# Vidare kontext för en CBRN-relaterad hotbild

ANNICA WALEIJ, BIRGITTA LILJEDAHL,
SUSANNE BÖRJEGREN OCH DAVID LINDAHL

FOI-R--4781-SE
ISSN 1650-1942 September 2019

**Annica Waleij, Birgitta Liljedahl, Susanne Börjegren och David Lindahl**

# Vidare kontext för en CBRN-relaterad hotbild

| | |
|---|---|
| Titel | Vidare kontext för en CBRN-relaterad hotbild |
| Title | A wider perspective on CBRN related threats |
| Rapportnr/Report no | FOI-R--4781-SE |
| Månad/Month | September |
| Utgivningsår/Year | 2019 |
| Antal sidor/Pages | 50 |
| ISSN | 1650-1942 |
| Kund/Customer | Försvarsdepartementet |
| Forskningsområde | CBRN-frågor |
| FoT-område | Inget FoT-område |
| Projektnr/Project no | A405119 |
| Godkänd av/Approved by | Åsa Scott |
| Ansvarig avdelning | CBRN-skydd och säkerhet |

Bild/Cover: Hans Lundholm, Halustudio

# Sammanfattning

Denna rapport syftar till att illustrera några trender avseende samhället och säkerhetslägets tänkbara betydelse för CBRN-hotet i ett vidare sammanhang i fredstid, höjd beredskap samt i störd miljö och gråzon. Med begreppet störd miljö avses ett tillstånd eller ett händelseförlopp som kan vara- men inte nödvändigtvis är antagonistiskt orsakat utan även kan vara naturligt åsamkat. Samhällets krisberedskap måste dock kunna hantera båda två och i värsta fall samtidigt. Störd miljö kan i detta sammanhang förstås som ett komplement till gråzon där det finns problem som måste hanteras oaktat orsak.

Samhällets sektorer är starkt beroende av varandra. Bland de utmaningar för samhällsviktig verksamhet som konstaterats de senaste åren är sårbarheten för energibortfall och ett växande beroende av sakernas internet (IoT). Det finns idag ingen sektor i samhället som skulle fungera obehindrat om datorsystemen stängdes ner. Dessa beroenden riskerar att göra Sverige mindre robust, och mer sårbart, för störningar än samhällen med mer manuell hantering och mekanisering.

Återupptagandet av totalförsvarsplaneringen har tillkommit som en följd av en mer instabil omvärld, där gråzonskontext, asymmetriska hot och hybridkrigföring aktualiserats. Aktörerna är terrorism förankrad i och utanför Sverige, militära aktiviteter i närområdet och cyberhot mot kritisk infrastruktur som utgörs av såväl kriminella som statliga aktörer. En större CBR- eller N-händelse bedöms därtill som en av de svårare påfrestningarna ett samhälle kan utsättas för, där allt från skydd till sjukvård, blåljusfunktioner och information till allmänheten behöver fungera samtidigt.

Sammantaget rustar Sverige idag för att möta en allt mer komplex hotbild, där osäkerhet kan råda om vad som egentligen har hänt och vem som ligger bakom en incident. Dagens kanske största utmaning omfattar i detta perspektiv att kunna identifiera svaga signaler/indikatorer. En övergripande utmaning är avsaknaden av en funktion som tar ansvar för helheten. Ofta sker planering för skydd och hotanalyser i etablerade stuprör vilket utgör en risk för att ingen ansvarar för utrymmen mellan stuprören.

I vilken mån olika former av hot, som kan tänkas uppträda simultant i en hybridhotskontext, påverkar varandra behöver undersökas närmare. Aktuella frågeställningar är kaskadeffekter, som t.ex. CBRN-händelser orsakade av cyberangrepp, och hur informations- och påverkanskampanjer har använts, och kan komma att användas, för att förstärka eller till och med konstruera ett CBRN-hot.

Nyckelord: CBRN, totalförsvar, hybridhot, medicinsk hotbild, teknikutveckling, gråzon, samhällsviktig verksamhet, cyber, desinformation, motståndskraft

# Abstract

This report aims to identify some trends regarding the wider context of societal and security challenges, with potential relevance for the identified CBRN threat. National defence as well as civil crisis preparedness capabilities must be able to handle antagonistic incidents as well as naturally caused events, gray zone situations and “disturbed environments”. Worst case, all of the above, simultaneously.

Strong interdependencies between the various sectors of society as well as vulnerabilities exist. Some challenges identified in recent years are vulnerabilities to energy breakdowns and a growing reliance on Internet of Things (IoT). There is presently no sector in society that would function well if the computer systems were shut down more than temporarily. The above mentioned interdependencies increases the risk of making Sweden less robust as a society, and more vulnerable to disruptions than mechanized societies with more manual routines.

The resumed total defence planning has emerged as a result of the increasingly strained security environment, where terms such as gray zone, asymmetric threats and hybrid warfare are used more frequently. Domestic grown, as well as foreign terrorism, increased military activities near Sweden and cyberattacks on critical infrastructure are increasing. In addition, a major CBR or N event is assessed to be one of the most pressing challenge to modern society, where e.g. physical protection, medical countermeasures, crises management and risk communication needs to function seamlessly and simultaneously.

In summary, Sweden is preparing for the possibility of increasingly complex threat scenarios, where disinformation and uncertainty may be additional factors. In this context, the most pressing challenge may be to be able to identify weak signals and create indicators for detecting those. An overarching challenge is the lack of a function that embraces the whole spectrum of possible scenarios as well as the fact that too often, threat analysis and protection planning takes place in stovepipes with little interaction.

The extent to which the different forms of threats, which may occur simultaneously in a hybrid threat context, impact on each other needs to be further investigated. Cascade effects caused by e.g. CBRN events caused by cyberattacks, or how disinformation campaigns have been launched, and may be used, to reinforce or even design a CBRN threat, are areas worth further attention.

Key words: CBRN, total defence, hybrid threats, medical threats, technological development, gray zone, disturbed environment, critical infrastructure, cyber, disinformation, resilience

# Innehåll

# 1. Inledning

Denna rapport är framtagen inom det av Försvarsdepartementet finansierade projektet CBRN-händelser i störd miljö. Projektet, som startades 2018, har som främsta syfte att utveckla kunskap för att systematiskt och kontinuerligt kunna analysera komplexa CBRN-relaterade händelser. Detta inkluderar aktörsdrivna hot i fredstid, under höjd beredskap samt i störd miljö och gråzon, med en ansats till ett helhetsperspektiv.

Det övergripande projektmålet är att erbjuda projektets mottagare ett kunskapsövertag genom att presentera ett underlag för att underlätta framtagande av en sammanlagd hotbild mot människors liv och hälsa samt samhällets funktionalitet, i ett totalförsvarsperspektiv. Genom att inkludera flera relevanta hotaspekter än enbart hotet från farliga ämnen tas även hänsyn till kaskadeffekter och beroenden. En viktig uppgift är att genom kontinuerlig omvärldsanalys studera och beskriva händelser samt trender av relevans. Genom att regelbundet sammanställa händelser, företeelser och trender på årsbasis kan så småningom avvikelser och mer svåridentifierade trender över tid identifieras med större precision. Detta förutsätter såväl samverkan med andra hotbedömande projekt inom FOI som samverkan med Försvarsmakten (FM), andra myndigheter/organisationer, såväl nationellt som internationellt.

Robust energiförsörjning är ett av sju utpekade prioriterade områden av MSB i den Nationella Risk- och Förmågebedömningen, NRFB 2017 [MSB 2017]. Tillika är det en sektor som ingår i de flesta kritiska beroenden som finns i samhället [MSB 2009]. Störningar i energiförsörjning kan vidare ha direkt och indirekt påverkan på civilbefolkningens hälsa. I projektet har under 2018 en särskild fördjupning avseende konsekvenser av energibortfall gjorts [Waleij m.fl. 2019] och en workshop på temat CBRN-händelse under elavbrott genomfördes för ca 200 deltagare under CBRNE- dagarna i Umeå hösten 2018.[1]

## 1.1 Syfte

Denna rapport syftar till att lyfta några trender i samhället och säkerhetsläget av tänkbar betydelse för CBRN-relaterade hotbilder i störd miljö[2] och gråzonskontext. Utgående från dessa trender har också frågeställningar som kan utgöra utgångspunkter för fortsatta studier identifierats. Under treårsperioden är ansatsen att bättre kunna utkristallisera olika kontextuella faktorers påverkan på det relevanta CBRN-hotet i en störd miljö.

[1] CBRNE-dagar i Umeå, https://www.msb.se/sv/Start1/Kalender/CBRNE-dagar-i-Umea/

[2] Begreppet ”störd miljö” saknar i nuläget definition. Författarnas definition ges på sidan 21

## 1.2 Avgränsning

I rapporten har följande avgränsningar gjorts;

- Författarna har summerat existerande hotbilder avseende CBRN men inte tecknat någon egen.[3]
- Avseende övriga trender har främst de av potentiell betydelse för planering för, och hantering av, hälsoaspekter vid CBRN-händelser beaktats.
- Kontexten är begränsad till störd miljö och gråzon.
- De händelser författarna exemplifierat trenderna med är tidsmässigt begränsande till 2017-2018
- Avseende trender av betydelse för teknikutveckling ges exempel, och inte en komplett beskrivning.

## 1.3 Metod och metodiskt utförande

Rapporten baseras på litteraturstudier av öppna källor (forskning, rapporter, instruktioner, doktriner, blogginlägg etc.). Samtal inom FOI har även förts för att konsultera experter inom CBRN, cyber, teknologisk utveckling, säkerhetspolitik, katastrofmedicin samt regionspecifik expertis. Rapporten har därmed producerats med en tvärvetenskaplig ansats. Vidare har intervjuer med experter på andra myndigheter och organisationer gjorts.

## 1.4 Läshänvisning

Rapporten inleds med en beskrivning av trender av betydelse för den generella hotbilden inkluderande CBRN-hotet, IT- och cybersårbarheter samt teknikutveckling (kapitel 2). I kapitel 3 beskrivs hur de sammanhang som de som behöver hantera en CBRN-händelse kan se ut och ett urval av de utmaningar för samhällsviktig verksamhet som identifierats. De omvärldsfaktorer som beskrivs är sådana som antas kan påverka eller utlösa en CBRN-händelse.

I kaptiel 3 berörs även aspekter av kritisk infrastruktur, inbördes beroenden och kaskadeffekter såväl som nationell resiliens i förhållanden till Natos sju civila förmågor. Slutligen diskuteras i kapitel 4 hur en störd miljö inverkar på den beskrivna CBRN-hotbilden. I bilaga 1 presenteras en ordlista med begrepp.

[3] CBRN-hotbilden avseende statliga respektive icke-statliga aktörer studeras i anslagsprojekten BC-hot respektive Icke-statliga aktörer.

# 2. Trender av betydelse för hotbilden

## 2.1 CBRN-hotbild

Hotbilder avseende CBRN produceras regelbundet inom ramen för FOI´s anslag från försvarsdepartementet (se ruta på sida 10). Under 2017-2018 har även aktörer från Säkerhetspolisen (SÄPO), FM, Polisen (NOA Und), Myndigheten för samhällsskydd och beredskap (MSB) och FOI inom det av krisberedskapsanslaget 2:4-finansierade projektet FACIT (Framtida hotbild avseende antagonistiska CBRN-hot samt dess implikationer för uppbyggandet av totalförsvar, Börjegren m.fl. 2019) gjort en ansats att bedöma det antagonistiska CBRN-hotet i ett framåtblickande perspektiv.

FACIT-studien konstaterar att sannolikheten att Sverige kommer att beröras av antagonistiska CBRN-händelser, i form av attacker eller subversiv verksamhet från statliga eller icke-statliga aktörer, har ökat. Detta till stor del på grund av att normen mot användning av kemiska vapen har urholkats under de senaste åren, vilket riskerar att i framtiden även omfatta antagonistisk användning av biologiska och radioaktiva ämnen.

Det är fört i bevis att den Syriska regimen vid ett flertal tillfällen har använt kemiska vapen i konflikten i Syrien [OPCW 2017]. I kombination med det politiska mordförsök som genomfördes i Salisbury, Storbritannien [UK Government 2018] visar det på att det finns stater som inte respekterar kemvapenkonventionen. Ett ytterligare exempel där nervgaser använts är mordet på halvbrodern till Nordkoreas ledare Kim Jong-un 2017 [Ohlsson 2017].

Det faktum att kärnvapen återigen betraktas som ett reellt hot påverkar också bedömningen. Konsekvensen av denna bedömning är att kunskapen om vilka antagonistiska CBRN-händelser som kan påverka oss, och rekommendationer för hur våra samhällsviktiga sektorer kan skyddas bör tas fram under de närmaste åren.

Terrororganisationer som visat intresse för och som lyckats bygga upp en förmåga att kunna sprida högtoxiska kemiska ämnen de senaste 25 åren och som även uttalat hot mot västländer har varit, al-Qaida i Irak samt Daesh (den s.k. Islamska Staten i Syrien och Irak) och tidigare sekten Aum Shinkrikyo i Japan (numera Aleph). Kemiska ämnen som varit aktuella har varit egen tillverkning av kemiska stridsmedel (senapsgas och nervgaser) och användning av växttoxiner, olika industrikemikalier samt bekämpningsmedel [Melin 2000, Normark m.fl. 2017].

Den militära förmåga Daesh byggde upp avseende kemiska vapen bedöms dock vara nedmonterad, men hot om användning av kemiska eller biologiska ämnen i

kampen mot väst är fortfarande kontinuerligt en del av dess retorik [Normark m.fl. 2019]. Det finns farhågor, framför allt i Storbritannien men även på andra håll i Europa och i USA att attacken i Salisbury kan inspirera ickestatliga aktörer, framför allt Daesh sympatisörer, att tillgripa liknande metoder. Enligt en brittisk nyhetsartikel från december 2018 bedömde landets Joint Terrorism Analysis Centre (JTAC) att sannolikheten för en kemisk attack i Storbritannien utförda av jihadistiska aktörer hade ökat efter händelsen i Salisbury, med störst farhågor för en klorgasincident utförd av Daesh. Som stöd för detta påstående angavs uppfångad dialog mellan seniora individer inom Daesh och den effekt även en mindre kemisk händelse kan ha [Nicol M. 2018].

Hot om terrorattentat mot samhällsviktig infrastruktur har uppmärksammats allt mer de senaste åren, vilket även skulle kunna drabba anläggningar som hanterar farliga ämnen [Roffey m.fl. 2019]. Mellan 2002-2017 var terrorattentat och attentatsförsök riktade mot infrastruktur generellt den mest vanliga form av terrorattentat i USA. Denna typ av terrorattentat var vanligare i Nordamerika och Europa än i resten av världen [Global Terrorism Index 2018].

