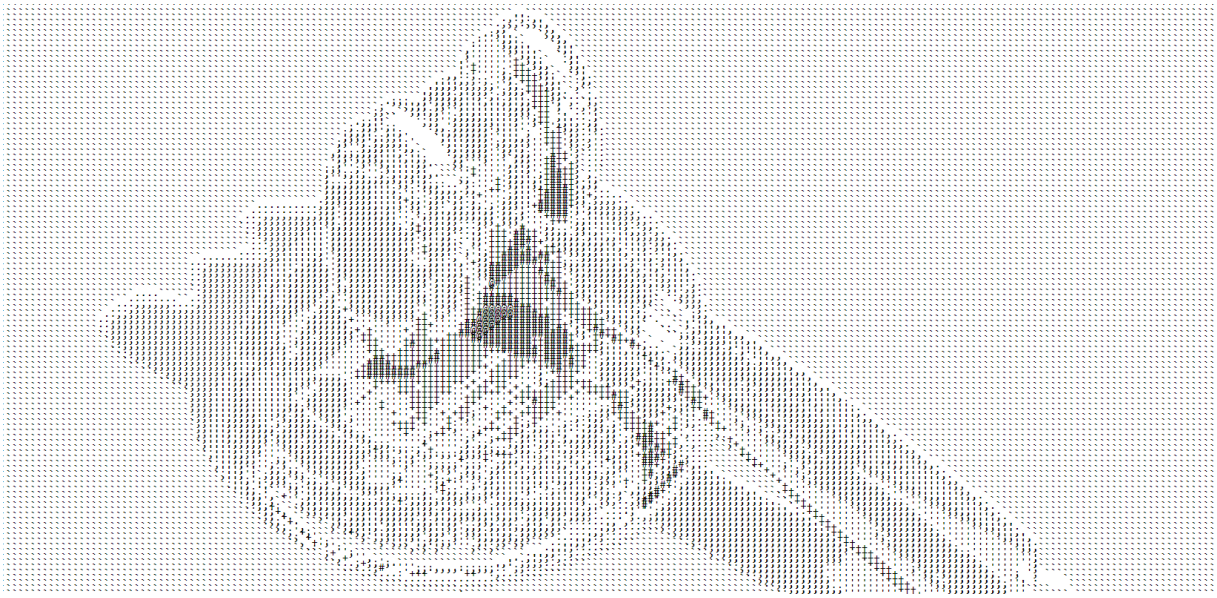
Aktiva operationer på cyberdomänen

Folkrättslig normativ utveckling

ERIK ZOUAVE



FOI-R--4776--SE
ISSN 1650-1942 Januari 2019

Erik Zouave

Aktiva operationer på cyberdomänen

Folkrättslig normativ utveckling

Titel	Aktiva operationer på cyberdomänen: Folkrättslig normativ utveckling
Title	Active operations in the cyber domain: The development of International law
Rapportnr/Report no	FOI-R--4776--SE
Månad/Month	Januari
Utgivningsår/Year	2019
Sidor/Pages	29 p
Kund/Customer	Försvarsmakten
Forskningsområde	12. Övrigt
FoT-område	Cyber
Projektnr/Project no	E72787
Godkänd av/Approved by	Christian Jönsson
Ansvarig avdelning	Ledningssystem

Sammanfattning

Totalförsvarets forskningsinstitut (FOI) har fått i uppdrag att stödja uppbyggnaden av Försvarsmaktens förmåga att genomföra operationer i cyberdomänen, särskilt med fokus på aktiva operationer och med efterlevnad av folkrätten. Denna rapport bidrar med en övergripande lägesbild av den internationella utvecklingen av folkrättsliga normer för cyberoperationer och dess implikationer för aktiva cyberoperationer. Lägesbilden fokuserar på normutveckling inom överstatliga organisationer av strategiskt intresse för svensk säkerhets- och försvarspolitik, i synnerhet Förenta nationerna, Europeiska Unionen, Nordatlantiska fördragsorganisationen, och Organisationen för säkerhet och samarbete i Europa. Det internationella normutvecklande arbetet sammanfaller ofta med en diplomatisk vilja att upprätta förtroendeskapande åtgärder för internets styrning och i synnerhet internets säkerhet och stabilitet. Medan det finns en utbredd konsensus att folkrätten gäller på cyberdomänen, särskilt FN-stadgan, krigets lagar och mänskliga rättigheter, finns det ingen utbredd konsensus om hur dessa ska tillämpas. I de fall där tillämpningsåtgärder börjar utvecklas tenderar man att välja icke-bindande former för tillämpning av folkrätten, såsom vägledningar, manualer och studier.

Nyckelord: Aktivt cyberförsvar, aktiv cyberförmåga; aktiva cyberoperationer, offensiva cyber; folkrätt; krigets lagar

Summary

The Swedish Defence Research Agency (FOI) has been commissioned to support the Swedish Armed Force's ability to conduct operations in the cyber domain, focusing on active operations and compliance with international law. This is a situational report on the current developments of international law norms for cyber operations and their implications for active cyber. The report focuses on normative development within supranational organizations of strategic interest for Swedish security and defence policy, especially the United Nations, the European Union, the North Atlantic Treaty Organization, and the Organization for Security and Cooperation in Europe. The normative development often coincides with a diplomatic will to establish confidence-building measures for the governance of and, in particular, the security and stability of the Internet. While there is a widespread consensus that international law applies in the cyber domain, especially the UN Charter, the international laws of armed conflict, and human rights, there is no widespread consensus on how to implement them. In cases where implementation measures are beginning to develop, it is frequently through non-binding instruments such as guides, manuals and studies.

Keywords: Active cyber defence; active cyber capabilities; active cyber operations; offensive cyber; international law; laws of international armed conflict

Innehållsförteckning

1 Inledning

Totalförsvarets forskningsinstitut (FOI) har fått i uppdrag att stödja uppbyggnaden av Försvarsmaktens förmåga att genomföra operationer i cyberdomänen. En del i detta är ”förmågan att, i enlighet med folkrätten, genomföra aktiva operationer i cybermiljön”[1].[2] Liksom andra militära förmågor måste den aktiva cyberförmågan förhålla sig till relevanta rättsakter och lagrum, inklusive folkrätten. Utgångspunkterna för svensk försvars- och säkerhetspolitik ligger dels i skyddet av svenska grundläggande rättigheter,[3] dels en världsordning i stort som grundar sig på efterlevnad av folkrätten.[4] Detta är även belagt i relation till Försvarsmaktens förmåga och verksamhet i cybermiljön:

> *Ett it-angrepps möjliga påverkan på flera sektorer i samhället har enligt Försvarsberedningen påskyndat diskussionerna om både nationell och internationell reglering och lagstiftning. Det är vidare Försvarsberedningens uppfattning att folkrätten i fred (FN-stadgans folkrätt) och folkrätten i krig (krigets lagar) kvarstår som legala principer även för aktioner i cybermiljön. Regeringen delar denna uppfattning.*[5]

I mars 2010 överlämnade Folkrättskommittén delbetänkandet *Krigets Lagar – centrala dokument om folkrätten under väpnad konflikt, neutralitet, ockupation och fredsinsatser SOU 2010:22.* Delbetänkandet reviderade dokumentsamlingen *Krigets Lagar*, som gavs ut 1996 av Försvarsdepartementet genom Totalförsvarets folkrättsråd. Betänkanden sammanställde bland annat en förteckning över gällande humanitärrättsliga traktat. Tematiskt sammanställdes de tillämpliga konventionerna, deklarationerna, manualerna och andra dokument angående folkrätten och militära operationer utan att särskilt beröra de militära operationerna på cyberdomänen. I oktober 2010 överlämnade Kommittén sedan slutbetänkandet *Folkrätt i väpnad konflikt – svensk tolkning och tillämpning SOU 2010:72* som utgör en kartläggning av folkrätten och svensk tillämpning av dessa samt förslag till lagändringar. Slutbetänkandet innehöll en särskild analys av *IT-krigets lagar*.[6] Kommittén uppmärksammade två tidiga konferenser för att förtydliga tillämpningen av krigets lagar i ”cyberrymden” och ”datanätverksattacker”.[7] Den första konferensen var den 28:e Internationella rödakors- och rödahalvmånekonferensen i december 2003 där diskussioner påbörjades om tillämpningen av krigets lagar vid dator- och nätverksattacker. Den andra konferensen kallades ”International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law” som anordnades av Regeringskansliet och Försvarshögskolan november 2004.[8] Folkrättskommittén bedömde under sitt arbete 2010 att det inte fanns förutsättningar att enas kring tolknings- och tillämpningsfrågor internationellt.[9]

Den specifika tillämpningen av folkrätten vid användningen av aktiva cyberförmågor är inte heller klarlagd. En analys av folkrättsliga utmaningarna för den aktiva cyberförmågan har

[1] Inriktning för Försvarsmaktens verksamhet för åren 2016 till och med 2020 (Fö2015/00953/~FI), sid 11
[2] Se även Försvarspolitisk inriktning – Sveriges försvar (Prop 2014:15:109); Nationell strategi för samhällets informations- och cybersäkerhet (Skr. 2016/17:213)
[3] Nationell strategi för samhällets informations- och cybersäkerhet (Skr. 2016/17:213); Försvarspolitisk inriktning – Sveriges försvar (Prop 2014:15:109); Motståndskraft Inriktningen av totalförsvaret och utformningen av det civila försvaret 2021–2025 (Ds 2017:66)
[4] Regeringsbeslut: FI Inriktning för Försvarsmaktens verksamhet för åren 2016 till och med 2020 (Fö2015/00953/~), sid 20
[5] Regeringsbeslut: FI Inriktning för Försvarsmaktens verksamhet för åren 2016 till och med 2020 (Fö2015/00953/~), sid 112
[6] Folkrätt i väpnad konflikt – svensk tolkning och tillämpning (SOU 2010:72), sid 259-261
[7] Notera att Kommittén använder begreppet ”datanätverksattacker” till skillnad från Försvarsmaktens och Försvarets radioanstalts begrepp ”dator- och nätverksattacker” – se Försvarsmakten och Försvarets Radioanstalt (2016) Överenskommelse Om gemensamma begrepp för Cyberområdet, Bilaga 1 Till FM 2016-129 50
[8] Folkrätt i väpnad konflikt – svensk tolkning och tillämpning (SOU 2010:72), sid 260
[9] Folkrätt i väpnad konflikt – svensk tolkning och tillämpning (SOU 2010:72), sid 260-261

tidigare efterfrågats vid Riksdagens interpellationer utan konkreta gensvar.[10] De medel och metoder som tillämpas i en aktiv cyberförmåga är inte kungjorda för allmän kännedom.[11] Även de internationella diskussionerna om folkrättens tillämpning vid användandet av aktiva cybercyberoperationer bedöms vara i ett formativt skede.[12] Således försvåras en grundlig analys av folkrättsliga aspekter på aktiv cyberförmåga.

Syftet med denna rapport är att bidra med en lägesbild av den internationella folkrättsliga utvecklingen; så kallad normutvecklande verksamhet. Lägesbilden innefattar en kartläggning av:

- överstatliga forum för normutvecklande verksamhet;
- samstämmighet, oenighet och kontroverser kring folkrättsliga normer samt
- konkreta exempel på förslag om folkrättens tillämpning inom aktiva cyberförmågor.

Lägesbilden fokuserar på överstatliga organisationer vars utveckling av normer är av strategiskt intresse för svensk säkerhets- och försvarspolitik.[13] Informationsinhämtningen är avgränsad till normer med relevans för cyberförsvar. Rapporten redovisar även kort över förhållandet mellan dessa normer och begreppsapparaten för aktiva cyberförmåga utifrån svensk försvarspolicy och doktrin. Lägesbilden påvisar en samstämmig syn om att folkrätten gäller även i cyberrymden, i synnerhet FN-stadgan, de mänskliga rättigheterna, och krigets lagar. Däremot saknas det samstämmighet om tillämpningen av dessa normer i cyberrymden. Avsaknaden av vedertagen tillämpning är särskilt påtaglig för militär cyberverksamhet, och i synnerhet för aktiva cyberoperationer.

