Offensiva cyberoperationer och Natos defensiva mandat

av Dirk Roland Haupt

Résumé

The relation between offensive cyber operations and NATO's defensive mandate has become relevant as a consequence of the recognition, at the 2016 Warsaw Summit, of cyberspace as "a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea." While NATO, as an international organization, is constrained by its mandate in developing own offensive cyber capabilities, it is argued here that sovereign offensive cyber capabilities could be used, under certain political and legal conditions, to support NATO military operations and missions. Whereas NATO stresses the need to focus on building robust cyber defense capabilities, it follows from the 2016 "Cyber Defense Pledge" that it is not only a national responsibility under Article 3 of the 1949 North Atlantic Treaty to enhance the cyber defenses of national infrastructures and networks, but also primarily a sovereign prerogative to respond to cyber attacks. With the twofold aim to keep NATO's defensive mandate clear of ambiguities and to clarify the scope and delimitations of the sovereign response prerogative, it would appear reasonable if Allies supported the integration of cyber effects into NATO operations and missions by an agreement on key principles.

FRAMVÄXTEN AV ALLTMER komplicerade och allvarliga hot från cyberrymden uppmanar en försvarsallians som Nato att förändra dess sätt att tänka på hur den utför militära operationer för att upprätthålla militär överlägsenhet och för att bevara Natos och de allierades frihet att agera i den digitala tidsåldern. Alliansen har därför tagit ett stort steg genom att erkänna cyberrymden som en operativ domän. Som en del av en militär operation kan uppdrag i den digitala rymden utföras som underrättelse-, försvars- och offensiv verksamhet mot fiender eller motståndare. Trots att Natos mandat är rent defensivt, kan alliansen ändå dra nytta av verkningar, vilka åstadkoms till stöd för Natos operationer genom offensiv IT-kapacitet som en allierad nation begagnar sig av i utövande av sin suveränitet. Det är emellertid absolut nödvändigt att alliansens begränsningar i detta hänseende beaktas.

Detta bidrag tar inte upp frågan om cyberkapaciteter som används för underrättelseändamål.

Natos defensiva mandat

På toppmötet i Warszawa den 8 och 9 juli 2016 bekräftade stats- och regeringscheferna Natos defensiva mandat, innan de erkände cyberrymden som ”en domän för operationer där Nato måste försvara sig lika effektivt som i luften, på land och till sjöss”.[1] Uttövande av ett lands suveränitet för att mobilisera nationell offensiv IT-förmåga till stöd för Natos militära operationer kan därför endast beaktas i den utsträckning detta bidrar till alliansens defensiva mandat. I samma anda och eftersom det är den

främsta prioriteten för alla försvarsinsatserna på IT-området måste Nato vidare fortsätta att förbättra sin förmåga att skydda och att försvara sina nätverk – dels genom att vidta de skyddsåtgärder som gör det möjligt för ett IT-system att motstå händelser som kan påverka tillgängligheten, integriteten eller konfidentialiteten av lagrad, bearbetad eller överförd data, dels genom att vidta de upptäckts- och reaktionsåtgärder som är nödvändiga för att skydda mot anfall[2] eller för att säkerställa driften av de berörda enheternas nätverk, alltmedan de allierade måste sätta upp ambitiösa kapacitetsmål för att skydda sina egna nätverk. Det är syftet med det åtagande om cyberförsvar[3] ("Cyber Defense Pledge"), som Nato antog den 8 juli 2016 och vilket de allierade nationerna nu måste genomföra.

Möjligheter och begränsningar för offensiva cyberoperationer

Offensiva cyberoperationer omfattar alla åtgärder som möjliggör en ej på samarbete grundad tillgång till motståndarens system eller nätverk i syfte att orsaka skada, tjänsteavbrott eller tillfällig eller varaktig avstängning. De bidrar till att uppnå ett specifikt mål, såsom att motverka en motståndare genom att hämma dennes förmåga att agera (t ex genom ledning och kontroll, propaganda eller finansiering) eller att stänga av infrastruktur som skulle kunna användas för att utföra kinetiska anfall.