En undersökning som Public Health England (PHE) genomfört av kemiska incidenter i England och Wales mellan 2011 och 2015 visade att ca 5 % av händelserna var avsiktliga [CHPR, 2016]. En sammanställning som gjorts utifrån den franska databasen ARIA (Analysis, Research and Information on Accidents) konstaterades att cirka 1 procent av de incidenter som rapporterades inom kemisk industri orsakats av antagonistiska handlingar [IMPEL 2017].

Det är möjligt att denna andel är underskattad: kring 30 % till 40 % av olyckor och incidenter som registreras i databaser av den typen har inte en tydligt identifierad orsak, och vissa av dessa kan därför faktiskt tänkas vara kopplade till säkerhetsfrågor [Roffey m.fl. 2019, Deleuze m.fl. 2008].

**Exempel på öppna CBRN-relaterade hotbilder samt hotbeskrivningar med CBRN-inslag.**

*CBRN-hotbilder*

Normark M., Lindblad A., Tunemalm A-K., Wiktelius, D., Wikström P. Holmgren Rondahl S., (2019) CBRN-hot från ickestatliga aktörer – Årsrapport 2018 FOI-R--4766--SE

Börjegren S., Liljedahl B., Larsson A., Normark M., Tunemalm A-K., Waldenvik M., Waleij A. och Wikström P. (2019) Totalförsvarsplanering med fokus på CBRN. Framtida antagonistiska CBRN-hot. FOI-R--4765--SE

Börjegren S., Liljedahl B., Larsson A., Normark M., Tunemalm A-K, Waleij A. och Wikström P. (2019) Metod för totalförsvarsplanering avseende CBRN skyddsförmåga FOI-R--4754--SE

*Ej specifikt CBRN*

Liljedahl, B., Waleij, A., Borg, S., Engelkes, T. *Redaktörer* (2017) Komplex antagonistisk attack i gråzon med elavbrott: Insats- och hälsoaspekter. Aktörsövergripande table-top scenario-övning 23-24 november 2017. FOI Memo 6263

Normark M., Knutson, R., Keremidis, H. Antagonistic threats against the food supply and the agricultural sector. FOI Memo 6510

Tunemalm, A-K., Lindahl, D., Liljedahl, B., Normark, M. (2019) Antagonistiska hot och kemiindustrin-. FOI-R--4785--SE

Roffey, R, Tunemalm, A-K., Waleij, A. (2019) Säkerhet för att motverka antagonistiska hot riktade mot kemisk industri: Internationell översikt. *Under tryck*.

Andersson, M., Ahlberg, S., Björklund, S., Karlsson, M., Carlberg, T., Berglund, R., Waleij, A., Tjärnhage, T., Hagström, M., Mårtensson, T. (2018) Stöd till skyddskoncept mot UAS –Slutrapport FOI-R--4668—SE

Waleij, A., Brännström, N., Liljedahl, L., Tjäder, Z., Tjärnhage, T., Wikström, P. (2016) Evolving technologies- Challenges and opportunities from an operational health perspective, FOI-R-4256-SE

## 2.2 IT- och cybersårbarhet

Dagens samhälle är i högsta grad beroende av informationsteknologi (IT) och den så kallade cyberdomänen. Samtidigt utgör cyberdomänen med sin snabba tillväxt, en ny del i vapendomänerna (se figur 3 sida 36). Cyberdomänen, ibland använt synonymt med cyberrymden [Karlzén mflr 2018], är den del av informationsmiljön som består av sammanlänkade och av varandra beroende IT-infrastrukturer med tillhörande data och information. Den inkluderar internet, intranät, telekommunikationssystem, datorsystem samt inbyggda processorer och styrenheter.

I den svenska militärdoktrinen nämns inte cyberdomän explicit, men om cyberrymden sägs följande; ”Gränsen mellan ekonomiska, kriminella, militära och politiska aktörer flyter ihop [...] Cyberrymden innebär strategiskt ett globalt gränslöst utrymme för att på distans genomföra attacker, underrättelsetjänst, påverkan, opinionsbildning och propaganda. Försvarsmaktens resurser ska stödja defensiva och offensiva operationer i syfte att stärka skyddet av Sverige i cyberrymden” [Försvarsmakten, 2016].

Cyberhot och attacker från antagonistiska aktörer mot Sverige ökar [FRA, 2019], och det amerikanska försvarsdepartementet varnar i en rapport [Oodaloop 2019] för ökad cyberförmåga hos aktörer vilka bedöms kunna ligga steget före militären. I samma rapport bedöms amerikanska militären vara dåligt rustad för att bemöta automatiserade cyberangrepp men även att hantera konsekvenserna av framtida angrepp. Särskilt allvarligt ansågs det ökande inflytandet på cybersäkerhet från artificiell intelligens-användning (både för försvar och angrepp) och automatiserade system, i synnerhet där risk för kaskadeffekter uppstår och där beroenden mellan kritisk infrastruktur och sakernas internet (eng. Internet of Things IoT)[4] föreligger.

Förmågeskillnaden inom cyberdomänen mellan kriminella, terrorgrupper och statsunderstödda individer kan förväntas vara stor. Även om terrorgrupper som Daesh och al-Qaida har avsikter att genomföra, och även uppmanar anhängare till cyberattacker, står deras intention sannolikt inte alltid i proportion till reell förmåga att kunna genomföra mer avancerade cyberattentat, mot ex kritisk infrastruktur än deras tidigare genomförda och/eller påstått genomförda datorintrång (hackning) av media och hemsidor. Som exempel på oklarhet kring faktisk aktör, kan nämnas den av Daesh påstådda hackningen av Tv5Monde, vilken enligt Frankrike inte utfördes av Daesh, utan av en statlig aktör som skulle ha gjort det som ett test [Pahi & Skopik 2019]. Samtidigt ses exempel på

[4] Sakernas internet (från engelskans Internet of Things) är vardagsföremål som hushållsapparater, fordon och andra föremål som med inbyggd elektronik och internetuppkoppling kan styras eller utbyta data över nätet.

hur kompetensöverföring sker mellan kriminella, statsunderstödda hackergrupper och terrorgrupper, där tjänster och förmågor köps och säljs mellan olika aktörer.

Cyberattacker på kritisk infrastruktur som kärnkraftverk, petroleumindustri, sjukhus, och finansiella system ökar. Även informationskanaler och då särskilt plattformar för sociala medier liksom TV drabbas. Det finns i dag statliga enheter både för anfall, (TAO, USA), och försvar (CERT-EU, EU). Många länder har skapat regelrätta militära förband, i vissa fall i en egen vapengren (Cyber Command, USA). Hos kriminella finns expertis, t ex ryska Fancy Bear och terrorgruppen Daesh har sitt IS Cyber commando. Det finns en väl utvecklad cybervapenindustri som säljer information om sårbarheter som kan utnyttjas eller färdigutvecklade datorprogram för angrepp. Ett exempel på en tidig framgångsrik cyberattack är Stuxnet 2011, riktad mot Irans nukleära program [Hållén 2011]. De senaste åren har framgångsrika cyberattacker eskalerat med exempel som;

- WannaCry (maj 2017) med hundratusentals utslagna datorer i över 150 länder [Wiklund 2017]. Attacken drabbade även företag i Sverige och det brittiska sjukvårdsystemet med inställda operationer. Attacken var troligen statsunderstödd.
- Den globala cyberattacken Petya/Notpetya mot bl.a Ukrainas energisystem och flera internationella storbolag 2017, däribland den danska olje- och rederijätten Maersk. Maersk förlorade ca 2 miljarder kronor som följd och attacken fick även kaskadeffekter för exempelvis Göteborgs hamn [Greenberg 2018, Campanello, 2017].
- Ytterligare ett exempel från 2017 är en attack mot ett petrokemiskt företag i Saudiarabien med en dittills ny målsättning för cyberangrepp [Perlroth & Krauss 2018]. Motivet verkade inte enbart vara att komma åt data i systemet eller att stänga ner produktionen utan syftet har bedömts av utredarna att vara att sabotera företagets verksamhet samt att orsaka en explosion. Hårdvara motsvarande den som användes på denna anläggning används även vid andra industrier [Synek 2018, Perlroth & Krauss 2018]. Analyser som utförts av säkerhetsföretag om denna attack pekar på statlig inblandning, där både Iran och senare Ryssland pekats ut [Sanger 2018].
- Enligt den ukrainska säkerhetstjänsten stoppades en cyberattack mot fabrik som tillverkar klor för dricksvattenrening, i Aulska, Dnipropetrovsk-regionen i centrala Ukraina. Ryssland antogs ligga bakom attacken [Security Service of Ukraine 2018].

- I oktober 2018 anklagades Ryssland av Nederländska myndigheter för cyberattacker mot OPCWs högkvarter i Haag.[5] Cyberattackerna skedde under våren 2018 och tros ha koppling till händelsen i Salisbury. Minst en av hackarna hade även försökt påverka den nederländska haveriutredningen kring det nedskjutna planet MH17 över Ukraina 2014.

En stor grupp förövare som generellt ligger bakom cyberattacker är kriminella aktörer som har ekonomisk vinning som syfte. Dessa kan till exempel infektera datornätverk med olika typer av program[6] som krypterar databaser och hårddiskar i syfte att få offret att betala lösensummor för att få tillgång till en kryptonyckel. Andra fall som skett i Sverige involverar att skicka e-post med skadlig kod för att kunna få in fjärrstyrningsprogram på offrens datorer och använda dessa för att göra inköp av olika slag och få dem levererade till andra adresser [Johansson 2017].

Det går inte att utesluta att denna typ av angripare även skulle kunna vara intresserade av att använda metoden mot kemisk industri och distributörer. Andra potentiella aktörer är terrorister och ”hacktivister”. De senare är kriminella eller agenter för stater som är politiskt motiverade och använder IT-brott som ett sätt att främja ett politiskt mål.

## 2.3 Teknikutveckling med implikationer för potentiella hot

Teknikutveckling som potentiellt hot, men även de möjligheter tekniksprång utgör för den egna militära och/eller civila insatsförmågan analyseras löpande och för olika syften av många aktörer som bl.a. NATO (2017), MSB/Kairos Future 2016, US Government Accountability Office (GAO 2018), Beverer & Martini m.fl. 2018, Försvarsmakten (2019) och FOI (Kindvall & Wiss 2017, tabell 1).

[5] Organisationen för förbud mot kemiska vapen

[6] Så kallad Ransomware.

**Tabell 1.** Översikt av några aktörers analyser av teknikutvecklingen och vilka aspekter som berörs av respektive aktör.

| | **NATO STO 2017** | **MSB/ Karios Future 2016** | **GAO 2018** | **Beyerer & Martini 2018** | **Försvarsmakten 2019/ Kindvall & Wiss 2017** |
|---|---|---|---|---|---|
| AI | √ | √ | √ | √ | √ |
| IoT/ everywhere computing | √ | | √ | | √ |
| Biotechnology | | | √ | | |
| AM | √ | √ | (√) | | √ |
| UAS | √ | √ | √ | | √ |
| Quantum technologies | | | √ | √ | √ |
| Human Performance Enhancement/ Soldier systems | √ | | | √ | √ |
| Nya material | √ | √ | | | |
| Sociala medier | √ | √ | | | |

I tabellen framgår att många aktörer identifierar en liknande hotbild avseende teknikutvecklingen, även om prioriteringen varierar (se tabell 2). Artificiell intelligens är det hot som identifieras av alla, medan endast en aktör identifierar utvecklingen inom bioteknologi. Som nämnts ovan varierar dock syftena med analyserna från att vara nyttiga för uppbyggnad av militär förmåga, blåsljusförmåga eller mer generellt för samhället i stort.

**Tabell 2.** Översikt över de olika bevakade teknikområdena.

| | |
|---|---|
| Nato STO 2017 | 1) Additive Manufacturing, 2) Everywhere Computing, 3) Predictive Analytics 4) Social Media, 5) Unmanned Air Vehicles, 6) Advanced Materials, 7) Mixed Reality, 8) Sensors are Everywhere, 9) Artificial Intelligence, 10) Electromagnetic Dominance, 11) Hypersonic Vehicles, 12) Soldier Systems |
| MSB/ Karios Future 2016 | 1) Snabbare och billigare datakraft, 2) Snabbare och billigare datakommunikation 3) Smartphone, 4) Sociala medier, 5) Sensorer, 6) Big data, 7) AI, artificiell Intelligens, 8) VR och "augmented reality", 9) Drönare, självstyrande farkoster, fjärrnärvaro etc., 10) 3D-skrivare, 11) Nya material |
| GAO 2018 | 1) Artificial Intelligence (AI), 2) Quantum Information Science, 3) Internet of Things (IoT), 4) Autonomous and Unmanned Systems, 5) Biotechnology, 6) Other Emerging Technologies incl additive manufacturing (i.e., 3D printing) |
| Beyerer, & Martini 2018 | 1) Artificial Intelligence and Autonomy, 2) Digital Battlefield, 3) Quantum Technologies for Defense Applications, 4) Advanced Radar Technologies, 5) Power Supply and Efficiency, 6) Next-Generation Effectors, 7) Human Performance Enhancement. |
| Försvarsmakten 2019/Kindvall & Wiss 2017 | 1) Additiv tillverkning, 2) Cyber, 3) HPM (High Power Microwave), 4) Hypersoniska system, 5) Informationsteknologi, 6) Obemannat/Autonoma system, 7) Plattformar (mark, sjö, luft), 8) Rymden, 9) Signaturanpassningsteknik (SAT), 10) Soldatsystemet |

GAO:s prioriterade teknikområden som möjliga hot, baserad på bedömningar av bl.a. det amerikanska försvarsdepartementet *(DoD),* Inrikes-säkerhetsdepartementet *(Department of Homeland Security, DHS)* samt Underrättelsetjänst *(Office* of the Director of National Intelligences, ODNI).

- *Artificiell intelligens (AI)* Området kan sägas omfatta de datorsystem som av en mänsklig användare uppfattas som ”intelligent” och användningsområdena är oräkneliga. Även inom försvaret har ett antal användningsområden föreslagits (Gustavi T. m.fl. 2018) som t.ex. utveckling av målklassificering och ledningssystem. Rapporten identifierar också lämplighet och begränsningar i utvecklingen, och lyfter farhågor om t.ex. eventuell möjlighet till övertagande av system från en antagonist. Till fördelarna med AI kan nämnas att den kan ge råd i komplexa situationer, t.ex. händelser med brand involverande

farliga kemikalier. En kombination av AI och genomik[7] för utveckling av individbaserad precisionsmedicin och försvarsmedicinska tillämpningar förutspås även. Till dess nackdelar innefattas att den kan ge fel råd och "spåra ur", vilket innebär problem om man litar för mycket på den.

