. Boktryckarkonsten ändrade förutsättningarna för informationsinhämtning på ett sätt som radikalt kom att påverka samhället. Radio och tv ändrade förutsättningarna några århundraden senare. På samma sätt som de som då förstod att använda boktryckarmediet och radio och tv kunde vinna fördelar, är de som förstår att använda internet för att bedriva politisk krigföring 2.0 vinnare i dag.

Internets funktion skärper effekterna av politisk krigföring. I slutändan handlar det om att forma och påverka människors sätt att tänka, handla och agera. Internet innebär en funktionell förändring som lämpar sig väl för manipulation, där målet är att främja de egna strategiska intressena som ett led i konkurrensen med andra länder.

En rad länder ägnar sig åt politisk krigföring 2.0. Men omfattningen och framgången i Rysslands agerande sticker ut. Under kalla kriget bedrev Sovjetunionen politisk krigföring på bred front. I dag bedriver Ryssland liknande kampanjer där kraft hämtas från nätet.

Arenan vidgas

Sommaren 2010 påbörjades ett nytt kapitel inom politisk krigföring 2.0 när det avslöjades att Irans kärnvapenprogram saboterats med hjälp av internet-trojanen Stuxnet. USA och Israel ansågs ligga bakom sabotaget, som visade att verklig skada kan åsamkas i relativt enkla fysiska system med hackermetoder (bland annat programmerades urananriktnings-centrifugerna till att snurra fortare än designen tillät och därmed slitas ut). Kunde centrifuger förstöras i slutna bergrum i Iran

kunde hissar, luftreningssystem, kylaggregat och vattenreservoarer förstöras och manipuleras i princip var som helst. Skadan kunde i värsta fall bli densamma, eller större, som vid ett fysiskt militärt angrepp. Med Stuxnet hade arenan för politisk krigföring vidgats.

Cyberverktyg kan användas direkt och indirekt för militära ändamål. Stuxnet är ett tydligt exempel på detta, men arenan för politisk krigföring vidgas i ytterligare två riktningar: dels riktas den politiska krigföringen 2.0 mot en större del av samhällskroppen. Dels används arenan av fler aktörer.

Iran och Nordkorea exemplifierar båda dessa riktningar. Vintern 2016 hackade Iran det amerikanska kasinoföretaget Las Vegas Sands Corporation sannolikt eftersom bolagets ägare uttryckt åsikter som ledarna i Teheran ogillade.[61] Landet outsourcar hackertjänster enligt en modell som påminner lite om svensk upphandling av offentliga tjänster, till specialister som kanske inte ens känner till uppdragsgivarens identitet. Iran agerar alltmer i linje med vad som kan förväntas av ett land som bedriver politisk krigföring 2.0. Detta gäller även Nordkorea.

I slutet av 2014 hackade Nordkorea via gruppen *Guardians of Peace* filmbolaget Sony Pictures Entertainment. Orsaken: en kommande komedi om ett lönnmord på Nordkoreas diktator Kim Jong-Un. Filer förstördes, filmmanus och information om enskilda medarbetare stals. Premiären av filmen *The Interview* fick ställas in med kort varsel även i Sverige.[62]

61 Denning (2017).

62 Criminal Complaint (2018).

Både Irans och Nordkoreas agerande syftar till att straffa och avskräcka enskilda bolag, men också till att avskräcka andra aktörer från att kritisera eller på annat sätt försöka undergräva regimernas auktoritet. Tidigare saknade, ur ett globalt perspektiv, svagare länder aptit och förmågan att ge sig på enskilda intressen hos konkurrerande länder. Nu har detta ändrats.

Kina agerar också mer utåtriktat, ytterligare ett exempel på att internet öppnar upp arenan för politisk krigföring. Enligt Freedom House bedriver Kina informationskampanjer över internet i 36 av de 65 länder som organisationen undersökt. Ett två veckor långt seminarium för representanter från länder i anslutning till Kinas satsning the Belt and Road Initiative är en indikation på den nya inriktningen. Kina har naturligtvis all rätt att informera, det intressanta är vad som sägs. Seminariet innehöll information gällande verktyg för att mäta negativa opinioner i realtid och ett ”posivite energy public-opinion guidance system”.[63] Utvecklingen kan ha betydelse även för Sverige. Enligt forskare från Totalförsvarets forskningsinstitut (FOI) kan Kina ha testat gränserna för vad som kan göras när tre kinesiska medborgare avvisades från ett hotell i Stockholm hösten 2018. Kinesiska representanter reagerade kraftigt mot Sverige som förklarades osäkert för kinesiska medborgare och kritiserades i media.[64]

Trycket ökar

Inget land kan hålla sig borta från de höjda konfliktnivåerna på nätet, inte heller Sverige. Enligt Försvarets radioanstalt

63 Freedom House (2018).

64 Wong (2018).

(FRA) drabbas vårt land av tiotusentals cyberattacker varje månad,[65] inofficiellt kan det röra sig om mellan tusen och femtusen attacker per dygn enligt andra experter. Detta har fått näringslivet, en av de stora måltavlorna vid angreppen, att reagera: ”Sverige är redan ockuperat” har Saabs koncernchef Håkan Buske konstaterat.[66] Och kanske påminner situationen om ett militärt angrepp? Utifrån en strikt tolkning är Sverige naturligtvis inte ockuperat. Men med det sagt utmanas Sverige och andra länder av att cyberhotet ritar om den internationella säkerhetskartan.