Följande egenskaper är kännetecknande för offensiva cyberoperationer:

- De kräver en betydande och långsiktig investering. Den förutsättningslösa utvecklingen av ett cybervapen är resultatet av en långsiktig process. Först måste sättet att få tillgång till motståndarens nätverk bestämmas och sedan sättas i drift, genom teknisk eller mänsklig förmedling, forcerat intrång eller andra tillvägagångssätt. Valet och utvecklingen av nyttolasten liksom dess hopsättning kräver också stora investeringar i form av arbetskraft, resurser och tid. Efter detta första steg måste tid avsättas för den valda metoden för att kunna verka.
- Mot en bestämd motståndare kan ett cybervapen som regel endast användas en enda gång. Efter ett cyberanfall kommer en motståndare att anpassa sina system och nätverk; ett IT-vapen kan därför normalt inte användas mot samma motståndare med samma konfiguration och under samma förhållanden. Framgången av ett dylikt program beror därför på extremt strikta sekretesskrav.
- De bär på en spridningsrisk.[4] Som framgår av den befintliga variansen av Stuxnet-viruset[5] kan ett cybervapen replikeras i all oändlighet. Även om det ibland krävs storskaliga resurser för att utveckla ett cybervapen, krävs det däremot endast få resurser – eller inte större resurser än dem som är tillgängliga för alla – för att återskapa dess design, när den en gång har blivit avslöjad. Det är denna tillgänglighet som gör cybervapen attraktiva, bl a för aktörer med begränsade resurser.

Dessa särdrag gör IT-vapen till en förmåga som kan vara svår att kontrollera, är komplex att generera och kräver en mycket hög konfidentialitet. De suveräna stater som utvecklar sådan kapacitet blir ansvariga för dem, vilket inte endast är en rättsföljd enligt internationell sedvanerätt, utan för de allierades vidkommande en konsekvens härledd ur artikel 3 i Nordatlantiska fördraget dagtecknat i Washington D.C. den 4 april 1949.[6]

Detta är skälet till varför Nato i egenskap av internationell organisation inte utvecklar och inte har planer på att utveckla sin egen offensiva cyberkapacitet.

Förutsättningar för bruk av suverän offensiv IT-kapacitet till stöd för Natos militära operationer och uppdrag

Mobilisering av suverän IT-kapacitet

Den operativa överlägsenhet som de allierades väpnade styrkor upprätthåller, d v s deras förmåga att dels kontrollera kriser som innebär militär handling, dels utöva militärt tvång mot en motståndare, kräver numera ofrånkomligen att de verkar för och uppnår överlägsenhet också i cyberrymden. Projektionen av makt i den fysiska rymden kan inte längre dissocieras från projektionen av makt i den digitala rymden. Handlingar i båda sfärerna måste tas samfällt. Erkännandet av cyberrymden som en operativ domän bekräftar denna fastställelse.

Härav följer att en lämplig operation eller mission som genomförs av Nato, inklusive en sådan enligt artikel 5 i 1949 års Nordatlantiska fördrag,[7] skulle kunna innefatta offensiva IT-åtgärder, under förutsättning att de frivilligt tillhandahålls av en allierad eller allierade. Detta skulle innebära användning av suverän IT-kapacitet för att bidra till uppnåendet av en verkning som identifierats av Natos överbefälhavare för de allierade styrkorna i Europa (SACEUR) som en del av dennes verksamhetsplan. Medan en sådan effekt skulle ha definierats av Nato enligt etablerade förfaranden, skulle de IT-kapaciteter som användes för att få fram den, förbli under uteslutande nationell kontroll på grund av deras mycket känsliga natur. Sådan nationell kontroll skulle utövas inom den bredare, av alliansen uppsatta politiska ramen för operationen eller missionen och i enlighet med folkrätten.

Specifik politisk och rättslig ram för erkännandet av cyberrymden som en operativ domän

Alliansens agerande i cyberrymden ska styras av den i tider av väpnad konflikt gällande folkrätten, vilket omfattar

- dels de folkrättsliga regler, som gäller med avseende på rätten att tillgripa militärt våld (jus ad bellum):[8] Offensiva cyberoperationer kan således endast genomföras inom den rättsliga ramen för en militär operation eller ett militärt uppdrag av Nato, d v s i enlighet med folkrätten (t ex enligt ett mandat från FN:s säkerhetsråd som är grundat på kapitel VII i FN-stadgan om inskridande i händelse av hot mot freden, fredsbrott och angreppshandlingar eller enligt den i artikel 51 i FN-stadgan erkända rätten till självförsvar såsom den får utövas jämlikt artikel 5 i 1949 års Nordatlantiska fördrag);
- dels den i väpnade konflikter tillämpliga folkrätten (jus in bello):[9] Offensiva cyberoperationer utförs i enlighet med krigets lagar, vilka omfattar bl a principerna om nödvändighet, proportionalitet, åtskillnad och försiktighetsåtgärder vid anfall.