- *Quantum Information Science* (kvantteknologier) Inom Quantum Information Science (QIS) tillämpas principerna och teknikerna för kvantfysik på verkliga problem inom kommunikation, databehandling och varseblivning (eng. *sensing*). Inom den militära professionen spås såväl stora möjligheter som hot där det amerikanska försvarsdepartementet betraktar fenomenet som ”*a very disruptive technology*”. Exempelvis kan radar som upptäcker smygflygplan, d.v.s. flygfarkoster med stealth-förmåga konstrueras och AI-applikationer avanceras. En kapprustning mellan USA och framförallt Kina befaras [Giles 2019, Cole, 2019].
- *Internet of Things* (IoT d.v.s sakernas internet*)* är ett samlingsnamn för produkter som innehåller elektronik med någon form av uppkoppling mot andra system, vanligtvis internet. Den ökande förekomsten av IoT skapar sårbarhet avseende cyberangrepp och risk för kaskadeffekter på kritisk infrastruktur i samhällen (Eidenskog & Kamrani 2017).
- *Autonomous and Unmanned Systems (*obemannade självkörande farkoster, drönare eller UAS*)* omfattar till exempel ansiktsigenkänning, rörelseigenkänning, röstmanipulation, samt obemannade farkoster på mark, i vatten och i luftrummet. Drönare ingår i de flesta moderna vapenprogram, med dess potential som vapenbärare och vid rekognosering, såväl på högteknologisk nivå som ’low tech warfare’ illustrerat av Daesh nyttjande av lättåtkomliga, billiga drönare i Syrien och Irak (Watson 2017). Civila tillämpningsområden riskerar att driva utvecklingen i en riktning som nyttjas antagonistiskt, till exempel från dess civila kapacitet för utspridning av pesticider inom jordbrukssektorn, till bärare för spridning av tårgas, t.ex. i Gaza (Green 2018).
- *Biomedicinsk teknologi (eng bioengineering)* där stora metodologiska genombrott inträffat där utvecklingen av CRISPR-Cas9[8] stått i fokus. Systemtillämpningar med Crispr-Cas började utvecklas 2013 och de har sedan exploderat i antal tillämpningar som kommer att leda till en ökad förståelse av sjukdomar och ge bättre möjlighet att identifiera nya

[7] Genomik kan beskrivas som studiet av arvsmassa, det vill säga en organisms fulla uppsättning DNA, som inbegriper såväl gener som icke-kodande DNA

[8] CRISPR-Cas9: Clustered regularly interspace short palindronic repeats – CRISPR associated protein 9: Tekniken genomgår en snabb utveckling och det finns numera flera nya varianter av Cas9-proteinet

faktorer och markörer för sjukdomstillstånd. Tekniken möjliggör genetisk modifiering med en större effektivitet och till en väsentligt lägre kostnad än vad som tidigare var möjligt.

Utöver de av GAO studerade områdena av försvarsmedicinsk relevans och/eller relevans för blåljusmyndigheter kan nämnas områden som bl.a. studerats av Försvarsmakten (2019) och MSB/Kairos Future (2016);

- *Additiv tillverkning (additive manufacturing, eller 3D-printing)* är ett samlingsnamn för en rad olika produktionstekniker som skapar tredimensionella ”utskrifter” i t.ex. plast- eller metall. Det finns även mer avancerade skrivare som kan arbeta med andra material, t.ex. organiska skrivare för bl.a. organproduktion. 3D-skrivares förmåga att snabbt och enkelt skapa olika avancerade produkter har också fått många att se dem som ett verktyg för att skapa reservdelar. Bland annat har USA:s militär introducerat 3D-skrivare i Afghanistan samt på hangarfartyg för att förenkla logistiken. Under 2017 använde Siemens en 3D-utskriven reservdel i ett kärnkraftverk i Slovenien.
- *Nya material*, Tillsammans med digitala tekniker erbjuder nya material, t.ex. nanomaterial som grafen, och nanocellulosa helt nya möjligheter. Exempelvis finns textilier som känner av puls och blodtryck och larmar om något blir fel.
- *Den framtida soldaten* med studier om t.ex. *Human enhancement***,** t**.**ex exoskelett. Ett exoskelett är en motordriven ”kostym” som används för att öka människors prestation (styrka och/eller hastighet). Konceptet är välkänt från science fiction och pionjärer har varit den amerikanska militären och robotik-orienterade asiatiska länder. Även rysk militär har visat intresse för tekniken. Militära tillämningar inkluderar att soldater kan bära mer utrustning. Utmaningar med att utveckla effektiva exoskelett inkluderar effekt-viktförhållande, livslängd för batteriet samt den relativt höga kostnaden.
- *Sociala medier;* Användandet av sociala medier har utvecklats explosionsartat. Till dess fördel kan nämnas möjligheten att snabbt hjälpa till att sprida varningar, organisera frivilliga etc. Dock kan falska rykten och desinformation spridas lika snabbt. Så kallade filterbubblor i sociala medier kan också bidra till att snabbt förstärka naturliga åsiktsmotsättningar till affekterade nivåer, med risk för bristande tilltro till exempelvis myndigheters rekommendationer.

Den i detta avsnitt beskrivna teknikutvecklingen kan antas ha betydelse även för CBRN-hotets utveckling men hur och i vilken omfattning behöver studeras närmare.

# 3. Omgivande faktorer

Den förändrade hotbilden och dess komplexa natur, illustreras av bl.a. Natos Strategic Foresight Analysis (Nato 2017a), den nationella säkerhetsstrategin, en återupptagen nationell totalförsvarsplanering, slutredovisningen av Försvarsmaktens perspektivstudie 2016-2018 (Försvarsmakten 2019) och de senaste årsrapporterna från Säpo, Försvarets Radioanstalt (FRA) och den Militära underrättelsetjänsten (MUST) [Försvarsdepartementet 2017, Regeringskansliet 2017, Säpo 2019, FRA 2019, MUST 2019].

De bakomliggande orsakerna till uppfattningen om det mer ansträngda säkerhetsläget och oro för utvecklingen av grundförutsättningarna för samhället är en kombination av såväl antagonistiska som naturliga händelser. Direkta och indirekta effekter från hybridkrigföring och cyberattacker, en snabb teknikutveckling och effekter från klimatförändringar med mera, påverkar såväl kritiska beroenden och kaskadeffekter som nationell motståndskraft (eng. *resiliens*). Ur ett CBRN-perspektiv innebär detta, att allt från hotbedömningar till hantering av CBRN-relaterade händelser behöver ses över i perspektivet av att omgivande faktorer har ändrats.

Detta kapitel lyfter översiktligt några centrala trender och grundläggande begrepp till stöd för en fortsatt diskussion om vad som kan krävas vid planering för och hantering av CBRN-händelser med hänsyn till dagens utveckling.

## 3.1 En ”all hazards” approach till CBRN

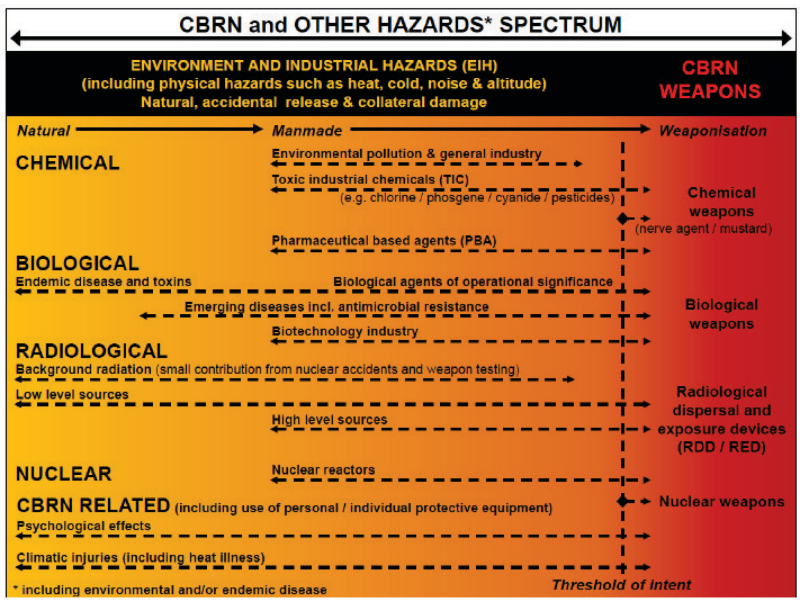
Inom Nato COMEDS[9] har en vidgning av det medicinska utfallsrummet av CBRN-händelser från att tidigare avgränsats till NBC/CBRN-hot kopplade till en resursstark aktör till något som omnämns som ”CBRNE3T all-hazard spectrum” (figur 1). Denna ansats omfattar (som tidigare) kemiska, biologiska, radiologiska och nukleära hot. Dessutom inkluderas hot från explosivämnen samt endemisk sjukdomsbild, miljö- och hälsorelaterade faktorer och trauma.[10] En av de bidragande anledningarna till förändringen kan vara att det uppmärksammats allt mer att vissa icke-antagonistiska CBR-relaterade händelser inte nödvändigtvis leder till lindrigare konsekvenser än de som orsakats av antagonistiska CBRN-hot. Några exempel på naturligt orsakade händelser med svåra konsekvenser är Ebolautbrottet i Västafrika 2014-2016, tsunamin med den efterföljande kärntekniska olyckan i Fukushima, Japan 2011 och tågurspårningen i Graniteville, USA 2005, med omfattande utsläpp av

[9] COMEDS = The Committee of Chiefs of Military Medical Services in NATO

[10] dvs. en livshotande fysisk skada med risk för sekundära komplikationer som chock, andnöd, och död

klorgas som följd. Den potentiella svårigheten att bedöma om till exempel ett sjukdomsutbrott är avsiktligt orsakat motiverar också att inte initialt skilja antagonistisk användning från naturligt orsakade händelser i planering för kris och krig. Ett sjukdomsutbrott kan framstå som naturligt orsakat, men kan vara avsiktligt underblåst av till exempel förstärkning av hygienreducerande faktorer.

CBRNE3T all-hazard-konceptet påminner i stort om det som under mitten av 2000-talet lanserades som EIH (Environment and Industrial Hazards) eller EIHH (Environment and Industrial Heath Hazards) inom det Euro-Atlantiska Partnerskapet och som alltså förefaller ha fått en renässans (Nato-EAPC 2005). Det förändrade omvärldsläget inklusive gränsförskjutningen av respekten för folkrätten och krigets lagar de senaste åren, har bland annat inneburit frekventa attacker mot civila mål. Statliga aktörer i bl.a. Jemen och Syrien attackerar sjukhus, energiförsörjning och annan kritisk infrastruktur och brända jordens taktik mot jordbruk och industriverksamhet har använts av Daesh i Irak och Syrien. Daesh anlagda svavelbrand i Iraq hösten 2016 orsakade hälsovådliga utsläpp av gränsöverskridande proportioner [Björnham et al 2017]. Det pågående kolerautbrottet i Jemen har förorsakats av den medvetet sönderslagna infrastrukturen för vatten- och avloppsrening. Utbrottet, tillika världens mest omfattande, diskuteras även i termer av att kunna klassas som en form av biologisk krigföring [Allana 2017].




**Figur 1.** En "all hazards approach" till CBRN-hotet, där den högra sidan av spektrat innefattar massförstörelsevapen och den vänstra naturligt förekommande CBR-relaterade hot och faror. Notera, att även om vissa faror ligger i den icke-offensiva vänstra delen av spektrat, betyder det inte att de nödvändigtvis leder till lindrigare konsekvenser [Nato 2018a].

## 3.2 Störd miljö-det nya normala?

Samhällets krisberedskap syftar till att förebygga, motstå och hantera krissituationer, oberoende av krisens orsaker.[11] Kriser kan vara orsakade av människan; antagonistiskt eller genom olyckor (den mänskliga faktorn). Andra kriser som kan vara naturligt orsakade, i meningen att de inte *direkt* förorsakas av mänsklig aktivitet, kan också skapa svåra påfrestningar för samhället såsom extrema väderhändelser.

Med begreppet störd miljö avses ett tillstånd eller ett händelseförlopp som kan vara naturligt åsamkat, exempelvis ett bortfall av, eller en svår störning i en eller flera samhällsviktiga verksamheter på kort tid kan leda till att en allvarlig kris inträffar i samhället. Detta tillstånd kan vara- men är inte nödvändigtvis antagonistiskt orsakat. Samhällets krisberedskap måste dock kunna hantera både och, i värsta fall samtidigt. Störd miljö kan i detta sammanhang förstås som ett komplement till gråzon där det finns ett problem som måste hanteras oaktat orsak.

En störd miljö kan också innefatta att en förmåga krävs för att lösa en kris samtidigt som de förväntade resurserna från ett ”normaltillstånd” inte finns tillgängliga. Detta innebär att det även behövs beredskap för att ta hand om en kris där förutsättningarna ändras t.ex. genom kommunikationsbortfall, eller att den egna utrustningen slutar fungera. Normalt arbetar räddnings- och incidentpersonal oftast utifrån förutsättningen att någon annan är drabbad och uppdraget är att rädda dessa individer. Extra utmaningar kan exempelvis vara beredskap för hämtning från barnomsorg vilket uppstår om de själva är drabbade, eller om gifta par samtidigt behöver tjänstgöra eller är krigsplacerade.

Några exempel på senare tids kriser med naturlig orsak;

- Orkanen Harvey som drabbade delar av USA sommaren 2017 visade på hur *kaskadeffekter* kan påverka ett samhälle med starkt beroende av kritisk infrastruktur. Orkanen orsakade bland annat en översvämning och påföljande brand i en kemisk anläggning i Houston, Texas. Anläggningen hanterade stora kvantiteter väteperoxid som är instabilt och måste förvaras kyld. I samband med stormen slogs såväl elen som reservkraften ut varvid temperaturen steg och kemikalierna självantände. Över hälften av USAs produktion av etylen, poly-propylen och poly-etylen stoppades under en period. Ca 200 personer som bodde nära det drabbade området evakuerades och fick återvända först efter en vecka [CSB 2018].

[11] En kris avser en händelse som drabbar många människor och stora delar av samhället. Den kan komma plötsligt (eng. *sudden onset*) eller smygande (eng. *protracted*).