[10] Offensiv cyberförmåga Interpellation 2017/18:22

[11] Se exempelvis Informationssäkerhet i Sverige och internationellt – en översikt (SOU 20014:32), sid 29-31; Svar på skriftlig fråga 2017/18:75 Svar på fråga 2017/18:75 av Pål Jonson (M) Aktiv cyberförmåga; Riksdagens protokoll 2017/18:21, sid 9-15

[12] Försvarsdepartementet (2014) Försvaret av Sverige- Starkare försvar för en osäker tid (Ds 2014:20), sid 32-34; Slutbetänkande av Folkrätt i väpnad konflikt – svensk tolkning och tillämpning (SOU 2010:72), sid 260-261

[13] Regeringsbeslut: FI Inriktning för Försvarsmaktens verksamhet för åren 2016 till och med 2020 (Fö2015/00953/~), sid 8, 46-47, 56

2 Aktiv cyberförmåga

Det finns ingen öppen, uttömmande, och tydlig förklaring av vilka operativa medel och metoder som utgör en aktiv cyberförmåga i svensk kontext. Detta är en avgörande begränsning för en rättslig analys då folkrätten främst förhåller sig till vilka medel och metoder som är tillåtna, respektive otillåtna, samt vilka rättsliga garantier som bör föreligga vid användningen av vissa medel och metoder. Nedanstående redovisning av begreppsapparaten ur svensk policy och doktrin utgör inte heller en uttömmande sammanställning av begreppens innehåll. Redovisningen används snarare för att inventera bredden av relaterade begrepp ur ett svenskt perspektiv och för att inrikta slutsatser om utvecklingen av normer som bedrivs inom överstatliga organisationer.

Begreppsapparaten för svensk försvars- och säkerhetspolitik omfattar ett flertal närliggande men diffust definierade begrepp avseende ett *aktivt cyberförsvar*; till exempel *aktiva cyberförmågor*, (*aktiva) operationer* i cybermiljön, *offensiv förmåga, offensiva cyberoperationer*, samt *aktivt informationsteknologiskt försvar*.[14] Dessutom finns oklarheter kring bruket av begreppen *aktivt* och *offensivt* i samband med militär verksamhet i cybermiljön, till exempel försvar, förmåga och operation.

En beskrivning av aktiv cyberförsvarsförmåga är att den, till skillnad från en passiv förmåga, inbegriper *motoperationer* till fientlig verksamhet. Detta är inte en vedertagen svensk definition, utan snarare ett svenskt perspektiv på Natos begreppsanvändning.[15] Offensivt agerande, å andra sidan, handlar om att ta initiativet i en situation för att kunna avgöra de på egna villkor, till skillnad från defensivt som snarare handlar om att förhindra att en situation förvärras.[16]

Flera källor antar att det finns en relation mellan aktivt cyberförsvar och *dator- och nätvärksoperationer*[17] (alternativt kallat *datornätverksoperationer*[18]).[19] Enligt Försvarsmaktens egen begreppsapparat skulle detta innebära att följande medel och metoder vore möjliga åtgärder inom det aktiva cyberförsvaret:

- *Dator- och nätverksförsvar (Computer Network Defense – CND)* som åsyftar skydd av *information, informationssystem (*alternativt *tekniska system), datorer* och *nätverk* från en offensivt agerande motståndare.[20]
- *Dator- och nätverksexploatering (Computer Network Exploitation – CNE)* som åsyftar *kartläggning* och *åtkomst* till motståndares *information, informationssystem [*alternativt *tekniska system], datorer* och *nätverk*.[21] *SOU 20014:32*

[14] Försvarsutskottets betänkande: Försvarspolitisk inriktning - Sveriges försvar 2016-2020 (2014/15:FöU11); Nationell strategi för samhällets informations- och cybersäkerhet (Skr. 2016/17:213)

[15] Försvarsdepartementet (2014) Försvaret av Sverige- Starkare försvar för en osäker tid (Ds 2014:20), sid 32

[16] Försvarsmakten (2016) *Militärstrategisk Doktrin 2016 (MSD16);* Försvarsmakten (2014) *Operativ Doktrin 2014 (OPD);* Försvarsdepartementet (2013) Försvarsmaktens redovisning av perspektivstudien 2013 (FM2013-276:1), sid 32

[17] Se Försvarsmakten och Försvarets Radioanstalt (2016) Överenskommelse Om gemensamma begrepp för Cyberområdet, Bilaga 1 Till FM 2016-129 50; Försvarsmakten (2008) Försvarsmaktens Handbok Informationsoperationer: Handbok Info Ops (09 833:61968)

[18] Se Informationssäkerhet i Sverige och internationellt – en översikt (SOU 20014:32), sid 29

[19] Svar på skriftlig fråga 2017/18:75 Svar på fråga 2017/18:75 av Pål Jonson (M) Aktiv cyberförmåga; Mikael Holmström. (2015). *Försvarsministern: Vi ska kunna genomföra cyberattacker.* från: https://www.dn.se/nyheter/sverige/forsvarsministern-vi-ska-kunna-genomfora-cyberattacker/. senast 23/01/2018; Dag Enander. (2016). *”DET DIGITALA STRIDSFÄLTET ÄR EN REALITET”: Därför vill Försvarsmakten ha aktiv cyberförmåga.* från: https://www.forsvarsmakten.se/siteassets/6-aktuellt/forsvarets-forum/2016/forsvarets-forum-3-2016.pdf. senast 23/01/2018; Jonas Lejon. (2016). *VAD INNEBÄR EN AKTIV SVENSK CYBERFÖRMÅGA?.* från: https://kryptera.se/cyberformaga/. senast 23/01/2017

[20] Försvarsmakten (2008) Försvarsmaktens Handbok Informationsoperationer: Handbok Info Ops 09 833:61968; Försvarsmakten och Försvarets Radioanstalt (2016) Överenskommelse Om gemensamma begrepp för Cyberområdet, Bilaga 1 Till FM 2016-129 50

[21] Försvarsmakten (2008) Försvarsmaktens Handbok Informationsoperationer: Handbok Info Ops 09 833:61968; Försvarsmakten och Försvarets Radioanstalt (2016) Överenskommelse Om gemensamma begrepp för Cyberområdet, Bilaga 1 Till FM 2016-129 50

Informationssäkerhet i Sverige och internationellt – en översikt föreslår (utöver Försvarsmaktens egen nomenklatur) föreslår även att CNE-förfarandet kan inbegripa utveckling och användning av skadlig programvara för att bereda tillgång till tekniska system.[22]

- *Dator- och nätverksattack (Computer Network Attack – CNA)* som åsyftar *försvårande* eller *förhindrande* av motståndares *utnyttjande av information, informationssystem [*alternativt *tekniska system], datorer* eller *nätverk.* [23] Detta försvårande och förhindrade åstadkoms typiskt genom åtgärder för att *störa, avbryta, förneka* eller *slå ut* tekniska system och tjänster för motståndaren.*[24]*

Det bör anmärkas att det saknas officiella erkännande eller nekande om användning av särskilda tekniska metoder för aktiva cyberoperationer, CNE och CNA.[25] Övergripande går det ändå att konstatera att cyberoperationer omfattar både offensiv och defensiv verksamhet i cyberrymden som utgörs av militära handlingar och åtgärder för att uppnå ett särskilt mål.[26]

[22] Regeringskansliet (2004) *Informationssäkerhet i Sverige och internationellt – en översikt* SOU 20014:32, 29

[23] Försvarsmakten (2008) Försvarsmaktens Handbok Informationsoperationer: Handbok Info Ops 09 833:61968; Försvarsmakten och Försvarets Radioanstalt (2016) Överenskommelse Om gemensamma begrepp för Cyberområdet, Bilaga 1 Till FM 2016-129 50

[24] Regeringskansliet (2004) *Informationssäkerhet i Sverige och internationellt – en översikt* SOU 20014:32, sid 29

[25] Svar på skriftlig fråga 2017/18:75 Svar på fråga 2017/18:75 av Pål Jonson (M) Aktiv cyberförmåga; Mikael Holmström. (2015). *Försvarsministern: Vi ska kunna genomföra cyberattacker*. Available: https://www.dn.se/nyheter/sverige/forsvarsministern-vi-ska-kunna-genomfora-cyberattacker/. Last accessed 23/01/2018; Dag Enander. (2016). *”DET DIGITALA STRIDSFÄLTET ÄR EN REALITET”: Därför vill Försvarsmakten ha aktiv cyberförmåga.* Available: https://www.forsvarsmakten.se/siteassets/6-aktuellt/forsvarets-forum/2016/forsvarets-forum-3-2016.pdf. Last accessed 23/01/2018; Jonas Lejon. (2016). *VAD INNEBÄR EN AKTIV SVENSK CYBERFÖRMÅGA?.* Available: https://kryptera.se/cyberformaga/. Last accessed 23/01/2017.

[26] Försvarsmakten och Försvarets Radioanstalt (2016) Överenskommelse Om gemensamma begrepp för Cyberområdet, Bilaga 1 Till FM 2016-129 50; Försvarsmakten (2014) *Operativ Doktrin 2014 (OPD)*

3 Utveckling av internationell rätt för cyberförsvaret

I dagsläget har inga bindande folkrättsliga instrument antagits angående militära operationer och militär verksamhet i cyberdomänen. Avsaknaden av vägledning om tillämpad folkrätt är särskilt tydlig för aktivt cyberoperationer. Detta är främst för att normutvecklande verksamhet riktad mot militära operationer eller konflikter har hittills inte skapat bred konsensus utan snarare formats av grupper med likasinnade stater. Internationella normutvecklande initiativ har varit framgångsrikare i att bereda icke-bindande vägledningar för tillämpningen av folkrättsliga normer, exempelvis manualer och studier,[27] än att fastställa bindande rätt såsom nya traktat. Uppslutningen mot sådana vägledningar för cyberförsvar har varit särskilt svag, då de sällan antas eller åstadkommer bred konsensus. Sveriges förhållning till de relevanta delarna av dessa vägledningar är dessutom inte offentligt belagd.[28] För att tydliggöra bristen på konsensus lyfts här fram belysande exempel från fyra organisationer och sammanslutningar med särskilt uttalad strategisk relevans för svensk säkerhetspolitik och svenska samarbeten:[29]

- FN:s expertgrupp på informations- och kommunikationsteknologi (IKT) inom ramen för internationell säkerhet (FN:s Expertgrupp),
- Europeiska Unionen (EU),
- Nordatlantiska fördragsorganisationen (Nato) och
- Organisationen för säkerhet och samarbete i Europa (OSSE).

3.1 Förenta Nationerna

De Förenta Nationerna (FN) är en särskilt viktig organisation för utvecklingen av folkrätten då internationella bindande traktat och resolutioner[30] utformas genom dess system. Sådana bindande instrument har inte antagits för sakfrågor som gäller militärt cyberoperationer. Däremot har det upprättats flera utredande och dialogförande grupper samt utkommit rekommenderande instrument, däribland:

- resolutioner och rapporter från generalförsamlingens Expertgrupp inom informations- och telekommunikationsområdet (IKT) inom ramen för internationell säkerhet,[31]
- förslag på en uppförandekod för informationssäkerhet vid generalförsamlingen,[32]
- vägledningar kring säkerhet samt cyberoperationers relation till fredlig rymdverksamhet,[33]

[27] Se exempelvis UNGA. (2011). *Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General.* A/66/359 från: https://ccdcoe.org/sites/default/files/documents/UN-110912-CodeOfConduct_0.pdf. senast 21/11/2017; UNGA Committee on the Peaceful Uses of Outer Space (2018) *Guidelines for the long-term sustainability of outer space activities.* A/AC.105/C.1/L.362

[28] Se exemplevis Betänkande av NISU 2014 (SOU 2015:23), sid 193

[29] Regeringsbeslut: Inriktning för Försvarsmaktens verksamhet för åren 2016 till och med 2020 (Fö2015/00953/~FI), 8, 46-47, sid 56

[30] Artikel 25 i FN-Stadgan gör Säkerhetsrådets beslut bindande för medlemsstater.