Härav följer således att alla offensiva cyberoperationer som genomförs inom ramen för Nato måste vara i överensstämmelse med gällande folkrätt, vilket tydligt underströks vid toppmötet i Wales den 4 och 5 september 2014, där det bekräftades Natos och dess allierades åtagande att i förekommande fall

agera i enlighet med folkrätten, inklusive FN-stadgan och internationell humanitär rätt – ett förtydligande som i kommunikén från 2016 års toppmöte i Warszawa också kom att uttryckligen nämna de mänskliga rättigheternas folkrätt.[10]

Suveränt företräde att reagera på ett cyberanfall

När det gäller att dra upp politiska ramar är det till hjälp att skilja mellan å ena sidan, samordningen av cybereffekter i alliansens operationer och uppdrag, och å andra sidan det potentiella svaret på ett cyberanfall mot en allierad. Dessa två frågor är endast delvis sammanlänkade. Behovet av att Nato och dess allierade fokuserar på att bygga upp robusta förmågor för försvar i cyberrymden i den andemening som förestavas av 2016 års åtagande om cyberförsvar, utgör visserligen den gemensamma nämnaren för båda. Vid cyberanfall riktade mot dem är de som är bättre förberedda också snabbare att återhämta sig.

Planering av ett omfattande, skräddarsytt och samordnat svar

Vid 2014 års toppmöte i Wales vidgick Nato att artikel 5 i 1949 års Nordatlantiska fördrag kunde åberopas om cyberanfall nådde upp till tröskeln för väpnade angrepp.[11] Det betyder emellertid inte att alliansens svar på ett cyberanfall måste i sin tur vara ett cyberanfall.[12] I en situation där artikel 5 är tillämplig måste alliansen kunna svara med alla instrument som står till dess förfogande på ett sammanhängande tillvägagångssätt.

Inte heller måste bruk av våld anses vara det enda sättet att reagera på ett cyberanfall, särskilt då de flesta nuvarande cyberanfall ligger under tröskeln för väpnade angrepp. Därför är det avgörande för alla politiska beslutsfattare att ha ett brett utbud av svar tillgängligt, vars optioner inte är begränsade till de militära eller informationsteknologiska sfärerna. Användningen av diplomatiska instrument måste ingå i sådana alternativ. Oaktat att beslut att reagera mot cyberanfall är av suverän beskaffenhet kan internationella organisationer spela en roll på detta område. I det avseendet är det viktigt att Nato samverkar med de andra internationella organisationer som på olika sätt kan vara involverade i sådana reaktioner, i främsta rummet EU som har ett brett utbud av mycket olika och kompletterande verktyg.[13]

Kalibrering av tillräknelighetsproblemet

Att tillräkna ett cyberanfall dess upphovsman är en svår och komplicerad process som inte alltid tillåter att slutsatser kan dras med säkerhet. Baserat på det bevismaterial som sammanställs genom att man dubbelkontrollerar beaktansvärda underrättelsekällor och med hänsyn taget till det bredare sammanhanget är tillräknelighetsproblemet inte i första hand något folkrättsligt spörsmål och i vart fall inte endast en teknisk fråga, utan ytterst ett ställningstagande grundat på en politisk bedömning.[14] Informationsdelning mellan stater kan, genom att man skapat lämpliga förfaranden och verktyg, bidra till att förbättra nationella möjligheter när det gäller tillräknelighetsavgöranden. Staterna förblir emellertid suveräna när det gäller deras beslut att identifiera anfallaren[15] respektive motståndaren samt att eventuellt vidta motåtgärder.[16] På samma sätt är staterna enligt folkrätten ansvariga i efterhand för sina handlingar om de skulle reagera oskäligt, oproportionerligt eller i övrigt folkrättsstridigt.[17]

Slutsats

Övervägandena ovan talar för att Nato och dess allierade vägleds av fastställda principer för att stödja samordningen av cybereffekter i Natos operationer och uppdrag. Vissa är direkta följder av folkrättsliga förpliktelser som åvilar de allierade eller av politiska beslut som de fattat eller bekräftat, i samförstånd eller individuellt med de övrigas godkännande, medan andra ter sig som skäliga konsekvenser eller plausibla slutledningar grundade på Natos och dess allierades handlingspremisser. I en dylik uppsättning av principer skulle ingå bl a följande:

- Nato har inga planer på att utveckla en egen offensiv IT-kapacitet.
- Nato kommer att vara effektivare i sitt avskräcknings- och försvarsuppdrag om de allierade förbereder sig för att kunna verka med likvärdig kraft i cyberrymden som i andra domäner.
- Nato kommer inte att uppmana de allierade att de förbinder sig att tillhandahålla offensiva IT-kapaciteter. Istället äger de frivilligt ställa suveräna cyberförmågor till förfogande till stöd för det inom Nato önskade och överenskomna resultatet.
- Inrättandet av en mekanism som stöder integrationen av IT-verkningar i Natos operationer och uppdrag. En sådan mekanism bör ta hänsyn till den suveräna naturen av de allierades IT-förmågor, återspegla de allierades kraftfulla politiska tillsyn av planeringen och målinriktningen och vara förenlig med Natos skyldigheter enligt gällande folkrätt.
- Allierade som bidrar med IT-kapaciteter kommer att behålla fullständig kontroll och omfattande ansvar över dessa. Detta inkluderar de bidragande allierades ansvar för folkrättsenligheten av bruket av IT-kapaciteter.
- För att mekanismen ska vara effektiv bör det krävas att sakkunniga kontaktpunkter bestäms, vilka är inbäddade i den operativa planeringsprocessen och som är kapabla att bedöma när en viss verkan skulle kunna uppnås med hjälp av den egna statens IT-kapaciteter.
- Framtida planering av operationer och övningar bör säkerställa en jämvikt mellan å ena sidan behovet av att planera för den potentiella samordningen av suveräna IT-verkningar med och till stöd för Natos operationer och uppdrag, å andra sidan nödvändigheten av att skydda känslig nationell information.
- Mekanismen bör så långt som möjligt respektera principerna för framgångsrika militära operationer inom den fysiska domänen och följa befintlig Natodoktrin.
- I framtiden bör allierade ta hänsyn till den möjliga integrationen av suveräna IT-verkningar för att öka rörlighet och effektivitet. Detta bör ske som en del av den tillämpliga överenskomna färdplanen för att omfatta cyberrymden som en operativ domän.
- De berörda allierades ledningar bör komma överens om ett militärt forum inom Nato för att kunna dryfta nödvändiga och önskvärda framsteg vid samordningen av suveräna offensiva nätverkseffekter som stöder en operation eller ett uppdrag som Nato ska eller är mandaterad till att genomföra.

Författaren är jur lic.

Noter

1. § 70 i ”Warsaw Summit Communiqué, Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Warsaw 8-9 July 2016”, *http://www.nato.int/cps/en/natohq/official_texts_133169.htm#cyber* (2017-06-13), vars tredje mening har följande ordalydelse: ”Now, in Warsaw, we reaffirm NATO’s defensive mandate, and recognise cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea.”
2. Detta bidrag använder terminologin ”anfall” resp ”cyberanfall” i stället för begreppen cyber- eller IT-angrepp resp cyber- eller IT-attacker, vilket också hade varit rimligt, inte minst med tanke på att artikel 51 i FN-stadgan om FN-medlemmarnas naturliga rätt till individuellt eller kollektivt självförsvar begagnar sig av uttrycket ”väpnat angrepp”. Skälet härtill är att söka lägga bidragets framställningssätt så nära definitionen av uttrycket ”anfall” i artikel 49:1 i 1977 års tilläggsprotokoll I (SÖ 1979:22) till Genèvekonventionerna den 12 augusti 1949 rörande skydd för offren i internationella väpnade konflikter som möjligt. Enligt denna bestämmelse avses med uttrycket ”anfall” våldshandling mot motståndaren, vare sig handlingen är offensiv eller defensiv.
3. § 71 i op cit, ”Warsaw Summit Communiqué, Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Warsaw 8-9 July 2016”, se not 1, innehåller en hänvisning till detta åtagande som emellertid antogs vid toppmötet i Warszawa som ett fristående dokument. Natos ”Cyber Defense Pledge”, *http://www.nato.int/cps/en/natohq/official_texts_133177.htm* (2017-06-13), har följande ordalydelse:
    1. In recognition of the new realities of security threats to NATO, we, the Allied Heads of State and Government, pledge to ensure the Alliance keeps pace with the fast evolving cyber threat landscape and that our nations will be capable of defending themselves in cyberspace as in the air, on land and at sea.
    2. We reaffirm our national responsibility, in line with Article 3 of the Washington Treaty, to enhance the cyber defences of national infrastructures and networks, and our commitment to the indivisibility of Allied security and collective defence, in accordance with the Enhanced NATO Policy on Cyber Defence adopted in Wales. We will ensure that strong and resilient cyber defences enable the Alliance to fulfil its core tasks. Our interconnectedness means that we are only as strong as our weakest link. We will work together to better protect our networks and thereby contribute to the success of Allied operations.
    3. We welcome the work of Allies and the EU on enhancing cyber security, which contributes to reinforcing resilience in the Euro-Atlantic region, and we support further NATO–EU cyber defence co-operation, as agreed. We reaffirm the applicability of international law in cyberspace and acknowledge the work done in relevant international organisations, including on voluntary norms of responsible state behaviour and confidence-building measures in cyberspace. We recognise the value of NATO’s partnerships with partner nations, industry and academia, including through the NATO Industry Cyber Partnership.
    4. We emphasise NATO’s role in facilitating co-operation on cyber defence including through multinational projects, education, training, and exercises and information exchange, in support of national cyber defence efforts. We will ensure that our Alliance is cyber aware, cyber trained, cyber secure and cyber enabled.
    5. We, Allied Heads of State and Government, pledge to strengthen and enhance the cyber defences of national networks and infrastructures, as a matter of priority. Together with the continuous adaptation of NATO’s cyber defence capabilities, as part of NATO’s long term adaptation, this will reinforce the cyber defence and overall resilience of the Alliance. We will:
        1. Develop the fullest range of capabilities to defend our national infrastructures and networks. This