- I september 2017 drog orkanen Maria in över flera karibiska öar inklusive det amerikanska territoriet Puerto Rico. Orkanen slog ut öns eldistribution och lämnade uppskattningsvis halva ön utan rent vatten. Bristen på el lamslog bl.a. den viktiga läkemedelsindustrin vilket påverkade internationella läkemedelsföretag med produktion i Puerto Rico. Exempelvis hade Baxter tre anläggningar för tillverkning av infusionsvätska på ön. Tio veckor efter orkanen drevs en av dess fabriker fortfarande med reservkraft medan de andra två försörjdes intermittent via elnätet. Detta fick som följd att även sjukhus på fastlandet drabbades av brist på infusionsvätska [Sanborn 2018].
- Sommaren 2018 utbröt ett 50-tal skogsbränder i Sverige som visade sig svåra att bekämpa. Bränderna inträffade efter en period av långvarig torka och ihållande höga temperaturer och föranledde EUs största krishanteringsinsats enligt civilskyddsmekanismen[12] det senaste decenniet. Torka och vattenbrist drabbade många jordbrukare hårt även i delar av landet som skonades från bränder. Julimånaden 2018 var på större delen av Götaland och Svealand den varmaste som någonsin uppmätts. Enligt Folkhälsomyndigheten hade en fjärdedel av Sveriges befolkning hälsobesvär på grund av värmen. Andelen EHEC- och vibrio-infektioner ökade under sommaren liksom dödligheten av värmerelaterade orsaker [Folkhälsomyndigheten 2018].

## 3.3 Utmaningar för samhällsviktig verksamhet

I följande avsnitt diskuteras ett urval av de utmaningar för samhällsviktig verksamhet som identifierats indelat i de sju prioriterade områdena i den nationella risk- och förmågebedömningen [MSB 2017]. Under respektive rubrik ges några exempel på händelser 2017-2018 som är kopplade till respektive område.

### 3.3.1 Energiförsörjning

Det moderna samhället, inklusive dess krisberedskapsförmågor, är helt elberoende. För privatpersoner har elen skapat livsmönster som det är svårt att frigöra sig från. Genom automatisering och datorisering påverkar redan korta elavbrott samhällsfunktioner och människors vardag, såväl på arbetsplatser som

[12] EU:s civilskyddsmekanism är en överenskommelse mellan EUs medlemsstater om att hjälpas åt vid större kriser och katastrofer inom och utom Europas gränser. Arbetet organiseras av EU-kommissionen genom Centrum för samordning av katastrofberedskap, (ERCC - Emergency Response Coordination Centre). Sverige har både givit och tagit emot stöd inom ramen för överenskommelsen.

i bostaden. Under den senaste tjugoårsperioden har det inträffat flera större energibortfall, nationellt och internationellt, som visat hur känsliga många verksamheter och samhällsekonomiskt vitala delar är.

Energibortfall orsakas bl.a. av extrema väderhändelser eller mänskligt utlösta händelser såsom driftfel eller sabotage, inklusive cyberattacker. Korta avbrott leder med vissa undantag till begränsade problem men samhällskostnaderna kan bli väldigt stora även för dessa. Störningar i energiförsörjningen kan även ha direkt och indirekt påverkan på civilbefolkningens hälsa [Jonsson 2018b, Waleij mfl. 2019].

Redan efter en timmes elavbrott kan vattentrycket i dricksvattenledningar drastiskt minska och det blir problem med att spola vattentoaletter. Reservkraften tar snabbt slut eftersom mobiltrafiken ökar då det är det enda sättet att kommunicera digitalt med familj och vänner. Enligt Post- och telestyrelsens nya regler, som börjar gälla 2020, har telekombolagen skyldighet att se till att det finns reservkraft till mobilmasterna i tätorter med fler än 8000 invånare, men endast i en timme [SVT 2019]. Hemsjukvård med elberoende utrustning och hemtjänst är extra känsliga för elavbrott. Långa avbrott har visat sig kunna orsaka stor psykisk påfrestning och inverkan på psykisk hälsa [Waleij mfl. 2019].

Svenska kraftnät har varnat för att växande städer, elektrifiering i samhället och nya industrier har gjort att delar av Sverige riskerar elbrist. Situationen är mest ansträngd i Mälardalen och Malmöregionen. Därför har myndigheten sagt nej till att öka nätkapaciteten på flera håll i landet. Egentligen råder det ingen brist på el, men mycket av elen produceras i landets norra delar och används i söder, och måste kunna ledas däremellan. När fler vill använda större mängder el samtidigt så behövs det en högre effekt i ledningarna för att få fram all el som efterfrågas. I dagsläget finns brister, både i överföringen mellan norr och söder och inom regionerna [SVT 2019].

Det svenska elnätet har konstaterats vara sårbart för såväl fysiska attacker som potentiella cyber- och insiderattacker. Nedan följer några exempel på relevanta incidenter kopplat till hot om, eller reella elbortfall. Serien ”Nedsläckt land” på SVT Play som släpptes våren 2019 är ett experiment där tio deltagare ska klara av att leva utan el under en längre tid, efter att en solstorm orsakat strömavbrott i hela Sverige. En grupp hamnar i ett modernt hus och en grupp på en äldre gård. Redan första kvällen ändras förutsättningarna dramatiskt när det blir strömavbrott. Ett scenario likt detta har hänt på riktigt då en solstorm i oktober 2003 slog ut elnätet i Malmö under en timmes tid.

- Sedan cyberattackerna mot Ukrainas elnät har det varnats för att utländska IT-spioner har gjort förberedelser för att slå ut svensk infrastruktur som elnät och kommunikationssystem [SVT 2017].

- I januari 2019 skedde ett sprängattentat mot Ellevios ställverk i Spånga. Polisen rubricerar händelsen som allmänfarlig ödeläggelse [SVT 2019b].
- Svenska Kraftnät medger säkerhetsbrister i och med att myndigheten anlitade utländska it-tekniker vilka fick tillgång till system som styr drift och övervakning av stamnätet, utan att det skett säkerhetsprövning enligt svensk lag [SR 2019].

### 3.3.2 Livsmedel & läkemedel

Livsmedelssystemet har de senaste decennierna genomgått ett antal förändringar och blivit alltmer komplext. Verksamhet som tidigare varit offentlig drivs nu många gånger i privat regi, ibland av internationella aktörer. Antalet livsmedelsbutiker har minskat och för konsumenten har avstånden till livsmedelsbutikerna ökat. Butikerna har dessutom allt mindre i lager och leveranser ska ske enligt ”just in time”-principen [Molin & Östensson 2015].

Den ökade internationaliseringen av livsmedelsproduktionen, där ungefär hälften av alla livsmedel har sitt ursprung i utlandet är en påtaglig samhällsförändring.

I dagsläget importerar Sverige ungefär hälften av all mat som konsumeras i landet. För vissa produkter som kaffe, te och ris är vi helt importberoende. För en stor del av frukt och grönt samt ca 50 % av allt kött är situationen densamma. Å andra sidan är andelen importerade mejeriprodukter och spannmål är liten [Brännström mfl. 2017]. Jordbruket brottas dock generellt med lönsamhets-problem.

Livsmedelssystemet är som de flesta sektorer starkt beroende av bland annat el, transporter, elektroniska kommunikationer och it-teknik vilket innebär att störningar i livsmedelsförsörjningskedjan kan uppkomma som en följd av många olika typer av händelser.

År 2017 antog Riksdagen en nationell livsmedelsstrategi som omfattar hela livsmedelskedjan med sikte mot år 2030. Bland annat beskriver regeringen en ambition att vända trenden med minskad nationell livsmedelsproduktion [Regeringskansliet 2018].

Riksrevisionen konstaterade 2018 i en granskningsrapport att Regeringen och ansvariga myndigheter inte har skapat tillräckliga förutsättningar för en väl fungerande livsmedels- och läkemedelsförsörjning i händelse av kris. Bland annat behövs det tydligare mål och ansvarsfördelning. Tidigare hade Sverige mat och läkemedel i beredskapslager, men dessa är med undantag från läkemedel mot influensa avskaffade. Vid omregleringen av apoteksmarknaden för snart tio år sedan avvecklades även det ansvar som Apoteket AB hade för

läkemedelsförsörjning i kristid, och några kompenserande åtgärder har inte vidtagits. Livsmedelsverket och Socialstyrelsen har visserligen vidtagit en rad kunskapshöjande åtgärder på området, men staten har enligt Riksrevisionens bedömning inte den information som behövs för att utveckla handlingsplaner och förberedelser för livsmedels- och läkemedelsförsörjning i kris och under höjd beredskap. [Riksrevisionen 2018]

I det som många bedömer som en osannolik, men inte helt otänkbar situation, där Sverige blir militärt angripet med taktiska kärnvapen skulle påfrestningarna på samtliga delar av samhället bli stora. Ett sådant angrepp skulle, utöver den direkta förstörelsen och förmodat stora skadeutfallet, också få stora konsekvenser för svensk livsmedelsförsörjning. Sverige har förlorat delar av sin förmåga att hantera kriser där radioaktivt nedfall är en faktor [Brännström m.fl. 2017].

- Ett till synes trivialt problem fick under sommaren 2018 stor uppmärksamhet i svenska medier; ”O'boy brist”. På grund av en maskinell uppdatering i tillverkningsfabriken som förser livsmedelsbutiker med O'boy uppstod en situation med tomma butikshyllor och frustrerade reaktioner på sociala medier [Nyheter 24 2018].
- Sommaren 2018 nödslaktades över 110 000 grisar i Rumänien efter ett utbrott av afrikansk svinpest.[13] Enligt en rapport från EU-kommissionen upptäcktes smittan i Rumänien för första gången sommaren 2017, i en del av landet som gränsar till Ungern och Ukraina. Regeringens teori är att smittan kom till Rumänien med vildsvin. Att få in svinpest i ett svinproducerande land, kan även om orsakerna är naturliga få enorma ekonomiska konsekvenser. Dels måste smittade besättningar slaktas ut, dels följer handelsstopp eftersom hela EU vet att det är en smitta svår att bli av med.

### 3.3.3 Transporter

En fungerande transportsektor är en nödvändig förmåga för att upprätthålla samhällets funktionalitet, vilken bl.a. förutsätter försörjning av livsmedel, läkemedel och drivmedel. Infrastrukturen har dock inte byggts ut i samma takt

[13] Afrikansk svinpest är en smittsam och dödlig virussjukdom som drabbar grisar och vildsvin. Viruset är mycket motståndskraftigt och överlever länge i miljön och även i kött från infekterade djur, inklusive fryst kött. Människan smittas inte, men om matrester som innehåller virus ges till grisar eller hamnar i naturen kan sjukdomen spridas till nya områden. Sedan 2014 förekommer afrikansk svinpest även i EU. Sverige har hittills varit förskonad från sjukdomen, men Europa har under åren haft flera utbrott framför allt på den iberiska halvön och på Sardinien, där smittan kvarstår.

som resandet och transporterna har ökat. Vägar, järnvägar, flygplatser är i många fall utnyttjade till bristningsgränsen, inte minst i våra storstadsregioner. I de glesare delarna av landet har istället efterblivet underhåll lett till dåliga, och ibland även farliga, vägar och järnvägar.

Sverige är i vissa delar starkt import- och exportberoende varför transporter inom landet är essentiellt. Marknaden är idag avreglerad och ingen myndighet har ett samlat ansvar för verksamhetsområdet kopplat till exempelvis höjd beredskap. Behovet av att skydda transporter och centrala lager av exempelvis drivmedel är centralt. I ett internationellt perspektiv är drivmedelsdepåer, raffinaderier och naturgasledningar anläggningar där det uppmanas till angrepp samt att försök till angrepp och framgångriska attentat har genomförts. I synnerhet i konfliktområden utgör sådana installationer av olika anledningar attraktiva måltavlor.

Nationellt har en kartläggning om flöden av transport av farligt gods gjorts, föranlett av ett regeringsuppdrag till dåvarande Räddningsverket [Räddningsverket 2006.] Som en följd av första kartläggningen genomfördes ytterligare en kartläggning kring databehov och datatillgång avseende flöden av farligt gods på väg, järnväg i luften och till sjöss med ovan nämnda rapport som grund [Trafikanalys tillsammans med MSB, Transportstyrelsen, Trafikverket och Sjöfartsverket 2015]. Den senare studien konstaterade att det möjligtvis skulle gå att identifiera huvudsakliga stråk för godstransporter på väg, med information om start och mål, men med bristande geografisk upplösning. Däremot blir det svårt att veta var godset lastats och lossats vid körningar med flera stopp. Studiens slutsats blev att det i dagsläget inte går att sammanställa statistik om flöden.

- I januari 2019 drabbades delar av Sverige och Finland av ymnigt snöfall vilket orsakade omfattande flygförseningar [Ståhl 2019].
- Några dagar före julhelgen 2018 uppmärksammade säkerhetspersonal på London Gatwick flygplats ett antal drönare som cirkulerade kring en av flygplatsens landningsbanor. De kommande tre dagarna påverkades kring 1000 flygrörelser och ca 140000 resenärer fick se sina flyg i jultrafiken inställda eller omdirigerade. Situationen bedömdes så allvarlig att den Brittiska Försvarsmakten kallades in [Grierson 2019, BBC 2019].
- Under sommaren 2017 framkom att sekretessbelagda uppgifter hade läckt i samband med att Transportstyrelsen anlitat utländska företag att sköta myndighetens IT-drift. Känsliga uppgifter som det svenska körkortsregistret och information om broar, tunnelbana, vägar och hamnar i Sverige gjordes tillgänglig för icke-säkerhetskontrollerad personal i utlandet.

### 3.3.4 Hälso- och sjukvård

Sjukvården är en viktig nationell strategisk resurs. Vid höjd beredskap, allvarliga händelser, eller krig ställs sjukvårdens kapacitet på sin spets, och kapacitetstaket inom vården kan snabbt uppnås. Försvarsmakten och Socialstyrelsen (SoS) inledde under 2015 ett projekt med syfte att identifiera sårbarheter och nödvändiga förändringar för att möta samhällets samlade behov av sjukvård vid stora olyckor, katastrofer och krig [Försvarsmakten & Socialstyrelsen 2017].

Försvarsmakten har till skillnad från många andra militära organisationer ingen egen sjukvårdsförmåga och är beroende av civil sjukvård i händelse av omfattande skadeutfall. Under det kalla kriget vilade den svenska krigssjukvårdsorganisationen på den militära sjukvårdsorganisationen, civilförsvaret och den civila sjukvården. FMs förmåga avseende traumavård har sjunkit och hela landets behov av traumavård i kris och krig vilar idag på den civila sjukvården. Enligt ett examensarbete utfört vid Försvarshögskolan (FHS) är den militära kirurgiska förmågan att omhänderta skadade reducerad till ca 1 % av tidigare kapacitet [Blimark 2014]. Militära - men även civila rörliga förstärkningsresurser är en nationell bristvara.

Parallellt har den civila sjukvården genomgått stora förändringar präglade av ekonomiska sparbeting, New public management samt en medicin-teknisk utveckling med hög grad av specialisering. Det är generellt en låg bemanningsgrad inom hälso- och sjukvården, och många vårdinrättningar har problem med att rekrytera den personal som behövs.