För att avsluta del I: Cyberhotet består av krafter som digitaliseringen har släppt lös. Cyberhotet växer i takt med digitaliseringen, står nära auktoritära ideal och kontrolleras inte särskilt väl av samhället och näringslivet. Cyberkriminalitet, ekonomiskt cyberspionage och politisk krigföring 2.0 är numera att räkna med. Trycket ökar dessutom då cyberhotet är i en uppåtgående trend.

65 FRA (2017).
66 Lindahl (2018).

DEL II

Konsekvenser

Kalla krigets auktoritära tankegods försvann under rasmassorna av Berlinmuren och historien var vid sin vägs ände, trodde vissa. Men historien tog naturligtvis inte slut i november 1989. Auktoritära krafter är ånyo på frammarsch och den liberala världsordningen är återigen satt under press. Hur kunde stämningsläget skifta så snabbt? Det finns naturligtvis många förklaringar, men kanske kan också cyberhotet hjälpa oss att förstå. Kanske spelar cyberkriminalitet, ekonomiskt cyberspionage och politisk krigföring 2.0 större roll för den liberala världsordningens kris än vad de flesta tidigare anat?

Liberalismens kris förklaras sällan närmare i förhållande till cyberhotet, men kanske borde den göra det. För trots allt har cyberhotet ökat parallellt med att liberalismens problem vuxit. Ryssland exempelvis, som kanske är den mest aktiva aktören inom politisk krigföring 2.0, gör alls ingen hemlighet av sina intentioner att skjuta den liberala världsordningen i sank. Inte heller Kinesiska kommunistpartiets företrädare tycks oroa sig över den liberala världsordningens svåra tid, lika lite som cyberkriminella, mullorna i Iran eller ledarna i Nordkorea.

Cyberhotet väger tungt på den liberala världsordningen och utmanar liberala principer och förutsättningar ur åtminstone tre hänseenden: för det första försvagas samhällskontraktet när tilliten sjunker, för det andra avkrävs i praktiken en tull på ekonomiskt välstånd och för det tredje utmanas folkstyret av den starkes rätt.

Samhällskontraktet försvagas, tilliten sjunker

”Land skall med lag byggas, eller gå under med laglöshet” [67] står det att läsa i *Njals Saga* från 1200 talet – den längsta och kanske mest citerade av de isländska sagorna. Gäller inte detta även internet? Internet är inte ett land i fysisk mening, men kan ändå betraktas som ett digitalt land med egen funktion och rätt.

Samhällskontraktet har på senare tid blivit ett omdiskuterat ämne i den politiska debatten. Graden av finess varierar. ”Vad f-n får jag för pengarna?” utbrast Leif Östling och fick lämna posten som ordförande för Svenskt Näringsliv. Arrogansen retade många, samhällskontraktet har betydelse och bör behandlas med respekt. För även om kontraktet inte existerar i fysisk mening håller det ihop samhället. Samhällskontraktet innebär i praktiken att fria individer ger upp en del av sitt självbestämmande till en gemensam instans, staten. Den demokratiska staten är vår tids *Leviathan*, om vi lånar ordet från filosofen Thomas Hobbes, som hanterar spelreglerna i samhället och upprätthåller en rättsordning. Utan ett fungerande samhällskontrakt äventyras samhällsordningen. Finns ingen Leviathan hamnar människan enligt Hobbes berömda porträtt i ett naturtillstånd som innebär anarki och ett allas krig mot alla där livet blir ”solitary, poor, nasty brutish and short”.[68]

Erik Schmidt (som citerades i början av del I av denna skrift) hade möjligen en poäng: Internet kanske är ett stort experiment i anarki. Hur påverkar det i sådana fall samhällskon-

67 Njal (1280).

68 Hobbes (1651) kapitel 12.

traktet? I dag är hackade användarkonton på sociala medier, bankbedrägerier och utpressning över nätet så vanligt förekommande att vi knappt reagerar när vi varnas för dem. Demokratiska val kan knappt längre genomföras utan att de misstänkliggörs på grund av orsaker som har med internet och cyberhot att göra. Det är svårt att avgöra om dagens opinionsbildning genomförs via botar eller riktiga människor på Twitter. Vem vet med säkerhet om de utsatts för falska nyheter och riktade kampanjer på nätet från främmande makt, eller i vilken grad de påverkats? Hur kan vi veta att etablerade medier inte springer andras ärenden utan att vara medvetna om det? I en värld där ”inget är sant och allting är möjligt” är det lätt att drabbas av intrycket att ingen går säker.

Hackade användarkonton och personuppgifter drabbar en betydande del av befolkningen. När hackandet sker inför öppen ridå och drabbar kända företag och demokratiska institutioner kan vi nog utgå från att det påverkar det allmännas medvetande på ett sätt som inte främjar bilden av ett starkt samhällskontrakt. När ekonomiskt cyberspionage drabbar många företag samtidigt, som Operation Cloud Hopper, uppstår en osäkerhet som går långt bortom ägarna och styrelsen i de drabbade bolagen – det påverkar samhället i stort. Att enskilda medborgare drabbas av cyberbrottslighet privat eller på sina arbetsplatser utan att få institutionellt stöd underminerar samhällskontraktet.

I slutändan sjunker tilliten, som fyller en viktig funktion i samhället: Inte minst funktionen att bygga upp länders sociala kapital. Enligt Francis Fukuyama är socialt kapital ”the ability of people to work together for common purposes in

groups and organizations".[69] Socialt kapital är en flyktig tillgång som lätt försvinner om tilliten minskar. Tänk bara på den sjunkande tilliten i USA och polariseringen där mellan demokrater och republikaner som diskuterades ovan.