[31] UNODA. (2017). *Developments in the field of information and telecommunications in the context of international security.* från: https://www.un.org/disarmament/topics/informationsecurity/. senast 21/11/2017

[32] UNGA. (2011). *Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General.* A/66/359 från: https://ccdcoe.org/sites/default/files/documents/UN-110912-CodeOfConduct_0.pdf. senast 21/11/2017

[33] UNGA Committee on the Peaceful Uses of Outer Space (2018) *Guidelines for the long-term sustainability of outer space activities.* A/AC.105/C.1/L.362; Jonatan Westman, Erik Zouave, Christian Valassi (2017) *Cybersäkerhet på rymdarenan.* (FOI-D--0820--SE)

- rapporter och rekommendationer från Expertgruppen om dödliga autonoma vapen vid FN:s Genevekontor,[34]
- forskningsrapporter om nedrustning och juridiska ramverk för cyberkrig och autonomteknologi från Institutet för nedrustningsforskning inom FN (UNIDIR)[35] och
- policydiskussioner vid Internet Governance Forum (IGF).[36]

Utvecklingen inom FN har inte resulterat i konkreta folkrättsliga tillämpningsåtgärder från svenskt håll men har fått svenskt uppmärksammande. Exempelvis avgränsade *Delbetänkandet SOU 2010:22* sin sammanställning vid bindande resolutioner från Säkerhetsrådet. Alltså beaktades inte FN:s arbete inom IKT och internationell säkerhet och inte heller utformningen av en uppförandekod. I samband med förslaget om en *Uppförandekod för informationssäkerhet*[37] ökade Sverige däremot sitt engagemang för expertgruppen för IKTs arbete. Ur ett svenskt perspektiv ansåg man inte att uppförandekoden kunde anses överensstämma med de mänskliga rättigheterna och särskilt yttrandefriheten.[38] Man ställer sig ändå likasinnad till principerna som uttrycks i resolutionerna för expertgruppens arbete.

3.1.1 Resolutioner och rapporter på IKT och säkerhetsområdet

Generalförsamlingens *Resolution 53/70* (1999) var den första resolutionen om IKT inom ramen för internationell säkerhet. Resolutionen syftade bland annat till att uppmuntra medlemsstaterna att bidra till en allmän bedömning av frågorna om informationssäkerhet. Därtill ville man utveckla definitioner av grundläggande begrepp för informationssäkerhet, exempelvis ”obehöriga ingrepp” eller ”missbruk” av informations- och telekommunikationssystem och informationsresurser. Slutligen ville man även bedöma lämpligheten i att utveckla internationella principer för att öka säkerheten i globala informations- och telekommunikationssystem samt bidra till att bekämpa terrorism och kriminalitet med anknytning till systemen.

Med *Resolution 56/19* grundades även en statlig expertgrupp (Governmental Group of Experts - GGE) på IKT inom ramen för internationell säkerhet under FN:s kontor för nedrustningsfrågor. Expertgruppen bidrar till årliga resolutioner och rapporter på området sedan 2009 och framåt.[39] Den utför sitt arbete i ett slutet format, med runt 15 till 25 deltagande nationer och utan medverkan från civilsamhället. Trots det begränsade formatet har expertgruppen under senare år varit utan konsensus vid flera tillfällen och då inte lyckats leverera rapporter.[40]

[34] UNOG. (2018). *Background on Lethal Autonomous Weapons Systems in the CCW.* från: https://www.unog.ch/80256EE600585943/(httpPages)/8FA3C2562A60FF81C1257CE600393DF6?OpenDocument senast 11/12/2018

[35] Se exempelvis UNIDIR. (2018). *Research project: The Weaponization of Increasingly Autonomous Technologies.* från: http://www.unidir.org/programmes/security-and-technology/the-weaponization-of-increasingly-autonomous-technologies-phase-iii. senast 12/12/2018.

[36] UNGA Resolution 70/125 *Outcome document of the high-level meeting of the General Assembly on the overall review of the implementation of the outcomes of the World Summit on the Information Society*. (A/RES/70/125); IGF. (2018). *About the IGF.* från: https://www.intgovforum.org/multilingual/tags/about. senast 09/12/2018S

[37] UNGA. (2011). *Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General.* A/66/359 från: https://ccdcoe.org/sites/default/files/documents/UN-110912-CodeOfConduct_0.pdf. senast 21/11/2017

[38] Betänkande av NISU 2014 (SOU 2015:23), sid 193

[39] UNODA. (2017). *Developments in the field of information and telecommunications in the context of international security.* från: https://www.un.org/disarmament/topics/informationsecurity/. senast 21/11/2017.

[40] UNIDIR (2017) The Weaponization of Increasingly Autonomous Technologies: Autonomous Weapon Systems and Cyber Operations. Report No. 7, sid 2

De resolutioner och rapporter som har antagits har också legat till grund för FN:s agenda inom IKT-området, inklusive normativa aspekter kring militär användning och internationell säkerhet. De har samlat kunskap om medlemsstaternas synpunkter och initiativ kring utvecklingen av internationella hot, dialoginitiativ angående normer för staters bruk av IKT, internationella förtroendeskapande åtgärder, stabilitet och riskminimering, samt en gemensam terminologi.

Kartläggningarna av medlemsstaternas synpunkter påvisar en bred samstämmighet om att folkrätten gäller och ska tillämpas av stater, även inom cyberdomänen. Till expertgruppens årsrapport 2014 bidrog svenska Försvarsberedningen med följande kommentar:

> *The Defence Commission is of the view that international law – which is applicable in peacetime (including the United Nations Charter) and during armed conflict - applies also in cyberspace. There are however particular difficulties in maintaining a clear distinction between situations of peace and armed conflict in cyberspace. Public international law that may be deemed of relevance includes sovereignty, state responsibility, human rights, self-defence and the use of force.*[41]

Försvarsberedningens kommentar är, i det stora, representativ för bidragen från många medlemsstater världen om. Medlemsstaterna uttrycker särskilt en avsaknad av vägledning om:

- *staters ansvar,* det vill säga det rättsliga ansvar som uppkommer vid folkrättsstridiga handlingar,[42]
- *de mänskliga rättigheterna* som utgörs av det lagrum inom folkrätten som reglerar individens fri- och rättigheter,[43]
- *krigets lagar* som är den del av folkrätten som reglerar förbudet mot aggressionshandlingar mellan stater, rätten till självförsvar, samt regleringen av krigföringens medel och metoder,[44]
- *suveränitet,* vilket är den folkrättsliga principen om staternas oberoende och rätt att utöva en stats funktioner utan ingripande från andra stater;[45]
- *jurisdiktion* eller stater kompetens att upprätta sina nationella rättssystem, till exempel genom att anta lagar och vidta brottsbekämpande åtgärder;[46] samt
- möjligheten att utveckla internationellt *ansvar att säkra ett fritt flöde av information, transparens* och *internationellt samarbete*.

Samstämmigheten kring behoven av vägledning bör inte tolkas som en ideologisk enighet kring folkrättens tvetydigheter eller hur problemen kan förtydligas. Expertgruppens arbete har ännu inte resulterat i fördjupade vägledningar för tillämpningen av lagrummen som berörs av medlemsstaternas bidrag. Ett hittills misslyckat försök till fördjupad samstämmighet kring inriktningen av expertgruppens normutveckling lades fram i form av en icke-bindande uppförandekod för informationssäkerhet (se nedan).[47]

---

[41] Swedish Government. (2014). *Submission by Sweden to UNGA resolution 68/243 entitled "Developments in the field of information and telecommunications in the context of international security", 12 September 2014.* från: https://unoda-web.s3-accelerate.amazonaws.com/wp-content/uploads/2014/10/Sweden.pdf. senast 21/11/2017.

[42] För mer information, se UNGA Resolution 56/83 *Responsibility of States for Internationally Wrongful Acts* (A/56/49(Vol. I)/Corr.4)

[43] Se exempelvis UN. (2019). The Foundation of International Human Rights Law. från: http://www.un.org/en/sections/universal-declaration/foundation-international-human-rights-law/index.html. senast 23/01/2019.

[44] Folkrätt i väpnad konflikt – svensk tolkning och tillämpning (SOU 2010:72)

[45] Se till exempel UN (2006) *Reports of International Arbitral Awards: Island of Palmas case (Netherlands, USA)* (VOLUME II pp. 829-871)

[46] Robert Jenning och Arthur Watts (2008). Oppenheim's International Law. Oxon: Oxford University Press.

[47] UNGA. (2011). *Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General.* A/66/359 från: https://ccdcoe.org/sites/default/files/documents/UN-110912-CodeOfConduct_0.pdf. senast 21/11/2017.

3.1.2 Uppförandekod för informationssäkerhet

Arbetet inom expertgrupp på IKT motiverade Kina, Ryssland, Tadjikistan och Uzbekistan att utforma en *Uppförandekod för informationssäkerhet* 2011.[48] En uppdaterad version av uppförandekoden som tog hänsyn till kommentarer från andra medlemsstater utkom 2015.[49] Syftet med uppförandekoden är att identifiera staters rättigheter och ansvar i informationsdomänen, främja konstruktiva och ansvarsfulla beteenden, samt stärka internationellt samarbete mot gemensamma hot och utmaningar. Koden skissar elva icke-bindande förslag för statsansvar inom informationssäkerhet, varav åtta skulle ha särskild betydelse för militära operationer och försvar:

- tillämpa FN-stadgan och universellt erkända normer som styr internationella förbindelser;
- avstå att utföra fientliga aktiviteter och aggressionshandlingar via IKT, inklusive nätverk;
- samarbeta för att motverka terrorism, extremism och separatism;
- underlåta att ingripa mot leverantörskedjan för IKT-produkter och tjänster på ett sätt som undergräver andra staters rättigheter;
- bekräfta alla staters rättigheter och ansvar att skydda sitt informationsutrymme och kritisk informationsinfrastruktur från hot, störningar, angrepp och sabotage, i enlighet med gällande lagar;
- respektera rättigheter och friheter i informationsdomänen till fullo;
- stärka bilaterala, regionala och internationella samarbeten, främja FN:s roll i att utforma internationella normer, fredliga lösningar av internationella tvister och förbättringar av det internationella samarbetet på informationssäkerhetsområdet; samt
- lösa eventuella tvister genom fredliga medel och avstå från hot eller användning av våld.

Uppförandekoden har inte antagits officiellt av generalförsamlingen eller någon annan del av FN. Det råder fortsatta meningsskiljaktigheter ifall koden, om den antogs, skulle kunna leda till en formalisering av regler och bli en vägledande tolkning av folkrätten. Därtill har det uppstått frågor kring vilka typer av fora och aktörer som är relevanta för en fortsatt utveckling av normerna – mellanstatliga eller flerpartsarrangemang – samt hur staters suveränitet ska balanseras mot individers fri- och rättigheter.[50] Roigas påpekar också på två mycket viktiga korrigeringar mellan upplagorna i uppförandekoden.[51] Först och främst ströks det icke vedertagna och tvetydiga begreppet *informationsvapen* ur avsnittet om staters skyldigheter att avstå aggressionshandlingar i andra upplagan. Sedan tillades en skyldighet för stater med en dominans på IKT området att inte utnyttja sin förmåga mot andra staters politik eller ekonomi. Således framstår det som att uppförandekoden delvis mist sin anknytning till militär verksamhet.

[48] UNGA. (2011). *Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General.* A/66/359 från: https://ccdcoe.org/sites/default/files/documents/UN-110912-CodeOfConduct_0.pdf. senast 21/11/2017.