includes: addressing cyber defence at the highest strategic level within our defence related organisations, further integrating cyber defence into operations and extending coverage to deployable networks;

ii. Allocate adequate resources nationally to strengthen our cyber defence capabilities;

iii. Reinforce the interaction amongst our respective national cyber defence stakeholders to deepen co-operation and the exchange of best practices;

iv. Improve our understanding of cyber threats, including the sharing of information and assessments;

v. Enhance skills and awareness, among all defence stakeholders at national level, of fundamental cyber hygiene through to the most sophisticated and robust cyber defences;

vi. Foster cyber education, training and exercising of our forces, and enhance our educational institutions, to build trust and knowledge across the Alliance;

vii. Expedite implementation of agreed cyber defence commitments including for those national systems upon which NATO depends.

6. To track progress on the delivery of our Pledge, we task an annual assessment based on agreed metrics, and we will review progress at our next summit.

4. Se härom Cohen, Daniel och Rotbart, Aviv: ”The Proliferation of Weapons in Cyberspace” i Siboni, Gabi (red): *Cyberspace and National Security. Selected Articles [I]*, Institute for National Security Studies, Tel Aviv 2013, s 105-125.

5. Se härom Haupt, Dirk Roland: ”Stuxnet i folkrättslig belysning”, *KKrVAHT*, 3. häftet 2015, s 72-88, och Lewis, James A: ”In Defense of Stuxnet” i Siboni, Gabi (red): *Cyberspace and National Security. Selected Articles II*, Institute for National Security Studies, Tel Aviv 2014, s 83-94.

6. Artikel 3 i Nordatlantiska fördraget innehåller en bestämmelse om de allierades åtagande att upprätthålla och utveckla individuella och kollektiva försvarsförmågor. Den har följande ordalydelse på danska, som är en av de autentiska språkversionerna:

. Med henblik på mere effektivt at virkeliggøre denne traktats formål vil deltagerne, hver for sig og i fællesskab, gennem stadig og effektiv selvhjælp og gensidig hjælp opretholde og udvikle deres individuelle og kollektive evne til at imødegå væbnet angreb.

7. Artikel 5 i Nordatlantiska fördraget är en bestämmelse om försvarsalliansparternas gemensamma reaktion på angrepp. Den har följande ordalydelse på danska:

. Deltagerne er enige om, at et væbnet angreb mod en eller flere af dem i Europa eller Nordamerika skal betragtes som et angreb mod dem alle; og de er følgelig enige om, at hvis et sådant angreb finder sted, skal hver af dem under udøvelse af retten til individuelt eller kollektivt selvforsvar, som er anerkendt ved artikel 51 i De Forenede Nationers pagt, bistå den eller de således angrebne deltagerlande ved straks, hver for sig og i forståelse med de øvrige deltagerlande, at tage sådanne skridt, derunder anvendelse af væbnet magt, som hver af dem anser som nødvendige for at genoprette og opretholde det nordatlantiske områdes sikkerhed.