Näringslivets betydelse för tilliten i samhället är ett annat belysande exempel. Tillit är en avgörande rekvisit i affärssammanhang, för i slutändan handlar affärer om mänskliga relationer. Här har framväxten av cyberhot ställt till problem: Kan du veta säkert att mailet från din kollega inte kommer från en hackare? Kan du tryggt installera den där nya produktionsenheten och vara säker på att den inte innehåller en trojan som installerats av en anställd hos en underleverantör? Kan företag lita på att de inte har köpt en server med avlyssningsutrustning? Eller kan kunden lita på att företaget i hemlighet inte samlar in data om personuppgifter?

Varken företag eller kunder vet med säkerhet svaret på dessa frågeställningar – därför sker en anpassning för att kompensera. Marknaden för cybersäkerhet växer snabbt, globalt har den multiplicerats 35 gånger under de senaste tretton åren.[70] Trots det upplever företag att de behöver satsa ännu mer på säkerhet. Enligt företagen själva, i en amerikansk studie av Barkly, saknar två tredjedelar av de undersökta företagen de resurser som krävs för effektiv cybersäkerhet.[71] Situationen är likartad för europeiska företag och globalt bedöms cybersäkerhetsmarknaden växa upp till 12 procent årligen fram till 2022 (CAGR).[72]

69 Fukuyama (1995) s 10.
70 Morgan (2017).
71 Barkly (2018).
72 Morgan (2017).

Poängen är att när cyberhotet växer ökar risken att tilliten sjunker och samhällskontraktet försvagas. Eftersom samhällskontraktet utgör en del av grunden för den liberala världsordningen har det betydelse för fler än de företag och individer som drabbats.

Tull på ekonomiskt välstånd

Gränsdragningen mellan ekonomi och nationell säkerhet suddas ut. Cyberhotet är att likna vid en tull på ekonomiskt välstånd, dels genom direkta effekter av ekonomiskt cyberspionage och dels genom att cyberhotet förstärker byråkratiska och teknokratiska instinkter.

Länder som drabbas av ekonomiskt cyberspionage berövas ekonomiskt välstånd, företagshemligheter kan inte stjälas utan att det får ekonomiska konsekvenser för de som drabbas. Naturligtvis främjas ekonomiskt välstånd av internet och digitalisering, men cyberhotets kostnader manifesteras till exempel i form av minskade resurser att investera i nya produkter och arbetstillfällen. Ekonomiska förluster ackumuleras också över tid. Företag kan tvingas bort från marknader helt och hållet. Ekonomiskt cyberspionage bidrar inte med ekonomiska värden, det flyttar värde från en part till en annan.

Cyberhot förstärker också teknokratiska instinkter i en tid när sådana redan tar stor plats inom företag. Författaren och *Economist*-skribenten Adrian Wooldridge satte huvudet på spiken när han försökte beskriva liberalismens kris i artikeln ”Some thoughts on the crisis of liberalism – and how

to fix it".[73] Artikeln målar bilden av ett liberalt samhällssystem som begränsas av teknokratiska instinkter och av den anledningen fungerar sämre och inte längre är lika bra på att lösa samhällsproblem. Detta spiller över på förmågan att skapa ekonomiskt välstånd. En form av samhällsystem har växt fram (eller kanske man kan säga en form av kapitalism) som förlorat sin tidigare kraft och är mindre dynamisk och inte längre är föränderlig och därmed är sämre på att generera ekonomiskt välstånd. För att låna från Hayek: det är som om kapitalismen "largely lost faith in the traditions that have made it what it is".[74]

Produktivitetstillväxten till exempel, som förenklat mäter ekonomins förmåga att använda sina resurser smartare, har sjunkit i stora delar av västvärlden under lång tid och inte minst i Sverige. En annan konsekvens är att byråkratiseringen av näringslivet tilltar. Enligt Boston Consulting Group har företagens byråkratisering ökat med sju procent per år det senaste halvseklet. Anställda har sedan länge haft att förhålla sig till alltmer kringgärdande förutsättningar, från detaljerade arbetsprocesser till förutbestämda beslutsparametrar – och möten. Omkring 60 procent av arbetstiden för chefer går åt till att möteskoordinera.[75] Till detta läggs nu ytterligare teknokratiska åtgärder för att bemöta cyberhotet.

Teknokratisk styrning som leder till ökad byråkratisering präglar hanteringen av cyberhot. Anställda anser redan att byråkratiseringen från cybersäkerhet hämmar företagens

73 The Economist, Bagehot (2018).
74 Hayek (2006) s 2.
75 Erixon & Weigel (2016).

utveckling. Tre fjärdedelar av IT-cheferna i en studie anser att cybersäkerhet och restriktiva IT-regler hämmar produktivitet och innovation.[76]

Till detta adderas krav på att företag ska stödja statens säkerhetsarbete. Enligt Försvarsberedningen från 2017 finns lagstadgade krav på näringslivets deltagande i totalförsvarsplaneringen och det torde inte undanta cyberområdet.[77] Ökade cyberförsvarskapaciteter inom näringslivet innebär dock att resurser läggs på teknokratiskt cyberförsvar och att uppmärksamhet läggs på annat än att utveckla de affärsverksamheter som i slutändan genererar ekonomiskt välstånd.