Detta har inneburit en långt driven effektivisering och rationalisering. Den beredskap för stora skadeutfall i händelse av väpnad konflikt, eller potentiella terrordåd som de svenska akutsjukhusen tidigare hade, finns inte längre kvar. Exempelvis kräver en händelse med flera brännskadade att hela Norden blandas in- samtidigt som civila luftburna resurser för medicinsk evakuering är en bristvara. Sjukvårdshuvudmännen uppfattar inte att de har uppgiften att planera för att hantera den storlek av skadeutfall som skulle följa på ett högintensivt väpnat angrepp. Många sjukhus ligger idag nära kapacitetstaket under ordinarie verksamhet och har små möjligheter att med uthållighet hantera en större belastning.

En trend från krigszoner internationellt är också att Genevekonventionens skydd och krigets lagar respekteras allt mindre. Vårdpersonal och vårdinrättningar utgör i vissa fall mål för krigshandlingar. Det kan inte uteslutas att en aggressiv handling på svensk mark inte skulle kunna ta till liknande handlingsmönster. Det finns således utmaningar för Sveriges katastrofmedicinska beredskap. Regeringen tillsatte under 2018 en utredning om stärkt krisberedskap i vården.

Utredningen om Hälso- och sjukvårdens beredskap (S2018:09). Utredningens uppdrag är bl.a. att göra en översyn av hälso- och sjukvårdens beredskap inför och vid allvarliga händelser i fredstid och höjd beredskap samt lämna förslag på hur hälso- och sjukvårdens förmåga att hantera denna typ av händelser långsiktigt bör utvecklas; uppdraget omfattar både krisberedskap i ett generellt perspektiv och katastrofmedicinska aspekter. Utredningen ska senast vara klar i december 2020.

- Det har visat sig att krigsliknande skadepanoraman även fredstid kräver god katastrofmedicinsk förmåga efter exempelvis terrorhandlingar som den på Drottninggatan i april 2017.
- Indien kallas ibland för den fattiga världens apotek, eftersom landet är världsledande på att tillverka kopior av läkemedel till ett lågt pris där patenten gått ut. Beroendet till Kina för ingående komponenter är starkt. Att råvarutillverkningen i huvudsak är koncentrerad till ett mindre antal företag med tillverkning i Asien är en av orsakerna till att läkemedelsförsörjningen globalt är sårbar.

### 3.3.5 Finansiella tjänster

En av de viktigaste sektorerna för samhällets stabilitet – den finansiella sektorn – är helt privatägd så när som på Riksbanken. Inom bankvärlden har man under ett flertal år haft stort fokus på ekonomisk motståndskraft, men inriktar sig nu allt mer mot de tekniska plattformar som man är beroende av. Exempelvis undersöks geografisk separation för att minska risker vid exempelvis omfattande energibortfall eller naturolyckor. Vissa banktjänster har identifierats som särskilt kritiska. Inom såväl bankvärlden som försäkringsbranschen har man börjat värdera cyberhotet som allomfattande. Till skillnad från t.ex. naturolyckor har man dock inte lika många historiska data. Försäkringsbolagen har därför börjat se på hur man kan värdera företags riskexponering och kreditvärdighet utifrån kriterier om hur kunden arbetar med cybersäkerhet [Olsson 2018].

Enligt en rapport av Carnegie Endowment for International Peace, har cyberattacker mot bankväsendet med statsunderstödda kopplingar ökat. Av 94 fall av cyberattacker som rapporterats som finansbrott sedan 2007 misstänktes närmare 25 % (23 st) vara statsunderstödda med kopplingar till länder som Kina, Ryssland, Iran och Nordkorea [Moon 2019].

- Flera cyberattacker mot banker under de senaste åren tros ha koppling till Nordkorea. Under 2018 misstänks hackare understödda av Nordkorea ha infiltrerat Chiles centralbanks bankomatsystem och förskingrat en större summa pengar. Samma år angreps även Indiens Comsos Bank och under 2015 Bangladesh centralbank [Mathews 2019] .

### 3.3.6 Information och kommunikation

Om en aktör skulle ha som mål att destabilisera Sverige i syfte att påverka det politiska landskapet är en enkel metod att med desinformation och destabilisering (subversion, sabotage, terror) skapa grogrund för stor pessimism vilket öppnar vägen för populism. Inbäddat i de populistiska åsikterna finns en åsiktsflora som passar angriparen ypperligt. Det kan handla om att inte gå med i Nato eller delta i andra internationella sammanslutningar eller att övergå från multilaterala till bilaterala säkerhets- och handelsrelationer.

- I januari 2019 rapporterades det att samtliga ryska internetoperatörer i ett planerat test kommer att koppla bort Ryssland från internet, som ett led i landets cyberförsvar. Syftet angavs vara att samla in data och kunskaper om hur landets interna internet, Runet, skull klara sig utan resten av världens nätverk. Testet skulle ske under första kvartalet 2019 under ledning av Roskomnazor, Rysslands motsvarighet till Post- och telestyrelsen, PTS [Dobos, L. 2019].
- USA erkände tidigare i år att det amerikanska cyberkommandot (US Cyber Command) genomfört en offensiv cyberattack mot ”The Internet Research Agency”, bättre känt som Rysslands trollfabrik, i St Petersburg. I preventivt syfte stängde man ned internet-förbindelsen, för att förhindra spridning av falsk information som kunde påverka det amerikanska mellanårsvalet i november 2018. Bara några dagar tidigare hade president Putin varnat för att hela Ryssland skulle kunna stängas ute från det globala internätet. Den globala uppkopplingen har länge porträtterats som en farlig sårbarhet under den eskalerande konflikten mellan Ryssland och väst. Duman tog snabbt fram ett lagförslag ”the sovereign internet bill”, som kräver att telekomleverantörerna noggrant ska övervaka all internet-trafik i Ryssland och skapa möjligheter att stänga av alla förbindelser till omvärlden i händelse av attack. Lagförslaget väntas skrivas under av presidenten i närtid [Roth 2019].
- I februari 2018 lades en video som påstod sig visa en brand och en explosion på en avfallsanläggning i Singapore med utsläpp av farliga ämnen upp på nätet. Videon visade sig emellertid visa en explosion på helt annan anläggning från flera år tillbaka. Anläggningen i Singapore brann inte alls [Yong 2017].
- Under sommaren 2018 sattes ett antal affischer upp på offentliga platser i Riga, där det varnades om en invasion av giftiga spindlar. Varningen delades flitigt via social nätverk, t.ex. Twitter, men enligt den lettiska hälsoinspektionen fanns det ingen substans bakom. Kampanjen blev dock ansträngande för sjukvården med många frågor från oroliga medborgare [The Baltic Course 2018].

- Ryssland har anklagats för att under den Nato-ledda försvarsövningen Trident Juncture i Skandinavien 2018 stört GPS-utrustning som användes under övningen, GPS jamming [O'Dwyer 2018, BBC 2018]. GPS-störning har blivit standard vid alla större militärövningar på Kolahalvön och påverkar bl.a flygbolagen som ska landa i Kirkenes och räddnings- och ambulanstjänster
- Ett exempel på hur känslig information kan spridas oavsiktligt är avslöjandet i början av 2018 att en populär träningsapp, Strava, kunde röja känslig information om amerikanska militärbaser och dess personal i aktiv tjänst på platser som Irak och Syrien. Data om joggingrutter som delas av soldater visade både välkända baser som även okända utposter och hemliga rutter [Toler 2018]. Senare under samma år visade fitness-appen Polar på samma problem [Postma 2018]. Pentagon har som en följd av ovanstående sedan mitten av 2018 förbjudit användandet av utrustning som kan spåras via GPS under tjänstgöring i internationella insatser.
- Vid ett antal tillfällen har det utretts om främmande makt försökt påverka nationella val, exempelvis i USA, Frankrike och Storbritannien. Inför det svenska riksdagsvalet hösten 2018 befarades att påverkan även skulle ske i Sverige. I efterhand kunde det konstateras att även om Säkerhetspolisen (Säpo) kunde notera en ökning i aktiviteter med syfte att påverka valet, så var det inget som stack ut bortom ramen för vad Säpo förutsett [Säpo 2019]. MSB noterade inte heller några större påverkanskampanjer inför valet. Dock förekom det ett antal incidenter av intresse. Exempelvis noterade Socialdemokraterna att partiets hemsida hackats tre gånger på två veckor där IP-adresser kunde spåras till Ryssland och Nordkorea. Moderaterna rapporterade att falska flygblad med koppling till en högerextrem kampanjsajt delats ut till hushåll i partiets namn i Stockholmsområdet samt i andra delar av landet. En artikel i den ryska tidningen Pravda där det diskuterades vilken valutgång som vore bäst ur ett ryskt perspektiv uppmärksammades av MSB [Aftonbladet 2018].

**Krigföring över flera domäner**

Fenomenet att använda telefoner för att positionsbestämma och/eller eldleda har förekommit under en tid, likaså mass-utskick med sms. Det mer innovativa på senare tid förefaller vara koordineringen mellan elektronisk krigföring, psykologiska operationer och kinetiska verkansmedel för att uppnå psykologiska effekter.

Modus operandi kan se ut som följer;

- Soldater får SMS som informerar om att de är omringade och övergivna
- Några få minuter senare, får deras familjer SMS som anger ”Din son har omkommit i strid”
- SMS:en följs av samtal eller ett SMS till soldaterna, följt av fler SMS med information om att för att överleva måste de retirera. Ovan aktiviteter följs av artilleriattacker på den/de platser där en koncentration av mobiltelefonaktivitet kunnat noteras [Dunn 2018, Unian Information Agency 2018].

### 3.3.7 Skydd och säkerhet

I Försvarsberedningens delrapport ”Motståndskraft” framfördes att det fysiska skyddet för civilbefolkningen i första hand ska åstadkommas genom tillgång till skyddande utrymmen såsom skyddsrum. Vidare ansåg beredningen att forskning och omvärldsbevakning av rörande massförstörelsevapen är av stor vikt för att kontinuerligt kunna bedöma behovet av skydd mot dessa inom befolkningsskyddet.

Efter att MSB i en rapport konstaterat att befolkningsskyddet i Sverige, där skyddsrummen ingår, inte är tillräckligt genomfördes under 2018 en skyddsrumsinventering. En databas över var skyddsrummen är fördelade i Sverige och närmaste skyddsrum finns har uppdaterats och finns på MSB:s hemsida.

Att beredskapen hos allmänheten för allvarliga påfrestningar i samhället är för låg har uppmärksammats allt mer. MSB har därför på uppdrag av regeringen tagit fram en ny version av broschyren Om krisen eller kriget kommer (maj 2018) i syfte att öka privatpersoners kunskap om krisberedskap, höjd beredskap och ytterst krig [MSB1186]. Den senast versionen publicerades 1961.

Näringslivets roll i totalförsvaret är under utredning och utredningens resultat ska presenteras december 2019 [Utredningen om totalförsvarets försörjningstrygghet (Fö 2018:01)]. Utredningen ska lämna förslag om hur totalförsvarsviktiga företag vid höjd beredskap och ytterst i krig ska kunna leverera varor och tjänster enligt olika avtalsformer med staten och andra offentliga aktörer. Här kan det bl.a. handla om att återskapa ett system som fanns tidigare i Sverige med särskilda avtal för särskilda krigsviktiga företag.

## 3.4 Kritisk infrastruktur, inbördes beroenden och kaskadeffekter

Stora delar av samhällets sektorer är beroende av varandra och det finns flera inbördes beroenden [MSB 2009]. *Kritiska beroenden* är beroenden som är avgörande för att samhällsviktiga verksamheter ska kunna fungera och dessa karaktäriseras av att ett bortfall eller en störning i verksamheterna, relativt omgående leder till funktionsnedsättningar, som kan få till följd att en extraordinär händelse inträffar [MSBFS 2015:5].

I den nationella säkerhetsstrategin[14] tas flera områdena upp som nationella intressen [Regeringskansliet 2017]. Robusthet och redundans som minskar beroendena mellan dessa områden och minskar påverkan från samhällsstörningar har också lyfts. Det finns därmed en stark koppling mellan de 7 civila områdena för att stärka nationell motståndskraft och utvecklingen av skyddet av samhällsviktig verksamhet på nationell nivå och vidare till en sammanhållen totalförsvarsplanering.

## 3.5 Hybridkrigföring, hybridhot och gråzon

### 3.5.1 Definitioner och begreppstolkningar

*Hybridkrigföring* ibland omnämnt som icke-linjär krigföring, har allt mer frekvent använts på senare år, inte minst efter Rysslands annektering av Ukraina 2014. Emellertid har det framförts argument kring att ökad användning av begreppet i sig inte ger vid handen att något ”nytt” egentligen förekommer. [Käihkö 2017]. Viktiga mål i hybridkrigföring är ofta strategiska civila och

[14] I strategin lyfts att robust försörjning och skydd av samhällsviktiga funktioner som centralt för befolkningens överlevnad och för ett fungerande samhälle. Alla delar av samhället är beroende av en trygg energiförsörjning. Tillgång till dricksvatten och livsmedel, fungerande sjukvård och läkemedelsförsörjning är nödvändigt för att trygga människors liv och hälsa. Transporter och kommunikationsmedel är vitala funktioner liksom en fungerande infrastruktur för försörjning, handel och ekonomi.

militära mål som ledningspersonal, ledningscentra och annan samhällsviktig verksamhet. Allianser där statliga aktörer utnyttjar en annan aktör som ombud, proxy, för att skapa större möjligheter och handlingsrum förekommer, inte minst, för att kunna förneka ansvar. Ickestatliga aktörer kan utrustas med resurser på statliga nivåer [Dengg & Schuria (eds) 2016].

I Försvarsutskottets utlåtande [2016/17:FöU2] ”Gemensam ram för att motverka hybridhot” sägs att begreppet *hybridhot* syftar till att fånga upp den blandning av konventionella och okonventionella metoder (såsom diplomatiska, militära, ekonomiska och tekniska) som statliga eller ickestatliga aktörer kan använda sig av på ett samordnat sätt för att uppnå särskilda mål, samtidigt som tröskeln för en formell krigsförklaring underskrids. Massiva desinformationskampanjer, där sociala medier används för att kontrollera det politiska landskapet kan användas för att underminera allmänhetens förtroende och försvåra beslutsfattandet. Påverkans- och desinformationskampanjer under eller före en masskadesituation eller sjukdomsutbrott kan urholka hälsosystemet genom exempelvis misstro mot vaccinationskampanjer. Likaså kan sociala medier användas för att radikalisera, rekrytera och styra proxy-aktörer. Hanteringen av hybridhot kräver omfattande samverkan och samordning mellan många olika offentliga och privata aktörer.