[49] UNGA. (2015). *Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General.* från: https://ccdcoe.org/sites/default/files/documents/UN-150113-CodeOfConduct.pdf. senast 21/11/2017.

[50] Henry Rõigas. (2015). *An Updated Draft of the Code of Conduct Distributed in the United Nations – What's New?* från: https://ccdcoe.org/updated-draft-code-conduct-distributed-united-nations-whats-new.html. senast 21/11/2017.

[51] Henry Rõigas. (2015). *An Updated Draft of the Code of Conduct Distributed in the United Nations – What's New?* från: https://ccdcoe.org/updated-draft-code-conduct-distributed-united-nations-whats-new.html. senast 21/11/2017.

3.1.3 Vägledningar om cyber- och rymdverksamhet

I FOI-rapporten ”Cybersäkerhet på rymdarenan” uppmärksammade Westman, Zouave och Valassi de folkrättsliga aspekterna av mötespunkterna mellan cyber- och rymdarenorna.[52] Där uppmärksammades att FN:s Kommitté för fredligt nyttjande av yttre rymden (COPUOS), särskilt dess Underkommitté för vetenskapliga och tekniska frågor, används som internationellt forum för normutveckling kring cybersäkerhetsaspekter av rymdverksamhet.[53] COPUOS arbete har även vidrört frågor med anknytning till krigets lagar och aktiv cyber, särskilt ett eventuellt ansvar att respektera (cyber)säkerheten i andra länders rymdinfrastruktur samt avstå från att störa infrastrukturen.[54] Störningarna som diskuteras inom COPUS omfattar störningar mot hårdvara, mjukvara, samt informationsflöden vilket gör att dessa diskussioner även berör eventuella cyberoperationer som riktar sig mot rymdinfrastruktur. COPUOS är (likt expertgruppen inom IKT och säkerhetspolitik) en GGE inom FN-systemet med statliga expertrepresentanter, som bland annat utforskar frågor om reglering av fredlig rymdverksamhet.[55] Underkommittén förhandlar om ett antal vägledningar med relevans för cybersäkerhet och cyberoperationer med potential att påverka fredlig rymdverksamhet, de så kallade *Guidelines for the long-term sustainability of outer space activties*:[56]

Riktlinje 1 - Anta, revidera och vid behov ändra nationella regelverk för yttre rymdverksamhet, inklusive nationella regler om och ansvar för säkerhet och tillförlitlighet.[57]

Riktlinje 9 - Genomför policy som syftar till att förhindra störningar av driften av objekt i yttre rymden genom obehörig åtkomst till deras inbyggda hårdvara och programvara, inklusive nationell policy för att avstå indirekt eller direkt deltagande i sådana störningar. [58]

Riktlinjerna 18 och 19 - Säkerställ säkerheten för den markbundna infrastrukturen, inklusive deras informationsflöden, som stöder driften av orbitalsystem och respektera säkerheten för utländsk rymdrelaterad mark- och informationsinfrastruktur, inklusive genom att på internationell och nationell nivå genomföra policy för att förebygga, identifiera, undersöka och avskräcka skadlig användning av informations- och kommunikationsteknologi och annan verksamhet med negativ påverkan på infrastrukturen.[59]

Medan Riktlinje 1 redan är antagen bör det uppmärksammas att om övriga riktlinjer antas skulle detta kunna innebära en icke-bindande internationell föreskrift som förtydligar ett påbud mot vissa typer av aktiva och offensiva cyberoperationer riktade mot fredlig rymdverksamhet.

[52] Jonatan Westman, Erik Zouave, Christian Valassi (2017) *Cybersäkerhet på rymdarenan*. (FOI-D--0820--SE)
[53] UNOOSA. (2017). *Committee on the Peaceful Uses of Outer Space and its Subcommittees.* från: http://www.unoosa.org/oosa/en/ourwork/copuos/comm-subcomms.html. senast 17/10/2017.
[54] UNGA Committee on the Peaceful Uses of Outer Space (2018) *Guidelines for the long-term sustainability of outer space activities.* A/AC.105/C.1/L.362
[55] Jonatan Westman, Erik Zouave, Christian Valassi (2017) *Cybersäkerhet på rymdarenan*. (FOI-D--0820--SE)
[56] UNGA Committee on the Peaceful Uses of Outer Space (2018) *Guidelines for the long-term sustainability of outer space activities.* A/AC.105/C.1/L.362
[57] UNGA Committee on the Peaceful Uses of Outer Space (2018) *Guidelines for the long-term sustainability of outer space activities.* A/AC.105/C.1/L.362; Jonatan Westman, Erik Zouave, Christian Valassi (2017) *Cybersäkerhet på rymdarenan.* (FOI-D--0820--SE)
[58] UNGA Committee on the Peaceful Uses of Outer Space (2018) *Guidelines for the long-term sustainability of outer space activities.* A/AC.105/C.1/L.362; Jonatan Westman, Erik Zouave, Christian Valassi (2017) *Cybersäkerhet på rymdarenan.* (FOI-D--0820--SE)
[59] UNGA Committee on the Peaceful Uses of Outer Space (2018) *Guidelines for the long-term sustainability of outer space activities.* A/AC.105/C.1/L.362 18.1; Jonatan Westman, Erik Zouave, Christian Valassi (2017) *Cybersäkerhet på rymdarenan.* (FOI-D--0820--SE)

3.1.4 Rapporter, rekommendationer och forskning för autonoma vapensystem och artificiell intelligens i cyberoperationer

Dödliga autonoma vapen anses i generell bemärkelse vara system med teknisk styrning snarare än mänsklig; till exempel genom användning av artificiell intelligens.[60] Vissa experter anser att det vore kontraproduktivt att försöka enas om en definition med hänseende till teknologins och i synnerhet den snabba utvecklingen av artificiell intelligens.[61] Internationella Rödakorskommittén föreslår däremot att dessa vapen bör betraktas som vapensystem som, oavsett om de är verksamma inom luften, på land eller till sjöss, med kritiska funktioner (som att upptäcka, identifiera, spåra, välja och anfalla mål, till exempel för att neutralisera, skada eller förstöra målet) som realiseras utan mänsklig intervention.[62] Vanliga exempel är fysiska system som drönare, robotar, missilsystem, eller farkoster. Den internationella normutvecklande verksamheten kring dessa vapensystem kan således verka marginellt relevant för cyberoperationer som typiskt sett är icke-fysiska (inte är fysiskt verksamma till land, luft eller sjöss) och icke-dödliga. En nyligen påbörjad utredning påvisar emellertid tekniska och normativa likheter mellan fysiska autonoma system som använder artificiell intelligens och cyberoperationer som använder artificiell intelligens.[63] Troligtvis kommer alltså den normativa utvecklingen kring artificiell intelligens i dödliga autonoma vapen att få ökad betydelse för cyberoperationer. Detta märks inte minst i arbetet som bedrivs inom Institutet för nedrustningsforskning inom FN (UNIDIR) som bedriver forskning parallellt med expertgruppers arbete.

I och med att flera stater, inklusive Sverige, diskuterat ett förbud mot dödliga autonoma robotar,[64] upprättades en GGE bildades under FN:s Genèvekontor.[65] Expertgruppen har varit verksam sedan 2013 och har haft ett öppnare och större format än expertgruppen på IKT och säkerhetspolitik.[66]

Expertgruppen på dödliga autonoma vapen har skissat ut flera normativa frågor. Det råder däremot ingen gemensam syn inom Expertgruppen om dödliga autonoma vapen kan verka i enlighet med folkrättsliga regler. Den så kallade Martensklausen från IV:e Haagkonventionen (1907), som fastställer att humanitära krav ska beaktas i krig även vid avsaknad av folkrättsliga regler,[67] framstår som relevant men särskilt svårtillämpad.

[60] Group of Governmental Experts of the High Contracting Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects (2017) *Report of the 2017 Group of Governmental Experts on Lethal Autonomous Weapons Systems (LAWS).* (CCW/GGE.1/2017/3); se även Guillaume Fournier (2016) Towards a definition of lethal autonomous weapons systems. (CCW/GGE.1/2017/WP.3, inlämnad av Belgien)

[61] Group of Governmental Experts of the High Contracting Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects (2017) *Report of the 2017 Group of Governmental Experts on Lethal Autonomous Weapons Systems (LAWS).* (CCW/GGE.1/2017/3)

[62] ICRC (2015) International humanitarian law and the challenges of contemporary armed conflicts Report Document prepared by the International Committee of the Red Cross. (32IC/15/11), 44-45

[63] UNIDIR (2017) The Weaponization of Increasingly Autonomous Technologies: Autonomous Weapon Systems and Cyber Operations. Report No. 7

[64] Campaign to Stop Killer Robots. (2018). *Consensus: killer robots must be addressed.* från: https://www.stopkillerrobots.org/2013/05/nations-to-debate-killer-robots-at-un/. senast 10/12/2018.

[65] Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons which may be deemed to be Excessively Injurious or to have Indiscriminate Effects (adopted10 October 1980, eneterd into force 2 December 1983) UNTS 1342, p. 137

[66] UNOG. (2018). *Background on Lethal Autonomous Weapons Systems in the CCW.* från: https://www.unog.ch/80256EE600585943/(httpPages)/8FA3C2562A60FF81C1257CE600393DF6?OpenDocument. senast 11/12/2018; UNOG. (2018). *2018 Group of Governmental Experts on Lethal Autonomous Weapons Systems (LAWS).* från: https://www.unog.ch/80256EE600585943/(httpPages)/7C335E71DFCB29D1C1258243003E8724?OpenDocument. senast 11/12/2018; UNIDIR (2017) The Weaponization of Increasingly Autonomous Technologies: Autonomous Weapon Systems and Cyber Operations. Report No. 7, sid 2.

[67] För ytterligare förklaring av Martensklausulen, se till exempel Rupert Ticehurst. (1997). *The Martens Clause and the Laws of Armed Conflict.* från: https://www.icrc.org/en/doc/resources/documents/article/other/57jnhy.htm. senast 01/04/2019.

Dessutom anses *distinktion* (att skilja mellan militära och civila mål),[68] *proportionalitet* (att risken för civila intressen står i proportion till betydelsen av det militära målet)[69] och *försiktighet* (att vidta åtgärder för att undvika skada mot civila intressen)[70] vara de mest relevant folkrättsliga principerna för dödliga autonoma vapen. För det fjärde, utreds ett antal nya principer för dödliga autonoma vapen avseende mänsklig tillsyn, inklusive mänsklig kontroll och mänskligt omdöme i det annars automatiserade förfarandet för att döda. Slutligen, även om bedömningar av vapensystem enligt Artikel 36 inte utgör uttömmande folkrättsliga analyser av dödliga autonoma vapen anses bedömningarna vara relevanta för teknologin.[71]

Institutet för nedrustningsforskning inom FN (UNIDIR), som förser FN-systemet med oberoende forskning på nedrustningsfrågor, har bedrivit tematisk forskning på relevanta teknologiska aspekter av internationell säkerhet och folkrätt. Till exempel utforskas de rättsliga aspekterna av cyberkrig,[72] inklusive dator- och nätverksoperationer,[73] samt kopplingarna mellan autonomteknik och cyberoperationer. [74] Till exempel behandlar Melzers ”Cyberwarfare and International Law” cyber och våldsanvändning mellan stater (*jus ad bellum*), neutralitet vid konflikt, samt krigets lagar (*jus in bello*) för att skildra folkrättsliga begränsningar, kontroverser, och konsekvenser av cyberkrig.[75] UNIDIR har även skrivit tematiska observationsrapporter[76] parallellt med expertgruppen[77] om dödsliga autonoma vapens verksamhet, vilka sammanställs i nedanstående tabell:

Tabell 1 Rapporter från UNIDIR om militär autonom teknik

Rapportering från UNIDIR	
Rapportnummer/år	**Ämne**
Report no. 1 (2014)	*Framing Discussions on the Weaponization of Increasingly Autonomous Technologies*
Report no. 2 (2014)	*The Weaponization of Increasingly Autonomous Technologies: Considering how Meaningful Human Control might move the discussion forward*

[68] Se exempelvis Protocol additional to the Geneva Conventions of12 August 1949, and relating to the protection of victims of international armed conflicts (Protocol I) (adopted on 8 June 1977) UNTS 17512, Artikel 48

[69] Se exempelvis Protocol additional to the Geneva Conventions of12 August 1949, and relating to the protection of victims of international armed conflicts (Protocol I) (adopted on 8 June 1977) UNTS 17512, Artikel 51(5)(b)

[70] Se exempelvis Protocol additional to the Geneva Conventions of12 August 1949, and relating to the protection of victims of international armed conflicts (Protocol I) (adopted on 8 June 1977) Artikel57(1)

[71] UNOG (2017) *Report of the 2017 Group of Governmental Experts on Lethal Autonomous Weapons Systems (LAWS).* CCW/GGE.1/2017/3

[72] UNIDIR. (2019). *Cyber.* från: http://www.unidir.org/est-cyber. senast 07/01/2019.