Folkstyret utmanas av den starkes rätt

Slutligen förstärker cyberhotet den auktoritära lockelsen i relation till folkstyret – cyberhotet är en dragning mot den starkes rätt. Länder som står och väger mellan demokrati och auktoritära samhällssystem där den starkes rätt råder inspireras av auktoritära regimer som Kina och Ryssland. Turkiet, Ungern och Rumänien är till exempel alla länder som befinner sig i gränslandet mellan demokrati och auktoritärt styre och där demokratin har backat från 2006 fram till i dag enligt tidningen *Economists* demokratiindex.[78]

Auktoritärt tankegods hotar att tippa ned samhällen i den auktoritära avgrunden, konstaterade Anne Applebaum i artikeln ”A Warning From Europe: The Worst Is Yet to Come”.[79]

76 Wood (2017).
77 Försvarsdepartementet (2017) s 137-142.
78 The Economist Intelligence Unit (2018).
79 Applebaum (2018a).

Och många aspekter förknippade med internet och cyberhotet hjälper till. Ofta påpekas hur internet undergräver demokratin eftersom nätet polariserar och underlättar förekomsten av exempelvis konspirationsteorier, eller att nätet är en tillflyktsort för extrema politiska idéer som kan frodas parallellt utan att konfrontera varandra. Delvis ligger det något i detta, men en viktigare konsekvens av cyberhotet handlar om något annat.

Den starkes rätt trumfar folkstyre på nätet. Hösten 2018 larmade organisationen Freedom House att friheterna på nätet för åttonde året i rad, lika länge som organisationen studerat utvecklingen, begränsas och att digital auktoritarism breder ut sig och hotar demokratin. Spridning av falska nyheter angavs som en orsak, och med ny teknik, som deep fakes, där vi inte längre kan avgöra vad som är sant och falskt, försämras förutsättningarna för att fakta ska få en framträdande roll.[80] Auktoritära krafter tar många skepnader på nätet, på sikt får vi nog också vänja oss vid risken att även företag, som investerar tungt i cybersäkerhet, kan agera med allt större auktoritär pondus och utmana folkstyrets principer. Företag investerar i cybersäkerhet och det får konsekvenser.

Det förstärker det auktoritära. I den fysiska världen anpassas militära kapaciteter till attack eller försvar men på nätet återfinns inte samma tydliga skiljelinje. Försvarsförmågor är svåra att urskilja från attackförmågor. Företag som utvecklar sitt cyberförsvar blir därmed också bättre på att exempelvis censurera och påverka politiska opinioner, hacka konkurrenter och initiera DDoS-attacker. De utvecklar också kom-

80 Freedom House (2018).

petenser inom marknadsföring med hjälp av metoder som liknar politisk krigföring 2.0, och har tillgång till produkter som i orätta händer kan orsaka skada och kan säljas till mindre nogräknade aktörer. I goda tider är problemet mindre, men vad händer när företag går sämre och kanske blir mer angelägna att kapitalisera på sina tillgångar? Företag och organisationer med växande cyberarméer riskerar att bli auktoritära krafter i sin egen rätt.

Problemet ska inte överdrivas, men trenden bör heller inte enkelt viftas bort. Vi är inte i ett akut läge där folkstyret löper omedelbar risk att tippas ned i den auktoritära avgrunden till följd av utvecklingen mot den starkes rätt på nätet. Men det finns heller ingen Berlinmur som snart kommer att kollapsa över auktoritära ideal, och trots allt avskräcker historien. Njal själv exempelvis blev föremål för den starkes rätt när han den tredje september år 1011, i ett land utan lag och rätt, brändes ihjäl i sitt hem tillsammans med sina söner.

DEL III

Åtgärder

Cyberhotet handlar om negativa krafter som växer sig starkare tack vare internet och digitalisering. Trenden måste brytas. Sverige kan inte själv lösa problemet – åtgärder förutsätter internationell samordning. Med detta sagt, vad mer kan samhället och näringslivet göra?

På senare tid har EU fattat en rad beslut om regleringar och resurskoordinering som också berör Sverige. EU:s allmänna dataskyddsförordning (GDPR) infördes i maj 2018. Lagen är tänkt att garantera gemensamma spelregler för dataskydd mellan EU:s medlemsländer samtidigt som personskyddet stärks. Augusti 2018 infördes regler om informationssäkerhet för samhällsviktiga och digitala tjänster som berör leverantörer av kritisk infrastruktur. En ny säkerhetsskyddslagstiftning träder i kraft i mars 2019 och delar av EU-direktivet för nätverks- och informationssystem (NIS) avser att förbättra cybersäkerheten. Gemensam certifiering blir del av svensk lag. EU har tagit fram ett ”Blueprint” för gemensamt agerande vid större attacker och en ”cyber diplomatic toolbox” för diplomatiska reaktioner. Unionen arbetar också för en effektivare delning av kunskaper och resurser mellan medlemsländerna.

På teknikområdet utvecklas motmedel. Ständigt skapas nya produkter och tjänster, som säkerhetsprogram, antivirusteknik, aktiva skyddsprogram, metoder för informationshantering och system för användarvänlig säkerhet. Om det finns vinnare på cyberhotet tillhör alla de företag som säljer skyddande tjänster och produkter den kategorin. Tekniken är delvis till hjälp mot i första hand mindre avancerade hot, men den är begränsad. ”Den olyckliga verkligheten är att troligtvis under

det närmaste decenniet kommer cyberkapacitetsförmågorna hos våra mest kapabla motståndare att överträffa USA:s förmåga att försvara kritisk infrastruktur", konstaterade Defence Science Board (DSB, rådgivare till det amerikanska försvarsdepartementet).[81] Om så är fallet i USA, som är ledande inom cybersäkerhet, gäller det i ännu större utsträckning för andra länder och företag i väst – Sverige icke undantaget.