Viktigt att beakta är att händelser och/eller företeelser som uppfattas som antagonistiskt skulle kunna och ibland visar sig ha helt andra och i vissa fall naturliga orsaker (dvs. vad författarna avser med ”störd miljö”). Samhällets krisberedskap måste kunna förebygga och hantera krissituationer, oberoende av krisens orsaker. Osäkerhet kring om ett hybridhot föreligger eller ej får inte påverka samhällsaktörernas beredskap och förmåga att vidta tillräckliga åtgärder.

*Gråzon* har blivit en allt vanligare term för att beskriva ett tillstånd mellan fred och krig, orsakad av ett antal kombinerade antagonistiska aktiviteter som angriparen inte avser ska uppfattas som krigföring. [Jonsson 2018a, Jonsson 2018b].

### 3.5.2 Exempel på okonventionella metoder

Säkerhetspolisen lyfte i sin senaste årsrapport Ryssland som en aktör med en tydlig avsikt och utvecklad förmåga till att aktivt såväl som dolt påverka andra stater i en för Ryssland gynnsam riktning. Bland de verktyg som används är påverkansoperationer, strategiska uppköp, cyberoperationer inklusive elektroniska sabotage och militära maktdemonstrationer. Inte sällan sker påverkan via mellanhänder (proxies). Gråzonen används inte bara av Ryssland, även andra stater, som till exempel Kina, använder den i syfte att skaffa sig ett övertag som kan användas för att påverka ett annat land. De senaste årens

snabba tekniska utveckling och globalisering av ekonomier har skapat sårbarheter som gör dessa verktyg kraftfullare än tidigare. Denna utveckling skapar sammantaget ett stort behov av en ökad förmåga hos svenska myndigheter som har ansvar för att möta angrepp som inte främst utgör militära hot [Säkerhetspolisen 2019].

- Under 2016 rapporterade en nyanländ amerikansk diplomat i Havanna att han hörde ett högfrekvent ljud i sin trädgård. Det utgjorde upptakten till en serie händelser som ledde till att flera amerikanska diplomater upplevde sig drabbade av diverse åkommor som yrsel, huvudvärk, tinnitus, trötthet, oro, ångest och sömnproblem. Under 2017 kallades halva ambassadpersonalen temporärt hem. En möjlig förklaring som lyftes var att diplomaterna utsatts för riktade ljudvågor från ett hemligt vapen. Efter att ljudinspelningar analyserats antas ljudet komma från en karibisk kortvingad syrsa [Zimmer 2019, Stubbs & Montealegre 2019].
- I augusti 2018 upptäckte anställda vid ett mindre vattenverk i Sala att anläggningen hade utsatts för inbrott. Kommunen misstänkte risk för sabotage och kontaktade såväl polisen och säkerhetspolisen samt lät vattnet analyseras. Analyserna visade dock inte på någon påverkan. [VLT 2018].
- Enligt världshälsoorganisationen WHO har antalet fall av mässling ökat dramatiskt i Europa de två senaste åren. Från 5 273 konstaterade fall 2016, 25 863 fall 2017 till 82 596 fall 2018 – en ökning med drygt 1400 procent på tre år. Under 2018 dog 72 barn och vuxna av mässling i EU. Under 2018 skedde det största mässlingsutbrottet i Europa på ett sekel. Värst drabbat var Ukraina, men även Italien, Grekland, Ryssland, Serbien och Frankrike. Orsaken kan bland annat kopplas till den debatt om vacciners förtjänster och nackdel som fått en stadig position i hälsodebatten i samhället.

**Det nya normala**

Aktörers modus operandi i Ukraina demonstrerar en hybridkrigföring, där parallella påtryckningsmedel med ekonomiska, politiska, mediala, sociala, militära medel samt cyberattacker, verkar i kombination [Lanoszka 2016]. Medan fokus i medierapportering ofta ligger på militära aktioner, anges exempelvis i rysk militär doktrin att icke-militära, mer subtila attacker, utgör merparten av metoderna i moderna konflikter [Sinovets & Renz 2015].

## 3.6 Sveriges sju prioriterade områden vs Natos sju civila förmågor för nationell resiliens

*I raminstruktion* för det svenska civila beredskapsarbetet inom ramen för Nato/PFF (Partnerskap för fred) har sju prioriterade områden pekats ut för att stärka fredstida krisberedskap och arbetet med civilt försvar. Dessa sju områden har sin ungefärliga motsvarighet i Natos sju civila förmågor för att stärka nationell resiliens [Justitiedepartementet 2017]. Svenska myndigheter[15] måste förhålla sig till dessa baskrav (se figur 2).


**Figur 2**. Sveriges sju prioriterade områden i relation till Natos sju civila förmågor för nationell resiliens. Tre av de svenska prioriterade områdena har en ungefärlig motsvarighet i Natos civila förmågor medan tre av Natos förmågor utgör en delmängd av de svenska prioriterade områdena. En övergripande utmaning som inte definierats inom ramen för de sju svenska prioriterade områdena är ”Säkerställandet av civilt beslutsfattande och centrala ledningsfunktioner i händelse av en kris”.

Inom ramen PFF (Partnerskap för fred) är Sverige sedan 2014 en del av Natos *Enhanced Opportunities Programme* vilken möjliggör ett utvecklat och fördjupat samarbete med Nato, både avseende militärt samarbete och försvars- och säkerhetspolitisk dialog. Under 2014 undertecknades också ett värdlandsavtal med Nato som efter ett antal lagändringar trädde i kraft under

[15] Berörda myndigheter är enligt raminstruktionen; MSB, Socialstyrelsen, Jordbruksverket, Livsmedelsverket, Energimyndigheten, Transportstyrelsen och Trafikverket. Vid behov kan andra myndigheter bistå i arbetet; exempelvis FOI, FM, FHS, Affärsverket Svenska kraftnät, Sjöfartsverket, Kustbevakningen, Post- och telestyrelsen, SVA, Strålskyddsmyndigheten.

2016. Avtalet underlättar för Sverige att ta emot och ge militärt stöd i kristid och att stå som värdland för Natoövningar. Den nationella försvarsplaneringen är också nära sammankopplad med Natos och erfarenheter från deltagande i Nato-ledda insatser i t.ex. Afghanistan, Kosovo samt övningar som Trident Juncture 18, har ökat interoperabiliteten.

Det förändrade omvärldsläget har medfört återförsäkringsåtgärder inom alliansen och att principen om kollektivt försvar (Artikel 5 i det nordatlantiska fördraget) åter är i centrum, samtidigt som Natos engagemang i Afghanistan kvarstår och kapacitetshöjande stöd till Irak sker.

Ett fungerande samhälle utgör en barriär mot militära anfall och utan ett fungerande civilsamhälle finns inga förutsättningar för ett kollektivt försvar. Under kalla kriget hade Nato en omfattande logistikapparat, mobiliseringsplaner och oljelager, något som sedan dess successivt nedmonterats och nu är i behov av att återupptas [Lasconjaria 2017]. En av anledningarna till det återuppstådda behovet av beredskapslager och planer är den ökande insikten om att militära övningar och insatser i stor utsträckning idag är i princip helt beroende av civil infrastruktur såsom transporter, energiförsörjning och telekommunikationer.

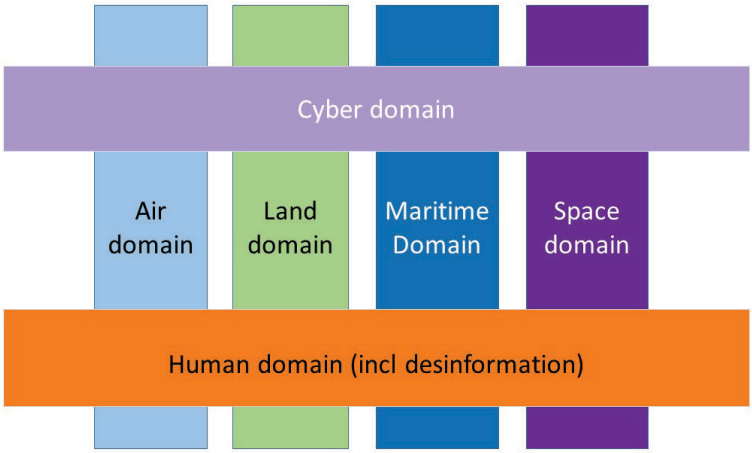
*Avskräckande motståndskraft (deterrence by resilience)*

En allt mer tydlig koppling görs mellan resiliens (Artikel 3 i det nordatlantiska fördraget) och tröskelhöjande effekt. Vid Natos toppmöte 2016 uttalades att alliansen skulle;

> "continue to enhance […] resilience against the full spectrum of threats, including hybrid threats, from any direction. Resilience is an essential basis for credible deterrence and defence and effective fulfilment of the Alliance's core tasks" [NATO 2016].

Motståndskraft och resiliens används beroende på sammanhang synonymt där båda avser dels den militära dimensionen med mål och medel för att hantera externa hot, dels civila samhällets förmåga att möjliggöra den militära missionen. Genom att minska civilsamhällets sårbarhet minskar sannolikheten för att det ska bli attackerat, och således stärks motståndskraften [Lasconjaria 2017, Kramer m.fl. 2015].

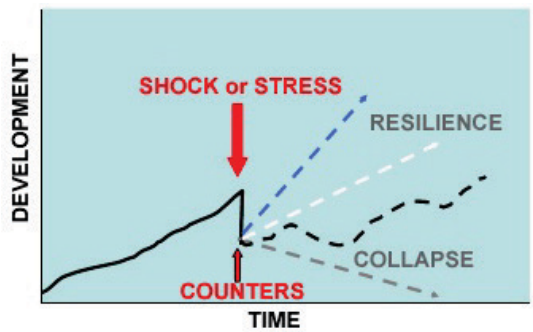
Traditionellt har fyra domäner för krigföring funnits inom Nato; mark-sjö- och luftstridskrafter samt rymden. Vid toppmötet 2016 adderades cyberdomänen och en cyberattack kan sedan dess aktivera Artikel 5. Inom Natos militärmedicinska verksamhet har ytterligare en domän börja diskuteras; informationsdomänen [Rots 2019]. Denna utvidgning reflekterar det "nya normala" där informationspåverkan och cyberattacker är något som tillhör vardagen snarare än utgör undantaget.




**Figur 3.** Natos traditionella och nya domäner för krigföring, där hybridhot, cyberattacker och desinformationskampanjer blivit en del av det ”nya normala” [Rots 2019].

## 3.7 Resiliens och nationell resiliens

Begreppet *resiliens* har olika betydelser beroende på det sammanhang[16] där det används men i korthet innebär resiliens hur ett system klarar av att motstå och återhämta sig från chocker och snabbt förändrade förutsättningar, se figur 4 [MSB 2013].




**Figur 4.** Resiliens som förmågan att motstå och återhämta sig från störningar över tid [Börjesson 2010.]

[16] Resiliens används inom exempelvis ekologi, sociologi och psykologi.

*Nationell resiliens* som ett centralt mål för samhällets krisberedskap har vuxit fram allt mer på senare år, inte minst sedan den uppdaterade raminstruktionen för det svenska civila beredskapsarbetet inom ramen för Nato/PFF fastställdes juni 2017 [Justitiedepartementet 2017, se även Försvarsdepartementet 2011].

Detta är inte ett nytt begrepp utan andemeningen finns beskrivet bl.a. i Nationell strategi för skydd av samhällsviktig verksamhet [MSB 2011]. Strategin syftar till att skapa ett mer resilient samhälle med en förbättrad förmåga att motstå och återhämta sig från allvarliga störningar i samhällsviktig verksamhet[17]. Syftet var också att skapa förutsättningar för att samhället ska fortsätta fungera på en acceptabel nivå vid allvarliga händelser och störningar.

Baserat på den nationella strategin har MSB i [NRFB 2017, MSB 2017] pekat ut sju prioriterade områden för att stärka såväl den fredstida krisberedskapen som arbetet med civilt försvar; energiförsörjning, livsmedel (inklusive dricksvatten), transporter, hälso- och sjukvård samt omsorg, finansiella tjänster, information och kommunikation, samt skydd och säkerhet.

**Hur samhällelig resiliens kan utgöra en första försvarsbarriär**

I likhet med åtgärder som syftar till att stärka motståndskraft och säkerhet mot antagonistiska händelser kan man se motståndskraft som bredare än så. I Gatwick-exemplet, se sida 25, skulle konsekvenserna för de drabbade i princip varit lika oavsett om orsaken till de inställda flygen varit en drönarattack, en isländsk vulkan eller en extrem väderhändelse. Förmågan att hantera och återhämta sig från en händelse kan dock variera mycket beroende på om händelsen är naturlig eller antagonistisk. Vissa naturligt orsakade händelser kan prognostiseras medan antagonistiska händelser vara mer svårbedömda. Man kan således se det som att motståndskraft handlar om att utforma sina system så att de är mer hållbara och innefattar en kontinuitetsplan och ett back-up-system för när det oönskade inträffar [Harris 2019].

[17] Samhällsviktig verksamhet definieras som en verksamhet som uppfyller minst ett av följande villkor; 1) Ett bortfall av eller en svår störning i verksamheten kan ensamt eller tillsammans med motsvarande händelser i andra verksamheter på kort tid leda till att en allvarlig kris inträffar i samhället. 2) Verksamheten är nödvändig eller mycket väsentlig för att en redan inträffad kris i samhället ska kunna hanteras så att skadeverkningarna blir så små som möjligt [MSBFS 2015:5].

# 4. Diskussion och förslag till fortsatt arbete

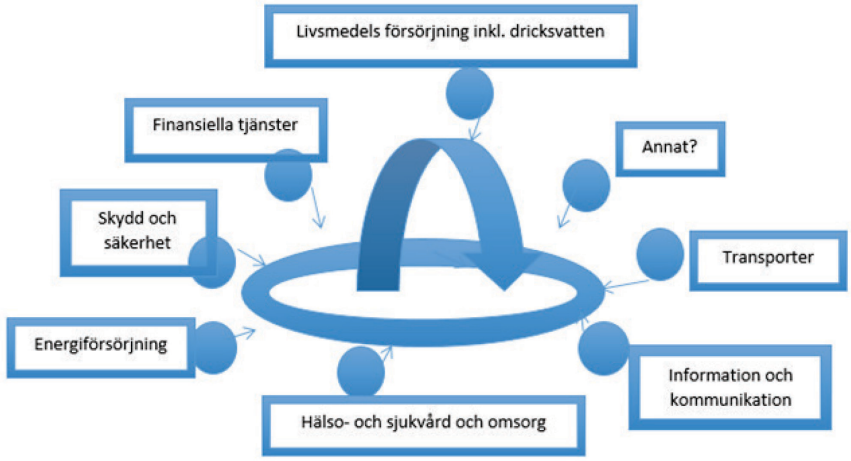
Hotbilden och hantering av en CBRN-händelse sker i ett sammanhang beroende på många omvärldsfaktorer (omvärldskontext). Vid en oavsiktlig CBR-händelse i fredstid och normaltillstånd, kan händelsen vara allvarlig, samtidigt som förutsättningarna för hantering (resiliensen) är relativt goda. Inövade och resurssatta förmågor och samverkansrutiner rörande hotanalys, identifikation, verifikation, spridningsmodellering, utrymning, sanering, sjukvård, säkrad forensik, transport och kommunikation kan väntas fungera väl.