[73] Nils Melzer. (2011). *Cyberwarfare and International Law.* från: http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf. senast 07/01/2019.

[74] UNIDIR (2017) The Weaponization of Increasingly Autonomous Technologies: Autonomous Weapon Systems and Cyber Operations. Report No. 7

[75] Nils Melzer. (2011). *Cyberwarfare and International Law.* Available: http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf. Last accessed 07/01/2019.

[76] UNIDIR. (2018). *Research project: The Weaponization of Increasingly Autonomous Technologies.* Available: http://www.unidir.org/programmes/security-and-technology/the-weaponization-of-increasingly-autonomous-technologies-phase-iii. Last accessed 12/12/2018.

[77] Se även Expertgruppens sammanställning av vetenskapliga artiklar och rapporter på ämnet UNOG. (2018). *Lethal autonomous weapons systems (LAWS): Articles and papers on lethal autonomous weapons systems.* Available: https://www.unog.ch/80256EDD006B8954/(httpAssets)/4C452E8607E0FBC3C12581D400341DE1/$file/CCW+Website_Articles_LAWS_Archive.pdf. Last accessed 04/01/2019.

Report no. 3 (2015).	*The Weaponization of Increasingly Autonomous Technologies: Considering Ethics and Social Values*
Report no. 4 (2015)	*The Weaponization of Increasingly Autonomous Technologies in the Maritime Environment: Testing the Waters*
Report no. 5 (2016)	*Safety, Unintentional Risk and Accidents in the Weaponization of Increasingly Autonomous Technologies*
Report no. 6 (2017)	*The Weaponization of Increasingly Autonomous Technologies: Concerns, Characteristics and Definitional Approaches*
Report no. 7 (2017)	*The Weaponization of Increasingly Autonomous Technologies: Autonomous Weapon Systems and Cyber Operations*
Report no. 8 (2018)	*The Weaponization of Increasingly Autonomous Technologies: Artificial Intelligence*
Report no. 9 (2018)	*Algorithmic Bias and the Weaponization of Increasingly Autonomous Technologies*

UNIDIR argumenterar för att utbyten mellan expertgrupperna för IKT och säkerhetspolitik samt dödliga autonoma vapensystem och forskningsområdena behövs.[78] Det mest konkreta inslaget kring cyberoperationer inom expertgruppen för dödliga autonoma vapens rapportering är att påpeka att dödliga autonoma vapen kan ha sårbarheter som kan exploateras för cyberangrepp.[79] Ytterst är inte *vapensystem*, som operativ del av en definition exkluderande för potentiella cyber- eller informationsvapen.[80] Även en begreppsapparat som fokuserar på land-, luft- och sjödomänerna utan att likställa den militära betydelsen av cyber- eller informationsdomänen med dessa, blir det inte tydligt att cyberoperationer inte kan omfattas av dessa domäner när de möjliggörs av deras infrastruktur. Snarare är det ett formativt exemplifierande av begreppsapparaten med fysiska system som skulle utesluta autonoma informationsvapen ur diskussionerna. Det är också anmärkningsvärt att diskussionerna tar avstamp i operationer med *dödligt* utfall. Trots att cyberoperationer hittills inte tenderat att ha utfall som är direkt vådliga för mänsklig hälsa och liv så är det en återkommande farhåga från säkerhetsexperter, särskilt i diskussionerna kring cyberangrepp mot industriella kontrollsystem.[81] Det andra centrala föremålet för diskussionerna, det vill säga *autonomi*, särskilt artificiellt intelligent automatisering, kan möjligtvis få bredare implikationer bortom dödligt våld och i synnerhet för cyberoperationer. Expertgruppen uppmärksammar även denna potentiella militära

[78] UNIDIR (2017) The Weaponization of Increasingly Autonomous Technologies: Autonomous Weapon Systems and Cyber Operations. Report No. 7

[79] UNOG (2014) *Report of the 2014 informal Meeting of Experts on Lethal Autonomous Weapons Systems (LAWS).* CCW/MSP/2014/3, 7; UNOG (2015) *Report of the 2015 Informal Meeting of Experts on Lethal Autonomous Weapons Systems (LAWS).* CCW/MSP/2015/3, sid 7

[80] Se till exempel Gary D. Brown and Andrew O. Metcalf. (2014). Easier Said than Done: Legal Reviews of Cyber Weapons. *Journal of National Security Law and Policy*. 7 (1), 115-138; Colonel David Wallace (2018) Cyber Weapon Reviews under International Humanitarian Law: A Critical Analysis. (Tallinn Paper no 11)

[81] Nicole Perlroth and Clifford Krauss. (2018). *A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try.* Available: https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html. Last accessed 12/12/2018; Andrew Tsonchev. (2018). *The implications of TRITON for the future of ICS security.* Available: https://www.darktrace.com/en/blog/the-implications-of-triton-for-the-future-of-ics-security/. Last accessed 12/12/2018; Riskinsight. (2018). *INDUSTRIAL CONTROL SYSTEM CYBERSECURITY NEWS #1 – WHAT TO REMEMBER FROM 2017?.* Available: https://www.riskinsight-wavestone.com/en/2018/03/ics-news-1-en/. Last accessed 12/12/2018; Thomas Nuth. (2018). *Cybersecurity concerns intensify for critical infrastructure worldwide: A combination of evolving IoT and lack of security spending in ICS space can be lethal.* Available: https://www.securityinfowatch.com/cybersecurity/information-security/article/12399943/cybersecurity-concerns-intensify-for-critical-infrastructure-worldwide. Last accessed 12/12/2018; Steven P. Lee. (2014). The Ethics of Cyberattack. *The Ethics of Information Warfare*. 14 (1), sid 105-122.

användning av artificiell intelligens.[82] Flera aspekter av skadlig kod automatiseras redan i dagsläget.[83] Forskning inom artificiell intelligens bedrivs även i syfte att automatisera cyber- och informationsoperationer.[84] Därtill är de grundläggande folkrättsliga principerna *distinktion*, *proportionalitet* och *försiktighet* samt artikel 36-bedömningar är inte bara avgränsade till dödligt våld utan även till mer generella avvägningar såsom frågor kring distinktion mellan militära och civila mål, samt skydd av egendom,. Således bör relevanta nya lärdomar om folkrättsliga aspekter av automatisering, till exempel principer om mänsklig kontroll, även utredas för icke-dödliga cyberoperationer.[85]

3.1.5 Policydiskussioner vid Internet Governance Forum (IGF)

Internet Governance Forum (IGF) är en intressentplattform inom FN-systemet som faciliterar diskussioner om internationell internetpolicy.[86] Enligt *Tunis Agenda for the Information Society*[87] (från världstoppmötet om informationssamhället) som begärde öppnandet av IGF, innefattar IGF:s mandat att diskutera offentlig policy och framväxande problem för internetstyrning. Under 2018 har IGF, tillsammans med Global Commission on the Stability of Cyberspace (GSCS) diskuterat internationell cybersäkerhet, normer och förtroendeskapande åtgärder.[88] GSCS är en internationell kommission med 25 kommissionärer, som likt IGF anordnar möten för olika intressenter med syfte att främja säkerhet och stabilitet i cyberrymden.[89] Diskussionerna vid IGF fokuserade på ett antal föreslagna normer med relevans för militära cyberoperationer:

- skyddet av ”Internets offentliga kärna”,
- skydd av infrastruktur vid val,
- norm för statliga och icke-statliga aktörer att undvika att modifiera produkter före deras frisläppande,
- norm mot övertagande av IKT-enheter till botnät,
- norm för stater att skapa en sårbarhetbedömningsprocess,
- norm för att minska och åtgärdabetydande sårbarheter,
- norm för grundläggande cyberhygien som grundförsvar samt en

[82] UNOG (2015) *Report of the 2015 Informal Meeting of Experts on Lethal Autonomous Weapons Systems (LAWS).* CCW/MSP/2015/3, 7; UNIDIR (2017) The Weaponization of Increasingly Autonomous Technologies: Autonomous Weapon Systems and Cyber Operations. Report No. 7, sid 1.

[83] Se till exempel Curtis Franklin Jr. (2018). *DanaBot Malware Adds Spam to its Menu.* Available: https://www.darkreading.com/threat-intelligence/danabot-malware-adds-spam-to-its-menu/d/d-id/1333454. Last accessed 12/12/2018; Kelly Sheridan. (2018). *Anti-Botnet Guide Aims to Tackle Automated Threats.* Available: https://www.darkreading.com/threat-intelligence/anti-botnet-guide-aims-to-tackle-automated-threats/d/d-id/1333371?_mc=rss_x_drr_edt_aud_dr_x_x-rss-simple. Last accessed 12/12/2018.

[84] GAO (2018) *Long-Range Emerging Threats Facing the United States As Identified by Federal Agencies.* GAO-19-204SP; Curtis Franklin Jr. (2018). *AI Poised to Drive New Wave of Exploits.* Available: https://www.darkreading.com/application-security/ai-poised-to-drive-new-wave-of-exploits/d/d-id/1333289. Last accessed 12/12/2018; Dustin Fraze. (2016). *Cyber Grand Challenge (CGC).* Available: https://www.darpa.mil/program/cyber-grand-challenge. Last accessed 12/12/2016.

[85] UNIDIR (2017) The Weaponization of Increasingly Autonomous Technologies: Autonomous Weapon Systems and Cyber Operations. Report No. 7, sid 1-3.

[86] UNGA Resolution 70/125 *Outcome document of the high-level meeting of the General Assembly on the overall review of the implementation of the outcomes of the World Summit on the Information Society*. (A/RES/70/125); IGF. (2018). *About the IGF.* Available: https://www.intgovforum.org/multilingual/tags/about. Last accessed 09/12/2018.

[87] World Summit of the Information Society (2005) *Tunis Agenda for the Information Society*. (WSIS-05/TUNIS/DOC/6(Rev. 1)-E, 18 November 2005)

[88] IGF. (2018). *IGF 2018 Global Commission on the Stability of Cyberspace.* Available: http://www.intgovforum.org/multilingual/content/igf-2018-global-commission-on-the-stability-of-cyberspace. Last accessed 09/12/2918.

[89] GCSC. (2018). *THE COMMISSION.* Available: https://cyberstability.org/about/. Last accessed 09/12/2018.