De åtgärder som vidtagits inom EU och teknikutvecklingen gör säkert viss nytta, men det är tveksamt om de räcker. De flesta experter är överens om att cyberhotet kommer fortsätta att öka, och därmed fördjupas också de negativa konsekvenserna. Om vi antar att experterna har rätt måste samhället och näringslivet göra mer. Det finns många tillämpbara åtgärder, men innan dessa implementeras måste först två grundantaganden utmanas:

1) "Cyberhotet är ett tekniskt problem"

En stor del av det som sker när det gäller att bemöta cyberhotet utgår från antagandet att det är ett tekniskt problem, vilket i sig är tveksamt. Som denna rapport illustrerat förefaller snarare cyberhotet vara mer av ett politiskt och ekonomiskt problem. Politisk krigföring 2.0 och ekonomiskt cyberspionage utgår från kända aktörer med politiska respektive ekonomiska intressen – internet råkar vara en av de arenor de använder.

2) "Cyberhotet är övergående"

Det andra grundantagandet är att cyberhotet är övergående. De vanliga argumenten som framförs här är att ny teknik

81 Defense Science Board (2017), s 5.

snart kommer att åtgärda nätets säkerhetsbrister för gott, eller att aktörerna kommer att ändra sina beteenden. Detta är ett tveksamt antagande. Historiskt är det svårt att hitta belägg för att utvecklingen följer en sådan logik. Det går på tvärs mot vad vi vet om hotaktörerna och mot vad vi vet om digitaliseringen. Emellanåt hörs liknelsen att nätets säkerhetsbrister är lika svåra att åtgärda som att laga ett punkterat däck på en bil som fortfarande rullar, men det stämmer inte. Det räcker inte med däcken. Ett helt säkert internet är i praktiken ouppnåeligt eftersom det förutsätter att bilens motor och chassi, ja det mesta faktiskt, byggs om från början.

Om dessa två grundantaganden frångås kan samhället vidareutveckla redan sjösatta åtgärder och överväga att pröva nya. Tre områden diskuteras här: att värna samhällets integritet, att anpassa åtgärder och att värna balansen i det ekonomiska maskinrummet.

Värna samhällets integritet

Öppna samhällen och näringslivet kastade sig huvudstupa in i den digitala tidsåldern, oförberedda på vilka förändringar och hotbilder som väntade. Snart tre decennier in i den nya eran är det hög tid att på allvar värna samhällets integritet på nätet. Det måste ske långsiktigt och syfta till ett stabilt och robust förhållande som står sig även på sikt. Anpassningen behöver ske på flera nivåer: från individnivån som avgörs av enskildas hantering av digital information, till systemnivå inom stater och institutioner som EU där det behövs effektivare beslutsvägar, tydligare rollfördelning, bättre processer för att utvärdera konsekvenser och att utveckla motåtgärder.

Ingen enskild åtgärd kan lösa alla problem, men oavsett vilka åtgärder som vidtas krävs ökade och fördjupade kunskaper i hela samhället om cyberhotet och dess konsekvenser. Breda utbildningsinsatser bör därmed initieras. Varför inte söka inspiration och erfarenheter av svenska folkbildningskampanjer? Detta skulle kunna bidra till att sprida kännedom om problemet även i de bredare folklagren. Utbildningsinsatserna bör samordnas internationellt: ökade kunskaper hos våra viktigaste handelspartners även utanför EU liksom hos ideologiskt och geografiskt närliggande stater gynnar även oss.

Ett konkret sätt att öka kunskapen hos beslutsfattare vore att utveckla effektivare forum som för samman aktörer från näringslivet och politiken i strategiska samtal kring hur samhället tillsammans kan bemöta cyberhotet på längre sikt.

Anpassa åtgärder

Åtgärder riskerar att bli oprecisa och förlora i verkningsgrad när hotaktörer buntas ihop. Det gäller också motåtgärder som behöver anpassas beroende på hot och efter respektive politiska och ekonomiska arenor. Verkningsfulla åtgärder innebär också att de sträcker sig bortom ord och protester, i värsta fall kan sådant annars snarast förstärka problemet. Ett exempel på åtgärd är att attribuera – som är att tillskriva ansvar i samband med cyberkriminalitet, ekonomiskt cyberspionage och politisk krigföring 2.0 – kopplat med påföljder.

I vissa fall kan tillskrivandet av ansvar dämpa de anklagades handlingsutrymme. I andra fall kan det få direkt motsatt effekt, särskilt om attribuerandet inte följs upp av påföljder.

Antagonistiska aktörer bakom ekonomiskt cyberspionage, till exempel, vill ogärna vidkännas skuld om det samtidigt innebär risk för ekonomiska sanktioner, åtminstone är det intrycket efter att USA efter påtryckningar lyckades få till stånd stoppavtalet med Kina. Tillskrivande av ansvar måste dock följas upp tydligare än i dag så att företag och länder som tjänar på ekonomiskt cyberspionage avskräcks med större kraft. Här går det att tänka sig flera åtgärder, inklusive att försvåra kommersialisering, erbjuda statligt stöd till företag i juridiska processer mot både stater och företag, införa strafftullar mot företagsägare och konfiskera tillgångar. Varor och tjänster tydligt kopplade till ekonomiskt cyberspionage får inte vara lika enkla att marknadsföra och sälja som i dag. Så länge åtgärder inte vidtas som faktiskt ändrar beteenden har västvärlden i praktiken accepterat förekomsten av ekonomiskt cyberspionage.