Hantering av händelser med kemiska stridsmedel i Syrien komplicerades däremot av rådande krigstillstånd med begränsade sjukvårdsresurser, bristande förutsättningar till adekvat provtagning och säkrande av forensisk beviskedja, omfattande desinformation, försämrat grundhälsotillstånd hos drabbade och tillämpande av ny teknik i form av drönarförmåga och cyberkapacitet hos antagonisten eller dess allierade. Generellt sett präglas rapportering och analyser av händelser där kemiska ämnen använts av motstridiga uppgifter, antingen på grund av variationer i bedömningen av fakta, men även på grund av medveten desinformation med politiska förtecken.

Den här rapporten lyfter ett antal samhälls- och tekniktrender, av möjlig direkt eller indirekt betydelse för förmågor och förutsättningarna att effektivt identifiera och hantera en CBRN- händelse, och där kaskadeffekter kan påverka kritiska steg i hanteringskedjan. Exempel på en allvarlig kaskadeffekt kan vara en CBRN-händelse orsakad av längre energi- och internetbortfall, oavsett om dessa orsakats av ett tekniskt fel, en naturhändelse eller en antagonistisk aktivitet. Vilka steg i hanteringskedjan av CBRN-händelsen påverkas? Hur kan en robusthet skapas som säkrar hantering med tillräckliga förmågor av reservkraft och säkrad kommunikation?

En annan aspekt central för CBRN-händelser berör säkrade fakta, kommunikation och tillit. Ett exempel kan vara om dagens snabbt framväxande filterbubblor i sociala medier, inte sällan influerade av trollfabriker och ibland med stöd av AI vad gäller såväl manipulerad text som ansikten, fotografier och verbala yttranden, motsäger myndigheters information och budskap vid en CBRN-händelse. Kan detta påverka befolkningens vilja att agera i händelse av evakuering och utrymning? Ett ytterligare område som behöver utvecklas är förmågan att fånga upp och analysera multipla svaga signaler, som t.ex. mindre cyberattacker mot kritisk infrastruktur, i kombination med informationspåverkan och andra samhällsstörningar (se figur 5).

En annan fråga är hur eventuella antagonistiska attacker hanteras på olika nivåer (nationellt, regionalt och kommunalt) när osäkerhet råder om faktisk orsak till en CBRN-händelse.




**Figur 5.** Dagens prioriterade områden där behov finns av sektorsöverskridande samverkan m.a.p analys av svaga signaler.

I det fortsatta arbetet föreslås att olika nivåer av frågeställningens komplexitet hanteras successivt. I vilken mån olika former av hot, som kan tänkas uppträda simultant i en hybridhotskontext, påverkar varandra behöver undersökas närmare. Aktuella frågeställningar är kaskadeffekter, som t.ex. CBRN-händelser orsakade av cyberangrepp, och hur informations- och påverkanskampanjer har använts, och kan komma att användas, för att förstärka eller till och med konstruera ett CBRN-hot.

Teknikutveckling på områden av relevans för CBRN-området, som t.ex. bioteknik, följs inom andra FOI-projekt, men inom områden som är mer distanserade från CBRN-området har endast översiktliga studier gjorts. Ett intressant område är t.ex. de sårbarheter som utvecklingen inom artificiell intelligens skapar, och hur de skulle kunna utgöra ett indirekt CBRN-hot.

Under året har ett arbete påbörjats att analysera hur olika former av hybridkrigföring kan påverka hanteringen av en CBRN-händelse, med fokus på elavbrott. Detta arbete kommer att fortsätta och utvecklas till att omfatta flera av de områden som identifierats som prioriterade (se figur 2 sidan 35). Vissa områden, som t.ex. hälsa och sjukvård, har en uppenbar betydelse för hantering av en CBRN-händelse, medan andra kräver en djupare analys.

Arbetet med att bedöma effekter är omfattande och görs inom flera pågående projekt. Hur en CBRN-händelse påverkar de prioriterade områdena har till del studerats, till exempel sårbarheter i livsmedelskedjan efter ett radioaktivt nedfall [Brännström mfl. 2017]. Det föreslås att en inventering görs av vad som gjorts, och vad som genomförts, och vad som behöver studeras närmare.

Ovanstående är områden som identifierats som prioriterade att inhämta mer kunskap inom, med syftet att öka förståelsen för hur risken för CBRN-händelser, oavsiktliga såväl som antagonistiska, bör omhändertas i det återupptagna totalförsvarsarbetet. Inom ramen för det fortsatta arbetet i projektet kommer endast mindre delmängder att vara möjliga att omhänderta.

# 5. Referenser

## Myndighetspublikationer

Försvarsmakten (2016) Militärstrategisk doktrin, MSD 16

Försvarsmakten & Socialstyrelsen (2017) Totalförsvarets sjukvårdssystem. En civilmilitär förmågeutveckling inom hälso- och sjukvårdssektorn genom hela hotskalan. Bilaga till FM2016-16189:15 och SoS 11.1-30361/2017

Försvarsmakten (2019) Slutredovisning av Försvarsmaktens perspektivstudie 2016-2018. Tillväxt för ett starkare försvar

Försvarsdepartementet (2017) Motståndskraft Inriktningen av totalförsvaret och utformningen av det civila försvaret 2021–2025. Ds 2017:66

Försvarsdepartementet (2011) Raminstruktion för det civila krisberedskapsarbetet inom Nato (EAPR/PFF) Bilaga till protokoll vid regeringssammanträde 2011-02-24

FRA (Försvarets Radioanstalt, 2019). Årsrapport 2018.

Justitiedepartementet (2017) Raminstruktion för det svenska civila beredskapsarbetet inom ramen för Nato/PFF, 2017-06-22

MSB/Karios Future AB (2016) Framtidsstudie år 2030 med fokus på kommunal räddningstjänst organisation, MSB 1062

MSBFS 2015:5 föreskrifter och allmänna råd om kommuners risk- och sårbarhetsanalyser

MSB (Myndigheten för samhällsskydd och beredskap, 2017) Nationell risk- och förmågebedömning 2017, April 2017

MSB (2013) Resiliens; Begreppets olika betydelser och användningsområden. MSB569

MSB (2011) Ett fungerande samhälle i en föränderlig värld. Nationell strategi för skydd av samhällsviktig verksamhet. MSB266

MSB (2009) Faller en – faller då alla? En slutredovisning från KBM:s arbete med samhällskritiska beroenden. MSB 0001-09

MUST (Militära Underrättelsetjänsten, 2019) Årsöversikt 2018

Olsson J-O (2018) Mötesrapport från Civil prepardeness seminar on cross-sectoral interdependencies, i Bryssel, den 10 december 2018. MSB 2018-13560

Regeringskansliet (2018) En livsmedelsstrategi för Sverige − fler jobb och hållbar tillväxt i hela landet. Prop. 2016/17:104

Regeringskansliet (2017) Nationell Säkerhetsstrategi

Riksrevisionen 2018, Oklara förutsättningar för livsmedels- och läkemedelsförsörjning i en krissituation. Granskningsrapport 15 mars 2018

Räddningsverket (2006) Kartläggning av farligt godstransporter

Säpo (Säkerhetspolisen, 2019) Årsbok 2018

Trafikanalys tillsammans med MSB, Transportstyrelsen, Trafikverket och Sjöfartsverket; Trafikanalys (2015) Möjligheter att kartlägga flöden av farligt gods i Sverige – en förstudie. PM 2015:3

## Rapporter, artiklar

Blimark, M. (2014) Reduktionen av svensk kirurgisk operationskapacitet vid höjd beredskap, Självständigt arbete, 15 p FHS

CHPR (2016) Chemical Hazards and Poisons Report, Issue 26 April 2016

CSB Investigation Report, May 13 2018, Organic Peroxide Decomposition, Release, and Fire at Arkema Crosby Following Hurricane Harvey Flooding Crosby, Texas Incident Date: August 31, 2017 Exposures to Emergency Responders, Community Evacuation, and Property Damage, https://www.preventionweb.net/publications/view/58550

Deleuze, D., Chatelet, E. Laclemence, P. Piwowar, J. Affeltranger, B. (2008) Are safety and security in industrial systems antagonistic or complementary issues? In Safety, *Reliability and Risk Analysis: Theory, Methods and Applications*, Vol. 4, pp. 3039-3102

Dengg, A & Schurian, M (2016, eds.) Networked Insecurity – Hybrid threats in the 21st century. Schriftenreihe der Landesverteidigungsakademie, Ban 17, 2016

Franklin D. Kramer, Hans Binnendijk, and Daniel S. Hamilton, NATO's New Strategy: Stability Generation, Atlantic Council and Center for Transatlantic Relations, Washington D.C., September 2015, http://www.atlanticcouncil.org/images/publications/NATOs_new_strategy_web.pdf

GAO (The Government Accountability Office) 2018, Report to Congressional Committees, National Security. Long-Range Emerging Threats Facing the United States As Identified by Federal Agencies, December 2018

Gentile, Gian, David E. Johnson, Lisa Saum-Manning, Raphael S. Cohen, Shara Williams, Carrie Lee, Michael Shurkin, Brenna Allen, Sarah Soliman, and James L. Doty III, Reimagining the Character of Urban Operations for the U.S.

Army: How the Past Can Inform the Present and Future. Santa Monica, CA: RAND Corporation, 2017

Guillaume Lasconjarias 2017, Deterrence through Resilience: NATO, the Nations and the Challenges, NATO Defense College (NDC), Eisenhower Paper 7, 9 Jun 2017

IMPEL (2017), Preventing and minimizing acts of malicious intent, IMPEL - French Ministry of Sustainable Development/DGPR/SRT/BARPI

Institute for Economics and Peace (2018) Global Terrorism Index 2018, Measuring the Impacts of Terrorism

Käihkö, I. (2017). ”All Krigföring är av Hybrid Natur”. Statsvetenskaplig Tidskrift 118 (4): sid. 623-641

Lanoszka, A. (2016), Russian hybrid warfare and extended deterrence in eastern Europe, International Affairs, Volume 92, Issue 1, January 2016, Pages 175–195

Nato (North Atlantic Treaty Organisation, 2018a) Medical management of CBRN casualties, Nato Standard AMedP-7.1, Edition A, Version, 1 June 2018

Nato (North Atlantic Treaty Organisation, 2018b) Nato Framework For Future Alliance Operations 2018

Nato (2017a) Strategic Foresight Analysis 2017 ReportNato (2017 b) STO (Science and technology Organisation, 2017) STO Technology Trends Report, 21 March 2017

Nato-EAPC (2005) Senior Defence Group on Proliferation. 2005. Draft EAPC (DGP) guidelines on environmental and industrial hazards (EIH). Working paper. NATO/EAPC (DGP)WP(2005)0001-REV1. Working paper. May 30. On file with the authors.

OPCW (2017) Seventh report of the Organisation for the Prohibition of Chemical Weapons-United Nations Joint Investigative Mechanism (S/2017/904)

Pahi, Timea; Skopik, Florian. (2019) DAESH/TV5: Cyber Attribution 2.0: Capture the False Flag, European Conference on Cyber Warfare and Security, Reading : 338-345,XVIII. Reading: Academic Conferences International Limited. (Jul 2019)

Sinovets, P & Renz, B. (2015) Russia’s Military Doctrine and beyond: threat perceptions, capabilities and ambitions.  Nato Research Papers, No 117, July 2015

## FOI-publikationer

Björnham, O. Grahn, H. Von Schoenberg, P. Waleij, A. Liljedahl, B. Brännström, N. (2017) The 2016 Al-Mishraq sulphur plant fire: source and health risk area estimation. *Atmospheric Environment 169 (2017) 287-296.*

Brännström, N., Nylén, T., Ramebäck, H. (2017) Livsmedelsförsörjning efter radioaktivt nedfall. Fem limpor och en hel befolkning. Särtryck ur Strategisk Utblick 7, november 2017. FOI Memo 6177.

Börjegren S., Liljedahl B., Larsson A., Normark M., Tunemalm A-K., Waldenvik M., Waleij A. och Wikström P. (2019) Totalförsvarsplanering med fokus på CBRN. Framtida antagonistiska CBRN-hot. FOI-R-4765-SE

Eidenskog, D och Kamrani, F (2017) Internet of Things – En IT-säkerhetsmässig mardröm FOI Memo 6172

Gustavi T m.fl. Försvarsnära tillämpningar av artificiell intelligens FOI-D—0807--SE December 2017

Jonsson, D. (2018a) Typfall 5: Utdragen och eskalerande gråzonsproblematik FOI Memo 6338

Jonsson, D. (2018b) Gråzonsproblematik och hybridkrigföring - påverkan på energiförsörjning. FOI-R--4590--SE

Karlzén, H., Granlund, H., Wedlin, M. (2018) Operationer i cyberdomänen - En inventering av svensk forskning, FOI-R--4594--SE

Kindvall, G. & Wiss, Å. (red.) (2017), Militärteknik i ett tjugoårigt perspektiv: Underlag till Försvarsmaktens Perspektivstudie 2017, FOI-R--4462--SE

Lindgren F. Hotbildsunderlag i utvecklingen av civilt försvar (2014) FOI Memo 5089

Melin, L. (2000) Terrorism och kriminalitet. Incidenter med kemiska ämnen 1964-1999, FOA-R--00-01450-865--SE

Molin, L, Östensson, M. (2015) Förutsättningar för livsmedelsberedskap på kommunal nivå. FOI-R--4109--SE

Normark, M. mfl. (2019) CBRN-hot från ickestatliga aktörer – Årsrapport 2018, FOI-R-4766-SE

Normark, M. m.fl. (2017) CBRN-hot från ickestatliga aktörer – Årsrapport 2017, FOI-R-4583-SE

Roffey, R, Tunemalm, A-K., Waleij, A. (2019) Säkerhet för att motverka antagonistiska hot riktade mot kemisk industri: Internationell översikt. Under tryckning.