- norm mot offensiva cyberoperationer av icke-statliga aktörer.[90]

Dessa förslag har utvecklats av GCSC inom ramen för deras *Singapore Norm Package* (paketet) som ytterligare förtydligar innehållet av normerna.[91] Flera av förslagen grundar sig på GCSC-intressenternas gemensamma förståelse av folkrätten. Till exempel anser man att det vore en folkrättsstridig handling om en stat gav uppdrag åt icke-statliga aktörer att genomföra offensiva cyberoperationer. Paketet hävdar alltså att endast stater bör tillåtas utföra sådana operationer under strikta folkrättsliga förutsättningar.[92] De flesta av de föreslagna normerna är emellertid nytänkande och hämtar inte stöd från folkrättsliga normer. Till exempel föreslår paketet att stater inte avsiktligt bör bygga in sårbarheter i teknologi som är kritisk för internets fungerande genom leverantörskedjan.[93] Paketet hänvisar dessutom till det amerikanska exemplet för en sårbarhetbedömningsprocess där sårbarheter som skulle kunna användas av underrättelse- och försvarsmyndigheterna i cyberoperationer bedöms under vissa kriterier för att avgöra om de ska komma till kännedom för aktörer som kan åtgärda dem med säkerhetsuppdateringar.[94] Dessa normer är inte utvecklade på internationell nivå och har hittills inte figurerat som implementeringsåtgärder för folkrätten.

3.2 Europeiska unionen

Europeiska unionen (EU) har sedan 1990-talet fört en gemensam policy för ökad cybersäkerhet. Detta framgår till exempel av tidig lagstiftning (samt rigorös uppdatering) av dataskyddslagar,[95] gemensam kriminalisering av it-relaterad brottslighet,[96] gemensam exportkontroll för vissa säkerhetsrelaterade tekniska produkter,[97] gemensamma bestämmelser för informations- och nätverkssäkerhet i samhällsviktiga tjänster[98] och senast ett gemensamt system för standardisering, ackreditering och certifiering för cybersäkerhet i IKT.[99] År 2013 antog Europaparlamentet och Europeiska rådet unionens första gemensamma cybersäkerhetsstrategi; *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.*[100] Strategin innehöll ett antal strategiska prioriteringar

[90] IGF. (2018). *IGF 2018 Global Commission on the Stability of Cyberspace.* Available: http://www.intgovforum.org/multilingual/content/igf-2018-global-commission-on-the-stability-of-cyberspace. Last accessed 09/12/2918.
[91] GCSC (2018) *Norm Package* (Singapore, November 2018)
[92] GCSC (2018) *Norm Package* (Singapore, November 2018), sid 9
[93] GCSC (2018) *Norm Package* (Singapore, November 2018), sid 9
[94] GCSC (2018) *Norm Package* (Singapore, November 2018), sid 13
[95] Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter; Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) (Text av betydelse för EES) OJ L 119, 4.5.2016, sid. 1–88
[96] Europaparlamentets och rådets direktiv 2013/40/EU av den 12 augusti 2013 om angrepp mot informationssystem och om ersättande av rådets rambeslut 2005/222/RIF OJ L 218, 14.8.2013, sid 8–14S
[97] Rådets förordning (EG) nr 428/2009 av den 5 maj 2009 om upprättande av en gemenskapsordning för kontroll av export, överföring, förmedling och transitering av produkter med dubbla användningsområden (omarbetning); Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL setting up a Union regime for the control of exports, transfer, brokering, technical assistance and transit of dual-use items (recast) COM/2016/0616 final - 2016/0295 (COD)
[98] Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen
EUT L 194, 19.7.2016, sid 1–30
[99] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act")
COM/2017/0477 final - 2017/0225 (COD)
[100] Europeiska Kommissionen (2013) *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace* (JOIN(2013) 1 final , 7.2.2013)

för unionen, inklusive utvecklingen av en europeisk cyberförsvarspolicy samt en gemensam internationell cyberpolicy som är enhetlig med unionen värderingar.

Traditionellt sett har EU haft ett relativt försiktigt normativt avtryck på medlemsstaternas försvars- och säkerhetspolitik i jämförelse med andra policyområden. Försvars- och säkerhetspolitik var inte del av den ursprungliga europeiska gemenskapen och nationell säkerhet och territoriell integritet är fortsatt medlemsstaternas ansvar i unionen.[101] Med *Maastrichtfördraget* (1992), *Saint-Malo-deklarationen* (1998) och senare *Lissabonfördraget* (2019) fick unionen ett utökat mandat för en Gemensam utrikes- och säkerhetspolitik (GUSP) samt Gemensam säkerhets- och försvarspolitik (GSFP). Således antogs ett ramverk för europeisk cyberförsvarspolicy (*EU Cyber Defense Policy Framework*)[102] 2014 under GUSP-GSFP för att tillämpa unionens cybersäkerhetsstrategi, [103] vilken sedan uppdaterades 2018.[104] Ramverkens prioriteringar innefattar att:

- utveckla medlemsstaternas GSFP-förmåga,
- stärka skyddet för kommunikationsnät inom GSFP,
- civil-militärt och privat-offentligt samarbete,
- forskning och utveckling,
- förbättra möjligheterna att träna, utbilda och öva, samt
- utöka samarbetet med relevanta internationella parter.[105]

Den europeiska policyn syftar till både samstämmighet med europeiska värderingar som härstammar ur folkrätten samt till utvecklingen av folkrättslig tillämpning. Policy och lag som utvecklas inom unionen ska också vara samstämmiga med unionens grundläggande värderingar, även när de gäller cyberrymden:

> *For cyberspace to remain open and free, the same norms, principles and values that the EU upholds offline, should also apply online. Fundamental rights, democracy and the rule of law need to be protected in cyberspace*.[106]

Detta är värt att nämnas då unionens stöd till medlemsstaternas cyberförmåga även inbegriper stöd till nationell doktrinutveckling.[107] 2018 års ramverk påpekar även att cyberförsvarslagstiftningen bland medlemsstaterna är diversifierad och i behov av en gemensam syn på cyberförsvar.[108] Således ska Europeiska försvarsbyrån (*European Defence Agency – EDA*) studera medlemsstaternas behov och lagstiftning för cyberförsvaret för att utveckla bästa praxis.[109] Utöver detta ska Europeiska kommissionen främja normutvecklande och förtroendeskapande verksamhet som syftar till implementeringen av gällande folkrätt, även mot samarbetspartners som Europarådet, OCECD, FN, OSSE, NATO, AU, ASEAN, OAS och USA.[110] Cybersäkerhetsstrategin påkallar ett brett ansvar

[101] Artikel 3a, Lissabonfördraget (C 306/1, 17.12.200)
[102] Europeiska Rådet (2014) *EU Cyber Defense Policy Framework*. (15585/14, 18 November 2014)
[103] Europeiska Rådet (2014) *EU Cyber Defense Policy Framework*. (15585/14, 18 November 2014), sid 2
[104] Europeiska Rådet (2018) *EU Cyber Defense Policy Framework (2018 update).* (14413/18, 19 November 2018)
[105] Europeiska Rådet (2014) *EU Cyber Defense Policy Framework*. (15585/14, 18 November 2014); Europeiska Rådet (2018) *EU Cyber Defense Policy Framework (2018 update).* (14413/18, 19 November 2018)
[106] Europeiska Kommissionen (2013) *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace* (JOIN(2013) 1 final , 7.2.2013, 2; Se även Eurpoeiska Rådet (2017) *Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox"*. (9916/17, 7 June 2017)
[107] Europeiska Rådet (2018) *EU Cyber Defense Policy Framework (2018 update).* (14413/18, 19 November 2018), sid 9
[108] Europeiska Rådet (2018) *EU Cyber Defense Policy Framework (2018 update).* (14413/18, 19 November 2018), sid 10
[109] Europeiska Rådet (2018) *EU Cyber Defense Policy Framework (2018 update).* (14413/18, 19 November 2018), sid 11
[110] Europeiska Kommissionen (2013) *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace* (JOIN(2013) 1 final , 7.2.2013, 15; Se även Europeiska Rådet (2018) *EU Cyber Defense Policy Framework (2018 update).* (14413/18, 19 November 2018), sid 8

för alla internets användare, från individ till stat, att följa gällande lagar[111] och att unionens perspektiv är att nya traktat och folkrättsliga instrument inte behövs för cyberrymden. Unionens människorättsliga fokus ligger på implementeringen av *FN:s konvention om medborgerliga och politiska rättigheter*, den *Europeiska konventionen om skydd för de mänskliga rättigheterna*, och den *Europeiska unionens stadga om de grundläggande rättigheterna.* Dessutom gäller både krigets lagar och de mänskliga rättigheterna om en konflikt utspelar sig i cyberrymden.[112]

Det uppdaterade cyberförvarsramverket uppmärksammar betydelsen av FN-stadgan (i sin helhet) i cyberrymden[113] och framhåller staters folkrättsliga ansvar för sina handlingar i cyberrymden. [114] Den gemensamma utvecklingen av förmågorna och skyddet av GSFP-nät innebär även att antagonister som bedriver illvillig cyberverksamhet måste hållas ansvariga.[115] Viljan att hålla antagonistiska aktörer, inklusive stater, ansvariga för sina handlingar ledde till att Europeiska rådet började utforska en så kallad ”cyberdiplomatisk verktygslåda” 2017.[116] Verktygslådan uttrycker unionens stöd för slutsatserna om statsansvar från FN:s GGE på IKT och säkerhetspolitik. Ansvaret innebär alltså att stater bör både avstå och förebygga illvillig cyberverksamhet på internetinfrastrukturen; det vill säga att stater inte medvetet bör upplåta sitt territorium så att det kan användas för sådan verksamhet.[117] Den illvilliga cyberverksamhetens hänförbarhet (även kallad ”attribution” inom cyberrelaterade studier), som generellt syftar till att identifiera vem eller vilka som är ansvariga för handlingen, är fortsatt medlemsstaternas ansvar. Hänförbarhet ska spåras på medlemsstaternas eget initiativ, med stöd av flera typer av underrättelsemetodik (”all-source intelligence”) och enligt folkrättspraxis för hänförbarhet av folkrättsstridiga handlingar. Ett gemensamt europeiskt svar på illvillig cyberverksamhet är däremot inte beroende av hänförbarhet.

Ett aktivt agerande framstår inte som en tydlig del av europeisk policy. Den cyberdiplomatiska verktygslådan klargör ett antal avgränsningar för gensvar på illvillig cyberverksamhet, till exempel att de bygger på gemensamma åtgärder inom GUSP samt att de är proportionerliga jämtemot ”omfattning, varaktighet, intensitet, komplexitet, sofistikation och inverkan av cyberverksamheten”.[118] Cyberdiplomatiska verktygslådan framhåller att internationella tvister i cyberrymden ska lösas med fredliga medel.[119] Dessutom antyder de flesta av de operativa skyddsåtgärderna inom ramverket ett defensivt (snarare än offensivt) ställningstagande; exempelvis åtgärder för att säkerställa motståndskraft, situationsmedvetenhet, informationsdelning, samt förbygga, upptäcka och hantera incidenter. Därtill förespråkar ramverket gemensamma it-säkerhetsvägledningar för GSFP-operationer med mera.[120]

---

[111] Se även Europeiska Rådet (2017) *Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox").* (9916/17, 7 June 2017), sid 4

[112] Europeiska Kommissionen (2013) *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace* (JOIN(2013) 1 final , 7.2.2013, sid 15-16

[113] Europeiska Rådet (2018) *EU Cyber Defense Policy Framework (2018 update).* (14413/18, 19 November 2018), sid 8

[114] Europeiska Rådet (2018) *EU Cyber Defense Policy Framework (2018 update).* (14413/18, 19 November 2018), sid 8

[115] Europeiska Rådet (2018) *EU Cyber Defense Policy Framework (2018 update).* (14413/18, 19 November 2018), sid 9

[116] Europeiska Rådet (2017) *Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox").* (9916/17, 7 June 2017), sid 4

[117] Europeiska Rådet (2017) *Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox").* (9916/17, 7 June 2017), sid 4

[118] Europeiska Rådet (2017) *Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox").* (9916/17, 7 June 2017), sid 5