När det gäller politisk krigföring 2.0 är det inte lika säkert att tillskrivande av ansvar har positiv effekt, i synnerhet inte utan konkreta åtgärder. Ta exemplet Ryssland: Förvisso förnekar Ryssland närmast rutinmässigt inblandning även när landets kampanjer inte kan bortförklaras med trovärdighet. Men samtidigt kan tillskrivande av ansvar hjälpa att driva igenom önskvärda beteenden hos Rysslands motståndare. Ett land som förknippas med vissa kompetenser kan göra andra mer fogliga – det påminner om hur vissa cyberkriminella gärna tillskrivs ansvar för cyberattacker de ej genomfört eftersom det förstärker deras status. Dessutom riskerar varje uppenbar aggression från rysk sida som enbart bemöts med verbala protester att fungera som bevis för att västvärlden är svag och inte förmår försvara sina egna intressen.

Anpassade påföljder för politisk krigföring 2.0 kräver politisk beslutsamhet. De som studerar kalla krigets historia inser snabbt att det inte var undfallenhet mot Sovjetunionen som gjorde att kalla kriget inte utvecklades till ett hett krig. Västeuropas integritet upprätthölls inte av att man lät Sovjet provocera ens grannländer, utan av att västmakterna stod upp mot provokationer. I samma anda krävs i dag politisk beslutsamhet och tydlighet för att bemöta politisk krigföring 2.0. För Sveriges del skulle det kunna bestå av att fördjupa underrättelsearbetet inom pågående samarbeten och att med större beslutsamhet verka för att den politiska kostnaden för att bedriva politisk krigföring 2.0 ökar inom EU, FN och Världshandelsorganisationen.

Värna balansen i det ekonomiska maskinrummet

Auktoritära krafter utmanar den liberala världsordningen och det liknar alltmer en konflikt som kommer att definiera internationella relationer under lång tid, och eftersom konflikter normalt vinns av den som har störst konfliktkassa bör länder i väst vårda sitt ekonomiska välstånd. Det ställer dock flera krav, till exempel på en balansgång mellan att tillåta ett fritt internet och att stoppa cyberhotet med till exempel regleringar och övervakning. Om internet regleras för mycket riskerar välståndet att drabbas. Dessutom är det inte säkert att regleringar alltid hjälper. Om internet däremot regleras för lite riskerar cyberhotet att öka.

Cybersäkerhet handlar inte främst om säkerhet utan om säkerhet *och* användarvänlighet. En balans förutsätter å ena sidan att marknadskrafter tillåts verka och har tillräckligt stort utrymme och inte begränsas av exempelvis övernitiska

regleringar, hur välmenande de än kan vara. I sin iver att mildra cyberhotet får inte samhället strypa kapitalismens och marknadsekonomins förmåga att skapa ekonomiskt välstånd. Digitaliseringen befinner sig fortfarande i en tidig fas, av det totala värdeskapandet mätt i andel av den totala BNP representerar den digitala ekonomin cirka 25 procent inom EU.[82]

Men ett fungerande internet förutsätter att nätet är tillräckligt säkert och det motiverar en viss inskränkning av frihetsgraden. Sverige kan även nödgas undersöka att tillsammans med likasinnade stater i väst skärma av delar av nätet för vilka cyberhotet är extra framträdande – även om det naturligtvis är förknippat med mycket stora tekniska, affärsmässiga och sociala utmaningar. Trots allt pågår redan i praktiken en form av uppdelning av nätet från vissa länder.

Det finns också andra sätt att värna balansen och vårda det ekonomiska välståndet. Ett exempel är att inte begränsa marknadsekonomins mekanismer från att hantera risker, såsom försäkringar. Försäkringar är marknadsekonomins metod för att skapa vertikal dämpning av risker i den mening att kostnader som uppstår absorberas i flera led bakåt från en incident. I dag är endast femton procent av företagens potentiella kostnader för cyberhotet försäkrade. Inom fastigheter är andelen närmare 60 procent.[83] När andelen ökar blir företagen bättre rustade att hantera ekonomiska förluster från cyberhotet. I praktiken är detta också ett sätt att fylla på konfliktkassan.

82 Accenture (2016).

83 The Economist (2018).

Slutligen

”När hela mänskligheten kopplade upp sig, inklusive de sämsta av oss, var jag naiv när jag trodde att den ryska maffian (eller den ryska regeringen för den delen) skulle bry sig särskilt mycket om konsensuella system för det allmännas bästa.”[84] Så gjorde John Perry Barlow avbön tjugo år efter forumet i Davos och ”Declaration of the Independence of Cyberspace”.

Auktoritära krafter accelererar sina försök att via nätet forma världen efter eget tycke och smak. De goda nyheterna är att västländerna äger kapaciteter för att hindra att cyberhotet växer, och att fördelarna med digitaliseringen fortfarande trumfar nackdelarna. Men med det sagt: En idealiserad bild av digitaliseringen leder fel. Digitaliseringens negativa krafter får konsekvenser för tilliten och samhällskontraktet, det ekonomiska välståndet och folkstyret, vilka ger den liberala världsordningens kris ytterligare en skjuts. Cyberhotet är här för att stanna, trenden är tydlig, riktningen är inte den önskvärda och det blir allt svårare att påstå att vi ingenting visste.