Tunemalm A-K. (2019) Antagonistiska hot mot anläggningar som hanterar kemikalier - Sammanfattande slutrapport. Ett projekt finansierat av anslag 2:4 Krisberedskap, juni 2017–december 2018. FOI Memo 6679

Waleij, A., Simonsson, L. Liljedahl, B (2019) Konsekvenser av energibortfall på samhället och civilbefolkningens hälsa" FOI-R-4755-SE

Waleij, A. Brännström, N. Liljedahl, L. Tjäder, Z. Tjärnhage, T. Wikström, P (2016) Evolving technologies- Challenges and opportunities from an operational health perspective, FOI-R-4256-SE

Waleij, A. Tjäder, Z. Liljedahl, L. Brännström, N (2015) Can additive manufacturing revamp supply chains for humanitarian aid or peace operations? FOI Memo 5569

## Hemsidor, bloggar, nyhetsartiklar

Allana, A (2017) How War Created the Cholera Epidemic in Yemen. New York Times, November 12, 2017, https://www.nytimes.com/2017/11/12/opinion/cholera-war-yemen.html

BBC (2019) Gatwick drones: Military stood down after airport chaos, 3 January 2019, https://www.bbc.com/news/uk-england-sussex-46741687

BBC, Russia suspected of jamming GPS signal in Finland 12 November 2018, https://www.bbc.com/news/world-europe-46178940

Beyerer, J. & Martini, P. (2018) Grand defence-technological challenges for Europe post-2020. Position paper. Fraunhofer Group for Defense and Security.

Börjesson, M. 2010 En mer riskfylld och osäker värld driver strukturella förändringar https://www.futuramb.se/en-mer-riskfylld-och-osaker-varld-driver-strukturella-forandringar/

Campanello, S. (2017) 500 000 routrar hackade – Ryssland anklagas för attacken, Ny Teknik, 24 maj 2017

Cole, S. (2019) Ready or not, the quantum computing revolution is here. Military Embedded Systems, 10 June 2019, http://mil-embedded.com/articles/ready-not-quantum-computing-revolution-here/

DARPA. Lightweight, Soft Exosuit Aims to Prevent Musculoskeletal Injury in Warfighters. DARPA. 2014.

Dobos, L. (2019) Ryssland testar att koppla bort internet, https://techworld.idg.se/2.2524/1.714370/ryssland-kopplar-bort-internet

Dunn 2018, Soldiers sent hate-SMS messages from rogue base stations, Naked Security 12 May2017, https://nakedsecurity.sophos.com/2017/05/12/soldiers-sent-hate-sms-messages-from-rogue-base-stations/

Folkhälsomyndigheten (2018) Ökad dödlighet under sommarens värmebölja, https://www.folkhalsomyndigheten.se/nyheter-och-press/nyhetsarkiv/2018/december/okad-dodlighet-under-sommarens-varmebolja/

Giles, M (2019) MIT Technology Rewiev (2019) The US and China are in a quantum arms race that will transform warfare, January 3, 2019, https://www.technologyreview.com/s/612421/us-china-quantum-arms-race/

Green, A (2018) Drones rain tear gas down on protesters as 35,000 Palestinians clash with Israeli security forces on the Gaza border. Mail Online, 14 May 2018. https://www.dailymail.co.uk/news/article-5728431/Israeli-drones-rain-tear-gas-Palestinian-protesters-Gaza.html

Grierson, J (2019) Gatwick returns to normality but drone threat remains, The Guardian Friday 4 Jan 2019 https://www.theguardian.com/world/2019/jan/04/gatwick-returns-to-normality-but-drone-threat-remains

Grenberg, A. (2018) The Untold Story of NotPetya, the Most Devastating Cyberattack in History. Wired 33 Augsut 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Harris T, 2019, Modern Deterrence and Societal Resilience, Commentary, 10 January 2019, Modern Deterrence, https://rusi.org/commentary/modern-deterrence-and-societal-resilience

Hållén, J. Israel och USA bakom Stuxnet. NyTeknik. 17 januari 2011.
Johansson, J. (2017) Så skyddar du dig mot Ransomware-attacker, SVT Nyheter, 12 maj 2017.

Maldarelli, C. (2015) Bionic Suits helps a paralyzed man takes thousands of steps, Popular Science, September 4, 2015

Mathews L. (2019) North Korean Hackers Have Raked in $670 Million Via Cyberattacks. Forbes, March 11, 2019. https://www.forbes.com/sites/leemathews/2019/03/11/north-korean-hackers-have-raked-in-670-million-via-cyberattacks/#4aeeeb1c7018

MIT Technology Rewiev 2019 Triton is the world's most murderous malware, and it's spreading https://www.technologyreview.com/s/613054/cybersecurity-critical-infrastructure-triton-malware/

Moon, A (2019) State-sponsored cyberattacks on banks on the rise: report. Reuters, March 22. https://www.reuters.com/article/us-cyber-banks-idUSKCN1R32NJ

NATO, “Commitment to enhance resilience,” issued by the Heads of State and Government, Warsaw, 8 July 2016, http://www.nato.int/cps/en/natohq/official_texts_133180.htm

Nicol, M. (2018) Jihadis are plotting a devastating Chemical Weapons attack in Britain and could launch a chlorine bomb on London Underground, security chiefs warn, Daily Mail, 8 December 2018. https://www.dailymail.co.uk/news/article-6474997/Security-chiefs-believe-Jihadis-plotting-devastating-chemical-weapons-attack-Britain.html

Nyheter 24 (2018) O'boy-brist i hela Sverige, https://nyheter24.se/nyheter/inrikes/913530-oboy-brist-i-hela-sverige

O'Dwyer Gerard, Finland, Norway press Russia on suspected GPS jamming during NATO drill, November 16, 2018, https://www.defensenews.com/global/europe/2018/11/16/finland-norway-press-russia-on-suspected-gps-jamming-during-nato-drill/

Ohlsson Erik (2017) Spåren efter giftmordet på Kim Jong-Nam leder till Nordkoreas makttopp. Dagens Nyheter 6 april.

Ooda Loop (2019) The Pentagon’s Cybersecurity Is Falling Behind https://www.oodaloop.com/briefs/2019/01/28/the-pentagons-cybersecurity-is-falling-behind/

Perlroth, N., Krauss, C. 15 mars 2018. A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try. The New York Times. 23 October 2018. https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html

Postma, F. (2018) After Strava, Polar is Revealing the Homes of Soldiers and Spies. July 8, 2018, https://www.bellingcat.com/resources/articles/2018/07/08/strava-polar-revealing-homes-soldiers-spies/

Roth, A (2019) Russia’s great firewall: is it meant to keep information in – or out?”, The Observer 28 April 2019, https://www.theguardian.com/technology/2019/apr/28/russia-great-firewall-sovereign-internet-bill-keeping-information-in-or-out

Rots G J.M. (2019) Update to COMEDS MedIntel-p. Presentation av NATO IMS Medical Advisor, 16 mars 2019, Bryssel.

Sanborn B. (2018) How hospitals are grappling with medical supply shortages caused by Hurricane Maria, 8 January, http://www.healthcarefinancenews.com/news/how-hospitals-are-grappling-medical-supply-shortages-caused-hurricane-maria

Sanger, D. E. Hack of Saudi Petrochemical Plant Was Coordinated From Russian Institute. The New York Times. 23 oktober 2018. https://www.nytimes.com/2018/10/23/us/politics/russian-hackers-saudi-chemical-plant.html

Ståhl, E. (2019) Snöoväder drar över Sverige - flyg inställda på Arlanda. Svenska Yle, 16 januari 2019, https://svenska.yle.fi/artikel/2019/01/16/snoovader-drar-over-sverige-flyg-installda-pa-arlanda

Synek, G. 15 mars 2018. Saudi Arabian petroleum plant hit with malware that tried to cause an explosion, Techspot. https://www.techspot.com/news/73730-saudi-arabian-petroleum-plant-hit-malware-tried-cause.html

SR (2019) Svenska Kraftnät medger säkerhetsbrister https://sverigesradio.se/sida/artikel.aspx?programid=83&artikel=7146888

SVT (2019a), Brist på el hotar delar av Sverige: ”Har kommit väldigt snabbt” Publicerad 21 januari 2019 https://www.svt.se/nyheter/inrikes/brist-pa-el-hotar-delar-av-sverige

SVT (2019b) Sprängattentat mot ställverk i Spånga, 7 januari 2019, https://www.svt.se/nyheter/lokalt/stockholm/sprangattentat-mot-stallverk-i-bromma

SVT (2017) FRA: IT-spioner förbereder attack mot elnätet, 9 januari 2017, https://www.svt.se/nyheter/inrikes/it-spioner-forbereder-attack-mot-elnatet

Toler, A. (2018) How to Use and Interpret Data from Strava’s Activity Map, January 29, 2018, https://www.bellingcat.com/resources/how-tos/2018/01/29/strava-interpretation-guide/

The Baltic Course 2018, Fake news about poisonous spiders spread in Riga, BC, Riga, 31.07.2018, http://www.baltic-course.com/eng/baltic_news/?doc=19743

Security Service of Ukraine (2018) Dnipropetrovsk region: SBU prevents cyberattack of Russian special services on critical infrastructure facility. 7 November 2018 https://ssu.gov.ua/en/news/1/category/1/view/5037#.f1hLYq98.dpbs

UK Government (2018) https://www.gov.uk/government/speeches/pm-statement-on -the-salisburty-investigation-5-september-2018 (Prime Minister

Theresa May´s statement to Parliament about the Salisbury incident, made on 5 September 2018.)

Unian Information Agency 2018, Donbas militants using terrifying text messages to shock adversary, changing face of warfare 15 August 2018 https://www.unian.info/war/10226025-donbas-militants-using-terrifying-text-messages-to-shock-adversary-changing-face-of-warfare.html

VLT 24 augusti 2018 Inbrott på vattenverk i Sala kan vara sabotage – Säpo har kopplats in, https://www.vlt.se/artikel/sala/inbrott-pa-vattenverk-i-sala-kan-vara-sabotage-sapo-har-kopplats-in

Watson, B. (2017) The Drones of ISIS. DefenceOne, 12 January 2017https://www.defenseone.com/technology/2017/01/drones-isis/134542/

Wiklund, K. (2017) Det här vet vi om Wannacry-attacken. Ny Teknik, 16 maj 2017, https://www.nyteknik.se/digitalisering/det-har-vet-vi-om-wannacry-attacken-6848974

Zimmer Carl (2019) The Sounds That Haunted U.S. Diplomats in Cuba? Lovelorn Crickets, Scientists Say. New York Times Jan. 4, 2019 https://www.nytimes.com/2019/01/04/science/sonic-attack-cuba-crickets.html

Stubbs, Alexander L & Montealegre-Z Fernando (2019) Recording of "sonic attacks" on U.S. diplomats in Cuba spectrally matches the echoing call of a Caribbean cricket bioRxiv January 04, 2019 doi: https://doi.org/10.1101/510834

Yong Jeremy Au, When a real fire and a fake video collide, Feb 26 2017. https://www.straitstimes.com/singapore/whatstrending-when-a-real-fire-and-a-fake-video-collide

Bilaga 1: Ordlista

| **Begrepp** | **Förklaring** |
|---|---|
| Aktör/antagonist | En aktör/antagonist är den eller de som genomför det praktiska angreppet. |
| Förmåga | Förmåga är de möjligheter en aktör har att fullgöra sina uppgifter |
| Gråzon | Det finns ingen allmänt vedertagen definition av ”gråzon”. Med gråzon avses här ett fredstida tillstånd med inslag av statsunderstödda antagonistiska angrepp, t ex cyberangrepp. |
| Hot | Ett hot är den sammanvägda bilden av en angripares vilja och förmåga att angripa ett skyddsvärde. I vissa fall kan hotet beskrivas som den sammanvägda bilden av intention, kapacitet och tillfälle. |
| Hybridhot | Hybridhot syftar till att fånga upp den blandning av konventionella och okonventionella metoder (såsom diplomatiska, militära, ekonomiska och tekniska) som statliga eller ickestatliga aktörer kan använda sig av på ett samordnat sätt för att uppnå särskilda mål, samtidigt som tröskeln för en formell krigsförklaring underskrids. |
| Hybridkrigföring | En kombination av flera gråzonstaktiker kan utgöra något som skulle kunna benämnas som hybridkrigföring. Men hybridkrigföring kan också vara ett påtagligt inslag i en krigssituation. Gråzonen kan ses som ett tillstånd eller ett skede som syftar till att vinna något utan eskalering och/eller att skapa fördelar inför en eventuellt eskalerad situation, dvs. krigsförberedelser. Hybridkrigföring är därmed något som kan förknippas med såväl gråzonen som kriget. |
| Intention | En angripares intention består av den uttalade eller påvisade vilja som angriparen innehar för ett angrepp. |
| Konsekvens | Den konsekvens som uppstår när ett skyddsvärde förloras eller komprometteras. |
| Kontext | Kontext betyder omständigheter, sammanhang, omgivning, eller övergripande situation. |
| Kritisk infrastruktur | Internationellt och inom EU används begreppet skydd av kritisk infrastruktur. Kritisk infrastruktur definieras som fysisk struktur vars funktionalitet bidrar till att säkerställa upprätthållandet av viktiga samhällsfunktioner. I Sverige har vi en bredare definition av begreppet, nämligen skydd av samhällsviktig verksamhet. |
| Modus | Det tillvägagångssätt eller den metod en angripare använder sig av vid angrepp. Begreppet Modus, eller Modus Operandi, används såväl för att ange en konkret metod som en strategi för angrepp. |
| Motståndskraft | Försvarsberedningens använder motståndskraft istället för resiliens (se resiliens). I denna rapport används dessa begrepp synonymt. |
| Sårbarhet | Det finns en hel del skilda uppfattningar mellan olika vetenskapliga discipliner om hur begreppet sårbarhet ska definieras eller tolkas. Gemensamt för flertalet definitioner är hur kapabla individer och samhällen är, givet deras sociala, ekonomiska och kulturella förmåga, att hantera de skador som kan uppstå som följd av exempelvis en antagonistisk händelse och/eller en naturolycka. |

FOI är en huvudsakligen uppdragsfinansierad myndighet under Försvarsdepartementet. Kärnverksamheten är forskning, metod- och teknikutveckling till nytta för försvar och säkerhet. Organisationen har cirka 1000 anställda varav ungefär 800 är forskare. Detta gör organisationen till Sveriges största forskningsinstitut. FOI ger kunderna tillgång till ledande expertis inom ett stort antal tillämpningsområden såsom säkerhetspolitiska studier och analyser inom försvar och säkerhet, bedömning av olika typer av hot, system för ledning och hantering av kriser, skydd mot och hantering av farliga ämnen, IT-säkerhet och nya sensorers möjligheter.

FOI
Totalförsvarets forskningsinstitut
164 90 Stockholm

Tel: 08-55 50 30 00
Fax: 08-55 50 31 00

www.foi.se