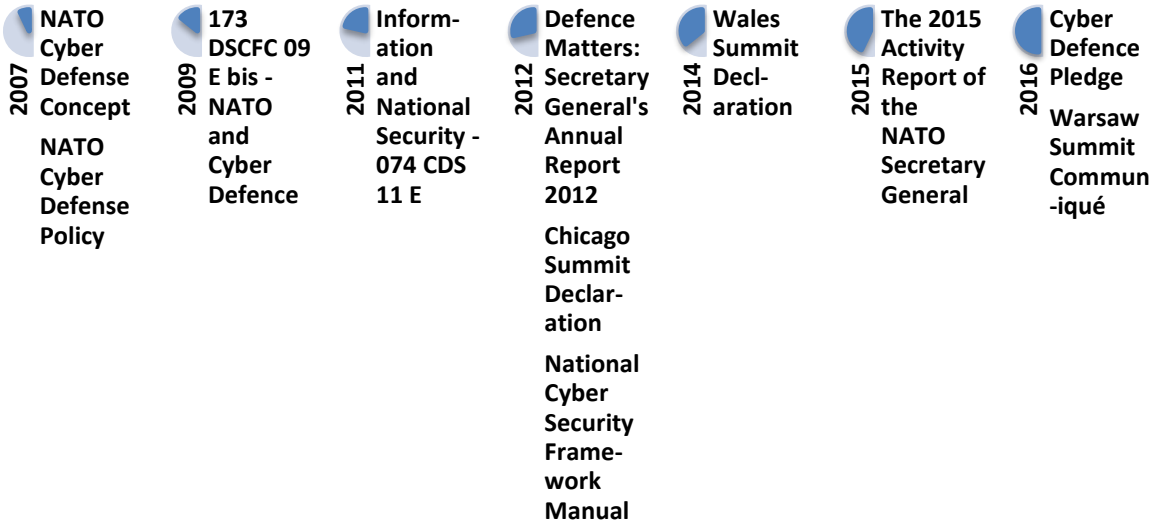
[119] Europeiska Rådet (2017) *Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox").* (9916/17, 7 June 2017), sid 4

[120] Europeiska Rådet (2018) *EU Cyber Defense Policy Framework (2018 update).* (14413/18, 19 November 2018), sid 12-14

3.3 Nordatlantiska fördragsorganisationen

Nordatlantiska fördragsorganisationen (Nato) är en multinationell allians som bildades med *Nordatlantiska fördraget 1949*,[121] bestående i grova ordalag av större delen av Europa, Nordamerika, samt Turkiet. Cyberförsvar har blivit en central del av alliansen,[122] och har fått en tilltagande betydelse sedan toppmötet 2007 och i synnerhet i och med toppmötena 2014 i Wales och 2016 i Warszawa.

Figur 1 Tidslinje över cyberinitiativ i Nato



Innehållet i de tidiga dokumenten från 2007 är inte offentligt men förhållningssättet till cyberförsvar inom Nato har blivit allt mer transparent med tiden. Redan innan Sverre Myrlis skrift[123] hade medlemsstaterna diskuterat huruvida cyberangrepp kunde föranleda kollektivt självförsvar enligt artikel 5 i *Nordatlantiska fördraget*. Myrli etablerade ett försiktigare tillvägagångssätt varvid cyberangrepp mot Nato-medlem motiverade konsultation enligt artikel 4 i fördraget. Konsultationen skulle då utgöra en grund för att gemensamt bedöma huruvida cyberangreppet kan utgöra ett hot mot medlemsstatens territoriala integritet eller politiska oberoende. En tudelad normutvecklande verksamhet påbörjades då medlemsstaterna dels skulle revidera nationella lagar för att tillgodose ett adekvat skydd vid cyberangrepp samt bistå uppbygganden av det så kallade Cooperative Cyber Defence Centre of Excellence (CCDCOE). CCDCOE har sedan dess fått ökande betydelse för forskning om krigets lagar och folkrätt. *National Cyber Security Framework Manual* redogjorde för Nato-medlemstaternas respektive förhållningssätt till folkrättsliga aspekter av cyberangrepp, cyberoperationer och utvecklingen av normer inom FN-systemet, utan att representera en gemensam ståndpunkt från Nato som organisation.

Mest utmärkande för denna studie är att paragraf 72 av *Wales Summit Declaration* och paragraf 70 av *Warszawa Summit Declaration* markerar medlemsstaternas samstämmiga syn på flera punkter. Till exempel anser man att Natos cyberförsvar primärt syftar till skydd av egna nätverk (vilket kan tolkas som en bekräftelse av det folkrättsliga våldsförbudet).[124]

[121] Se även ”Washingtonfördraget” och ”Atlantpakten”.
[122] NATO. (2018). *Cyber defence.* Available: https://www.nato.int/cps/en/natohq/topics_78170.htm. Last accessed 09/12/2018.
[123] Sverre Myrli (2019) *173 DSCFC 09 E bis*
[124] Se artikel 2(4) FN-stadgan; UNGA (1970) *Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations*. A/RES/25/2625

Dessutom belägger deklarationen att folkrätten, inklusive krigets lagar, mänskliga rättigheter och FN-stadgan gäller i cyberrymden. Därutöver fastställer man att ett cyberangrepp kan föranleda medlemsstaternas rätt till kollektivt självförsvar, vilket även betyder att Nato-medlemstaterna anser att cyberangrepp kan, i vissa fall, likställas med väpnat angrepp och därmed utgöra en aggressionshandling.[125]

Natos cyberpolicy implementeras av medlemsstaterna, Natos egna tekniska avdelningar, till exempel Nato Military Authorities och NCIRC Technical Centre, med tillsyn från Nordatlantiska rådet. Natos högkvarter kommer byggas ut med ett Cyberoperationscenter.[126] Utöver detta har Nato och EU ett samarbete för konceptualisering, standardisering, träning, övningar och innovation för cyberförsvar.[127]

Det bör inte minst uppmärksammas att experter inom Nato diskuterar huruvida *offensiva* cyberoperationer kan, eller redan har, integreras i Natos verktygslåda i och med det nya cyberoperationscentrat och dess möjlighet att samordna förmågor från medlemsstaterna.[128] Ett sådant ställningstagande kan anses väsentligt för hur våldsförbudet[129] tillämpas av Nato-medlemmar.

3.3.1 Cooperative Cyber Defence Center of Excellence

Natos CCDCOE är ett tvärvetenskapligt centrum beläget i Tallinn. Centret bidrar till kontraktsparternas målsättning att främja fredliga och stabila internationella förbindelser, fria institutioner och i synnerhet att utveckla förståelse för principerna som institutionerna vilar på enligt artikel 2 i fördraget. Centret fokuserar på teknik, strategi, verksamhet samt lag och utvecklar förståelsen för folkrättsliga aspekter av cyberförsvar. [130] CCDCOE sammanställde även den så kallade *Tallinnmanualen*.

3.3.1.1 Tallinnmanualen

Tallinnmanualen är bland de mest omfattande akademiska verken som publicerats om cyber och folkrätt. Den första upplagan av manualen, som utgavs 2013, riktar sig mot så kallad cyberkrigföring, det vill säga folkrätten som omfattar staters rätt till att föra krig (*jus ad bellum*) och staters skyldigheter i krig (*jus in bello*). Den andra upplagan av manualen, som utgavs 2017, som uppdaterar den tidigare manualen, riktar sig även till cyberoperationer i fredstid. Manualen är akademisk och icke-bindande och saknar därmed den normativa relevans den skulle haft om den utvecklats under FN-stadgan. I dagsläget är den ändå förmodligen den mest auktoritativa folkrättsliga studien gällande cyberoperationer. Sammantaget utvecklar manualen analyser kring cyberrymden, cyberoperationer och följande delar av folkrätten.

Tabell 2 Innehåll i Tallinnmanualen

[125] Artikel 5 Nordatlantiska fördraget (Washington D.C. - 4 April 1949); Artikel 51 FN-stadgan
[126] NATO. (2018). *Cyber defence.* Available: https://www.nato.int/cps/en/natohq/topics_78170.htm. Last accessed 09/12/2018.
[127] NATO/Europeiska Kommissionen (2016) *Statement on the implementation of the Joint Declaration signed by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization*
[128] James A. Lewis. (2015). *THE ROLE OF OFFENSIVE CYBER OPERATIONS IN NATO'S COLLECTIVE DEFENCE* (Tallinn Paper No. 8) Available: https://ccdcoe.org/sites/default/files/multimedia/pdf/TP_08_2015_0.pdf. Last accessed 09/12/2018; Thomas E. Ricks. (2017). *NATO's Little Noticed but Important New Aggressive Stance on Cyber Weapons.* Available: https://foreignpolicy.com/2017/12/07/natos-little-noticed-but-important-new-aggressive-stance-on-cyber-weapons/. Last accessed 09/12/2018; Nato News. (2017). *NATO Secretary General, Press Conference at Defence Ministers Meeting, 8 NOV 2017, 1/2.* Available: https://www.youtube.com/watch?v=8SNEOJn1qg4. Last accessed 09/12/2018
[129] Se artikel 2(4) FN-stadgan
[130] NATO CCDCOE. (2017). *About Cyber Defence Centre.* Available: https://www.ccdcoe.org/about-us.html. Last accessed 18/10/17.

Fred	Säkerhet	Krig
Statssuveränitet	*Fredlig tvistelösning*	*Krigets lagar generellt*
Försiktighet	*Icke-interventionsprincipen*	*Deltagande i fientligheter*
Jurisdiktion	*Våldsförbudet*	*Anfall generellt*
Statsansvar	*Självförsvar*	*Anfall mot personer*
Nödvändighets- och proportionalitetsprincipen	*Kollektiv säkerhet*	*Anfall mot objekt*
Statsansvar för folkrättsstridiga handlingar		*Medel och metoder för krigföring*
Internationella sammanslutningars ansvar		*Uppträdande vid angrepp*
Cyberoperationer som inte i sig regleras		*Försiktighetsåtgärder*
Mänskliga rättigheter		*Förrädiskt förfarande*
Diplomat- och konsulärrätt		*Blockader*
Havsrätt		*Medicinska och religiösa resurser*
Lufträtt		*Fångar*
Rymdrätt		*Barn*
Telekommunikationsrätt		*Journalister*
		Anläggningar och installationer som innehåller farliga krafter
		Objekt som är oumbärliga för civilbefolkningens överlevnad
		Kulturegendom
		Miljön
		Kollektiv bestraffning
		Humanitär assistans
		Ockupation
		Neutralitet

Då Tallinnmanualen utkom efter delbetänkandet SOU 2010:22 återfinns den inte i delbetänkandets kartläggning av tillämpliga manualer angående krigets lagar, såsom till exempel *San Remo-manualen* och *Luftkrigsmanualen*.