84 Thente (2018).

Referenslista:

Accenture (2016), *Unlocking the Digital Potential of Industries Across Europe,* Accenture Strategy

Aglionby, John, Feng, Emily, Yuang, Yuan (2018), ”African Union accuses China of Hacking headquarters”, 29 januari, *The Financial Times*

Albright, Madeleine (2018), *Fascism A Warning*. London: Harper Collins

Anderson, Mark (2017), ”Radar Summit 2017”, Radar https://youtu.be/7DotZlOhh6A

Applebaum, Anne (2018a), ”A Warning From Europe: The worst Is Yet To Come”, October issues, *The Atlantic*

Applebaum, Anne (2018b), ”Russian hackers were caught in the act – and the results are devastating”, 5 oktober, *Washington Post*

Barkin, Noah (2018), ”German officials sound China alarm as 5G auctions loom”, 13 november, *Reuters*

Barkly (2018), ”10 Must-Know Cybersecurity Statistics for 2018”, februari, Barkly, Ponemon Institute

Chambers, John (2015) ”What does the Internet of Everything mean for security” 21 januari, World Economic Forum

Choudhury, Saheli Roy, Kharpal, Arjun (2018) ”The ‘deep web’ may be 500 times bigger than the normal web. Its uses go well beyond buying drugs”, 6 september, *CNBC*

Cimpanu, Catalin (2018), ”Maersk Reinstalled 45,000 PCs and 4,000 Servers to Recover From NotPetya Attack”, *25* januari, *Bleepingcomputer News*

Cisco, (2018) ”Cisco 2018 Annual Cybersecurity Report Reveals Security Leaders Rely on and Invest in Automation, Machine Learning and Artificial Intelligence to Defend Against Threats”, San Jose

Clapper, R. James (2018), *Facts and Fear – Hard Truths From A Life In Intelligence*. New York: Viking

Criminal Complaint (2018), ”Case No: MJ 18-1479”, 8 June, *United States District Court*

CSIS (2018), *Economic Impact of Cybercrime – No Slowing Down,* februari, Santa Clara CA: McAfee

Defense Science Board (2017), ”Department of Defense, Defense science Board, Task Force Cyber Deterrence, Office of the Under Secretary of Defence for Acquisition, Technology, And Logistics”, februari 2017, Washington, D.C.

Demchak, C. Chris, Shavitt, Yuval (2018), ”China’s Maxim – Leave No Access Point Unexploited: The Hidden Story of China BGP Hijacking”, *U.S. Naval War College*, Volume 3, Issue 1, Tel Aviv University

Denning, Dorothy (2017) ”Iran´s Cyber Warfare Program Is Now A Major Threat to The United States”, 12 december, *Newsweek*

Department of Defense (2018), ”Cyber Strategy 2018”, USA

Edelman (2018), ”Edelman Trust Barometer The 18th annual trust and credibility survey”, Edelman Inc.

Erixon, Fredrik, Weigel, Björn (2016), *The Innovation Illusion – How So Little Is Created By So Many Working So Hard.* London: Yale University Press

Europol (2017), *Serious and Organised Crime Threat Assessment*, European Union Organised Crime

Försvarsdepartementet (2017), *Motståndskraft – Inriktningen av totalförsvaret och utformningen av det civila försvaret 2021–2025,* DS 2017:66

FRA (2017), Årsrapport 2016, Försvarets Radioanstalt

Freedom House (2018), ”Freedom on the Net 2018 – the rise of digital authoritarianism”, oktober, *Freedom House*, Washington

Fukuyama, Francis (1995), *Trust: the social virtues and the creation of prosperity*. New York: Simon & Schuster Inc

Goodman, Marc (2015), *Future Crimes, Inside The Digital Underground And The Battle For Our Connected World*. London: Penguin Random House

Hatmaker, Taylor (2015), “Four years later, Yahoo still doesn’t know how 3 billion accounts were hacked”, Tech Crunch

Hayek, F.A (2006), *The Constitution of Liberty*. Chicago: Routledge

Hegarty, Chuck, Ferreira, Jose, Grahn, Anne (2018), *8 Cybersecurity Trends for 2018*, 11 january, Sirius

Hiscox (2017), *The Hiscox Cyber Readiness Report*, Hiscox Insurance Company, London

Hobbes (1651), *Leviathan*, kapitel 12

ICA (2007), ”Assessing Russian Activities and Intentions in Recent US Elections”, 6 januari, Office of the Director of National Intelligence, Intelligence Community Assessment

Internet Hall of Fame (2018), ”A Declaration of the Independence of Cyberspace”

IP Commission Report (2017), *The Theft of American Intellectual Property: Reassessment of the Challenge and United States Policy*, The National Bureau of Asian Research

Ismail, Nick (2018), ”Cyber security leaders concerned about sharp rise in digital threats”, 14 februari, Information Age

Jing, Meng (2017), ”China plans network of ‘influential’ cybersecurity schools”, 16 augusti, *South China Morning Post*

Kania, Elsa, Sacks, Samm, Triolo, Paul, Webster, Graham (2017), ”China’s Strategic Thinking on Building Power in Cyberspace”, 25 september, *New America*

Kaspersky (2015), ”Carbanak APT: The Great Bank Robbery” februari, Kaspersky Lab HQ