3.4 Organisationen för säkerhet och samarbete i Europa

Organisationen för säkerhet och samarbete i Europa (OSSE) bedriver normutvecklande verksamhet i förtroendeskapande syfte.[131] Organisationens verksamhet omfattar policy för IKT-säkerhet, it-brottsbekämpning och cyberterrorism. Det förtroendeskapande arbetet inom it-säkerhet omfattar bland annat åtgärder för att förebygga angrepp och eskalerande konflikt på cyberdomänen.[132] Diskussionerna inom IKT och säkerhet ledde till att de

[131] OSSE. (2018). *Cyber/ICT Security*. Available: https://www.osce.org/secretariat/cyber-ict-security. Last accessed 01/07/2019.
[132] OSSE. (2014). *Cyber/ICT security*. Available: https://www.osce.org/secretariat/106324. Last accessed 07/01/2019.

deltagande staterna antog ett beslut om initiala interdimensionella förtroendebyggande åtgärder; *Decision No. 1106 Initial set of OSCE confidence-building measures to reduce the risks of conflict stemming from the use of information and communication technologies.*[133] Ett ytterligare beslut om interdimensionella förtroendebyggande åtgärder, följde 2016; *Decision No. 1202 OSCE confidence-building measures to reduce the risks of conflict stemming from the use of information and communication technologies.*[134] Båda besluten inleder med att framhålla folkrättens betydelse, särskilt med hänvisning till *FN-stadgan*, *FN:s konvention om medborgerliga och politiska rättigheter*, samt OSSE:s egna avtal; *Helsingforsdeklarationen (1975).* Medan besluten inte uppgav några särskilda folkrättsliga implementeringsåtgärder för aktiva och offensiva cyberoperationer innehåller *Helsingforsdeklarationen* förtydliganden om tio relevanta principer:

I. Staters suveräna likställdhet och respekt för suveränitet.

II. Att avstå från hot och aggression.

III. Statsgränsernas okränkbarhet.

IV. Staters territoriella integritet.

V. Fredlig lösning av tvister.

VI. Icke-intervention i staters interna angelägenheter.

VII. Respekt för mänskliga rättigheter och grundläggande friheter.

VIII. Folkens lika rättigheter och självbestämmanderätt.

IX. Samarbete mellan stater.

X. God tro i efterlevnad av folkrätten.

Det är även nämnvärt att Ryssland begärde att deras tolkning av beslutet från år 2012 skulle bifogas. I denna tolkning ställer sig Ryssland likasinnad till beslutet men trycker vidare på vikten av icke-intervention, staters suveräna likställdhet i diskussioner om internetstyrning, folkrättens betydelse och särskilt de mänskliga rättigheterna.[135]

[133] OSSE. (2013). *Decision No. 1106 Initial set of OSCE confidence-building measures to reduce the risks of conflict stemming from the use of information and communication technologies*. (PC.DEC/1106, 3 December 2013)

[134] OSSE. (2016). *Decision No. 1202 OSCE confidence-building measures to reduce the risks of conflict stemming from the use of information and communication technologies*. (PC.DEC/1202, 10 March 2016)

[135] OSSE. (2013). *Decision No. 1106 Initial set of OSCE confidence-building measures to reduce the risks of conflict stemming from the use of information and communication technologies (Russian Federation, interpretative statement.* (PC.DEC/1106, 3 December 2013)

4 Sammanfattning

Det internationella normutvecklande arbetet sammanfaller ofta med en diplomatisk vilja att upprätta åtgärder för internets säkerhet och stabilitet. Några generella trender är även tydliga i utvecklingen. För det första tenderar det att finnas en övergripande konsensus att folkrätten gäller och i synnerhet *FN-stadgan, krigets lagar* och *mänskliga rättigheter*. Statssuveränitet, icke-aggression och fredlig tvistelösning framstår som särskilt starka angelägenheter. För det andra finns det, trots denna övergripande konsensus, en avsaknad av ömsesidig förståelse om lämplig tillämpning för dessa normer, särskilt i relation till aktiva och offensiva cyberoperationer. Tillämpningen förtydligas typiskt sett genom icke-bindande vägledningar, utspridda över organisationer för likasinnade samt olika internationella expertgrupper. Även om dessa källor är icke-bindande är de formativa i det att de sätter agendan för vilka lagrum och principer som bör prioriteras i normutvecklingen, samt skapar en grundläggande förståelse för tillämpningsalternativ. Dessutom kan de i vissa fall leda till initiativ för bindande förslag, till exempel att EU ska verka för ett nytt kapitel till 1980 års vapenkonvention.[136] Det bör även påpekas att internationella domstolar och tribunaler ännu inte har dömt i något fall som relaterar till militära cyberoperationer stater emellan. Medan instrument som manualer och akademisk tolkning kan citeras i tvistefall är sådana domstolsprövningar relativt ovanliga medel för lösning av tvister mellan stater. Således förefaller sannolikheten till normativt styrkande av den aktuella förståelsen av folkrätten ändå begränsad i närtid. För det tredje är diskussionerna i stort förankrade i traditionell folkrätt med inslag av nya framväxande normer för militära cyberoperationer. Exempel på nya normer inbegriper upprättandet av bedömningsprocesser för sårbarheter som skulle kunna användas i militär- och underrättelseverksamhet, samt mänsklig kontroll över artificiell intelligens. Slutligen påvisar studien att det finns komplexa samband mellan hur normativ utveckling i angränsande lagrum, såsom i rymdrätten och i rätten för konventionella vapen, kan komma att påverka normer för aktiva cyberoperationer.

[136] Europaparlamentets resolution om autonoma vapensystem (2018/2752(RSP)); Europaparlamentets resolution om autonoma vapensystem (2018/2752(RSP))

5 Källor

Betänkande av NISU 2014 (SOU 2015:23).

Campaign to Stop Killer Robots. (2018). *All action and achievements.* från: https://www.stopkillerrobots.org/action-and-achievements/. senast 09/12/2018.

Campaign to Stop Killer Robots. (2018). *Consensus: killer robots must be addressed.* från: https://www.stopkillerrobots.org/2013/05/nations-to-debate-killer-robots-at-un/. senast 10/12/2018

Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons which may be deemed to be Excessively Injurious or to have Indiscriminate Effects (adopted10 October 1980, eneterd into force 2 December 1983) UNTS 1342.

Enander, D. (2016). *”DET DIGITALA STRIDSFÄLTET ÄR EN REALITET”: Därför vill Försvarsmakten ha aktiv cyberförmåga.* från: https://www.forsvarsmakten.se/siteassets/6-aktuellt/forsvarets-forum/2016/forsvarets-forum-3-2016.pdf. senast 23/01/2018.

Fournier, G (2016) Towards a definition of lethal autonomous weapons systems. (CCW/GGE.1/2017/WP.3, inlämnad av Belgien)

Försvarsdepartementet (2013) Försvarsmaktens redovisning av perspektivstudien 2013 (FM2013-276:1).

Försvarsdepartementet (2014) Försvaret av Sverige- Starkare försvar för en osäker tid (Ds 2014:20).

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

Försvarsmakten (2008) Försvarsmaktens Handbok Informationsoperationer: Handbok Info Ops (09 833:61968).

Försvarsmakten (2016) *Militärstrategisk Doktrin 2016 (MSD16).*

Försvarsmakten (2014) *Operativ Doktrin 2014 (OPD).*

Försvarspolitisk inriktning – Sveriges försvar (Prop 2014:15:109).

Försvarsutskottets betänkande: Försvarspolitisk inriktning - Sveriges försvar 2016-2020 (2014/15:FöU11).

Group of Governmental Experts of the High Contracting Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects (2017) *Report of the 2017 Group of Governmental Experts on Lethal Autonomous Weapons Systems (LAWS).* (CCW/GGE.1/2017/3).

Holmström, M. (2015). *Försvarsministern: Vi ska kunna genomföra cyberattacker.* från: https://www.dn.se/nyheter/sverige/forsvarsministern-vi-ska-kunna-genomfora-cyberattacker/. senast 23/01/2018.

ICRC (2015) International humanitarian law and the challenges of contemporary armed conflicts Report Document prepared by the International Committee of the Red Cross. (32IC/15/11).

IGF. (2018). *About the IGF*. från: https://www.intgovforum.org/multilingual/tags/about. senast 09/12/2018S.

Informationssäkerhet i Sverige och internationellt – en översikt (SOU 20014:32).

Inriktning för Försvarsmaktens verksamhet för åren 2016 till och med 2020 (Fö2015/00953/~FI).

Jenning, R, och Arthur Watts (2008). Oppenheim's International Law. Oxon: Oxford University Press.

Lejon, J. (2016). *VAD INNEBÄR EN AKTIV SVENSK CYBERFÖRMÅGA?.* från: https://kryptera.se/cyberformaga/. senast 23/01/2017.

Melzer, N. (2011). *Cyberwarfare and International Law.* från: http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf. senast 07/01/2019.

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

Nationell strategi för samhällets informations- och cybersäkerhet (Skr. 2016/17:213).

Offensiv cyberförmåga Interpellation 2017/18:22.

Protocol additional to the Geneva Conventions of12 August 1949, and relating to the protection of victims of international armed conflicts (Protocol I) (adopted on 8 June 1977).

Regeringsbeslut: Inriktning för Försvarsmaktens verksamhet för åren 2016 till och med 2020 (Fö2015/00953/~FI).

Riksdagens protokoll 2017/18:21.

Rõigas, H. (2015). *An Updated Draft of the Code of Conduct Distributed in the United Nations – What's New?* från: https://ccdcoe.org/updated-draft-code-conduct-distributed-united-nations-whats-new.html. senast 21/11/2017.

Folkrätt i väpnad konflikt – svensk tolkning och tillämpning (SOU 2010:72).

Svar på skriftlig fråga 2017/18:75 Svar på fråga 2017/18:75 av Pål Jonson (M) Aktiv cyberförmåga.

Swedish Government. (2014). *Submission by Sweden to UNGA resolution 68/243 entitled "Developments in the field of information and telecommunications in the context of international security", 12 September 2014.* från: https://unoda-web.s3-accelerate.amazonaws.com/wp-content/uploads/2014/10/Sweden.pdf. senast 21/11/2017.

Ticehurst, R. (1997). *The Martens Clause and the Laws of Armed Conflict.* från: https://www.icrc.org/en/doc/resources/documents/article/other/57jnhy.htm. senast 01/04/2019.

UNGA Committee on the Peaceful Uses of Outer Space (2018) *Guidelines for the long-term sustainability of outer space activities.* A/AC.105/C.1/L.362
UNGA Resolution 56/83 *Responsibility of States for Internationally Wrongful Acts* (A/56/49(Vol. I)/Corr.4).

UNGA Resolution 70/125 *Outcome document of the high-level meeting of the General Assembly on the overall review of the implementation of the outcomes of the World Summit on the Information Society*. (A/RES/70/125).

UNGA (2010). *Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions.* A/HRC/14/24/Add.6.

UNGA. (2011). *Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General.* A/66/359 från: https://ccdcoe.org/sites/default/files/documents/UN-110912-CodeOfConduct_0.pdf. senast 21/11/2017.

UNGA. (2015). *Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-Gene.* från: https://ccdcoe.org/sites/default/files/documents/UN-150113-CodeOfConduct.pdf. senast 21/11/2017.

UNIDIR (2017) The Weaponization of Increasingly Autonomous Technologies: Autonomous Weapon Systems and Cyber Operations. Report No. 7.

UNIDIR. (2018). *Research project: The Weaponization of Increasingly Autonomous Technologies.* från: http://www.unidir.org/programmes/security-and-technology/the-weaponization-of-increasingly-autonomous-technologies-phase-iii. senast 12/12/2018.

UNIDIR. (2019). *Cyber.* från: http://www.unidir.org/est-cyber. senast 07/01/2019.

UNODA. (2017). *Developments in the field of information and telecommunications in the context of international security*. från: https://www.un.org/disarmament/topics/informationsecurity/. senast 21/11/2017.

UNOG (2017) *Report of the 2017 Group of Governmental Experts on Lethal Autonomous Weapons Systems (LAWS).* CCW/GGE.1/2017/3.

UNOG. (2018). *Background on Lethal Autonomous Weapons Systems in the CCW*. från: https://www.unog.ch/80256EE600585943/(httpPages)/8FA3C2562A60FF81C1257CE600393DF6?OpenDocument senast 11/12/2018.

UNOG. (2018). *2018 Group of Governmental Experts on Lethal Autonomous Weapons Systems (LAWS)*. från: https://www.unog.ch/80256EE600585943/(httpPages)/7C335E71DFCB29D1C1258243003E8724?OpenDocument. senast 11/12/2018.

UNOOSA. (2017). *Committee on the Peaceful Uses of Outer Space and its Subcommittees.* från: http://www.unoosa.org/oosa/en/ourwork/copuos/comm-subcomms.html. senast 17/10/2017.

UN (2006) *Reports of International Arbitral Awards: Island of Palmas case (Netherlands, USA)* (VOLUME II pp. 829-871).

UN. (2019). The Foundation of International Human Rights Law. från: http://www.un.org/en/sections/universal-declaration/foundation-international-human-rights-law/index.html. senast 23/01/2019.

Westman, J, Erik Zouave, Christian Valassi (2017) *Cybersäkerhet på rymdarenan*. (FOI-D--0820--SE).

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