Kerravala, Zeus (2015), ”John Chambers’ 10 most memorable quotes as Cisco CEO”, 24 juli, *Networkworld*

Kozy, Adam (2018), ”Two Birds, One STONE PANDA”, 30 augusti, Crowdstrike

Lindahl, Björn (2018), ”Saabs vd: Sverige är redan ockuperat”, 1 juni, *Svenska Dagbladet* Näringsliv

Marr, Bernard (2018), ”How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read”, 21 maj, *Forbes*

Matsuda, Ayako, Muhammad, Irshad (2018), “APT10 Targeting Japanese Corporations Using Updated TTPs”, 13 september, *FireEye*

McKinsey (2017), ”Staying ahead on cyber security”, januari, McKinsey & Company

Morgan, Steve (2017), ”2017 Cybercrime Report”, 18 oktober, *Cyber Security Ventures*

Morgan, Steve (2017), ”Cyber Security Market Report”, 31 maj, *Cyber Security Ventures*

Morse, Sir Amyas (2017), ”Investigation: WannaCry cyber attack and the NHS”, 27 oktober Department of Health, National Audit Office, beställd av House of Commons

Mueller, S. Robert (2012), ”RSA Cyber Security Conference”, 1 mars, Federal Bureau of Investigation

Nakashima, Ellen, Sonne, Paul (2018), ”China hacked a Navy contractor and secured a trove of highly sensitive data on submarine warfare”, 8 juni, *Washington Post*

NCSC (2018), ”Foreign Economic Espionage Cyberspace”, 24 juli, National Counterintelligence Security Center

Negishi, Maymi (2018), ”Japan Scrutinizes China’s Huawei, ZTE Over Spying Fears”, 30 augusti, *The Wall Street Journal*

Newman, Peter (2018), ”IoT Report: How Internet of Things technology is now reaching mainstream companies and consumers”, 27 juli, BI Intelligence

News (2018), ”Russia tried to hack the official investigation into the downing of MH17”, 4 oktober. News.co.au

Nial (1280), *Nials Saga*, Icelandic Saga database, Sveinbjorn Thordarson, sagadb.org

Pew (2017), ”The partisan divide on Political Values Grows Even Wider”, 5 oktober, Pew Research Center

Poe, Ted (2018), ”China’s Predatory Trade and Investment Strategy”, 11 juli, Committee on Foreign Affairs House of Representatives, Serial No. 115–149, Washington

Polyakova, Alina, Laruelle, Marlene, Meister, Stefan, Barnett, Neil (2016), ”The Kremlins Trojan Horses, Russian Influence in France, Germany, and the United Kingdom”, november, Atlantic Council Policy on Intellectual Independence

Pomerantsev, Peter (2017), *Nothing is True and Everything is possible*. London: Faber & Faber

PwC (2017), ”Operation Cloud Hopper”, PWC & BAE Systems

PwC blogs (2017), ”For CEOs, cybersecurity is both rising concern and significant opportunity”, 23 mars, PWC

Richards, Kevin, LaSalle, Ryan, Devost, Matt, Van den Dool, Floris, Kennedy-White, Josh (2017), *Cost Of Cybercrime Study*, Accenture, Ponemon Institute: Michigan, USA

Risky (2018), ”Risky Business #502 – Inside China’s hacker scene”, https://risky.biz/RB502/

Rogin, Josh (2012), ”NSA Chief: Cybercrime constitutes the ’greatest transfer of wealth in history’”, Foreign Policy

Rosenberg, Eli (2018), ”Twitter to tell 677,000 users they were had by the Russians. Some signs show the problem continues”, 19 januari, *Washington Post*

Salinas, Sara (2018), ”Six top US intelligence chiefs caution against buying Huawei phones”, 15 februari, *CNBC*

Smith, A. Paul (1989), *On Political War*, National Defense University Press, Washington DC

SSCI (2018), ”Senate Select Committee on Intelligence”, 3 Juli, The Senate Select Committee on Intelligence (SSCI)

Symantec (2018), ”Internet Security Threat Report (ISTR)”, Symantec Corporation

Taylor, Jerome (2010), ”Google chief: my fears for generation Facebook”, 18 augusti, *Independent*

The Economist (2018), ”Insuring intangible risks”, 25-31 augusti

The Economist, Bagehot (2018), ”Some thoughts on the crisis of liberalism – and how to fix it”, 12 juni,

The Economist Intelligence Unit (2018), ”The Economist Intelligence Unit’s Democracy Index”, Intelligence Unit

Thente, Jonas (2018), ”Här är nätpionjärerna som sågar Internet”, 9 oktober, *Dagens Nyheter*

Thomas, Elise (2018), ”As the West warns of Chinese cyber spies, poorer nations welcome gifts with open arms”, 11 juni, *Wired*

Titcomb, James (2016), ”Why has Mark Zuckerberg taped over the webcam and microphone”, 23 juni, *Telegraph*

U.S. Department of Justice (2018), ”Case 1:18-cr-00032-DL”, 16 februari, In The United States District Court For The District Of Columbia

Verizon (2018), *2018 Data Breach Investigations Report*, Verizon

Weise, Elizabeth (2017), ”Russian fake accounts showed posts to 126 million Facebook users”, 1 november, *USA Today*

Wong, Ola (2018), ”Vad är det som händer på Kinas ambassad i Stockholm?”, 17 september, *Svenska Dagbladet*

Wood, Colin (2017), “Cyber security thwarts productivity and innovation, report says”, 27 oktober, *Statescoop*