. Ethvert sådant angreb og alle som følge deraf trufne forholdsregler skal uopholdeligt indberettes til Sikkerhedsrådet. Sådanne forholdsregler skal bringes til ophør, når Sikkerhedsrådet har truffet de til genoprettelse og opretholdelse af den mellemfolkelige fred og sikkerhed fornødne forholdsregler.

8. Schmitt, Michael N (red): *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, Cambridge 2017, s 328-356.

9. Ibid, s 373-562.

10. Hette det ännu i femte meningen av § 72 i ”Wales Summit Communiqué, Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Wales 4-5 September 2014”, *http://www.nato.int/cps/en/natohq/official_texts_112964.htm#cyber* (2017-06-13) att ”[o]ur policy also recognises that international law, including international humanitarian law and the UN Charter, applies in cyberspace”, så förklarades det i nionde meningen av § 71 i op cit, ”Warsaw Summit Communiqué, Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Warsaw 8-9 July 2016”, se not 1, att “[w]e reaffirm our commitment to act in accordance with international law, including the UN Charter,

international humanitarian law, and human rights law, as applicable".

11. § 72 i op cit, "Wales Summit Communiqué, Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Wales 4-5 September 2014", se not 10, vars sista mening har följande ordalydelse: "A decision as to when a cyber attack would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis."
12. Op cit, Schmitt, Michael N (red), se not 8, s 339-354.
13. Av särskild betydelse bland EU:s politiska koncept och verktyg, fast långt ifrån uttömmande, är
    - rådets slutsatser om det gemensamma meddelandet 'EU:s strategi för cybersäkerhet: En öppen, säker och trygg cyberrymd' från kommissionen och unionens höga representant för utrikes frågor och säkerhetspolitik, antagna den 7 februari 2013 (rådets dokument 12109/13),
    - ramen för EU:s politik för it-försvar, antagen av rådet den 18 november 2014 (rådets dokument 15585/14)
    - rådets slutsatser om cyberdiplomati, antagna av rådet den 10 februari 2015 (rådets dokument 6122/15)
    - rådets slutsatser om motverkande av hybridhot, antagna av rådet den 13 april 2016 (rådets dokument 7857/16)
    - kommissionens meddelande den 5 juli 2016 COM(2016) 410 final om att stärka Europas system för cyberresiliens och främja en konkurrenskraftig och innovativ cybersäkerhetsbransch
    - rådets slutsatser om den globala strategin för Europeiska unionens utrikes- och säkerhetspolitik, antagna av rådet den 17 oktober 2016 (rådets dokument 13202/16).

    Här bör också nämnas det av kommittén för utrikes- och säkerhetspolitik den 6 juni 2017 antagna utkastet till rådets slutsatser om en ram för ett gemensamt EU-diplomatiskt svar på skadliga cyberaktiviteter ("Cyberdiplomatiska verktygslådan") samt den omständighet att EU påbörjat arbetet med en översyn av 2013 års strategi för cybersäkerhet.

    Utvecklingslinjerna för samarbetet mellan Nato och EU på cyberområdet beskrivs dels av Areng, Liina: "International Cyber Crisis Management and Conflict Resolution Mechanisms", dels av Tiirmaa-Klaar, Helli: "Cyber Diplomacy: Agenda, Challenges, and Mission", båda i Ziolkowski, Katharina (red): *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations, and Diplomacy,* NATO Cooperative Cyber Defence Centre of Excellence, Tallinn 2013, s 574-580 [Areng] resp 509-531 [Tiirmaa-Klaar].
14. Se Brantley, Aaron Franklin: *The Decision to Attack. Military and Intelligence Cyber Decision-Making*, University of Georgia Press, Athens GA 2016, s 79-89. Motsatt åsikt hävdas av Schmitt, Michael N och Vihul, Liis: "Proxy Wars in Cyberspace: The Evolving International Law of Attribution", *Fletcher Security Review*, nr I:2 2014, s 56.
15. Det saknas ännu så länge internationellt överenskomna kriterier som skulle kunna tillämpas för ändamålet att en stat ska kunna tillräknas åtgärder vidtagna av icke-statliga aktörer. Jfr dock artiklar 4-11 i FN:s folkrättskommissions utkast till artiklar om staters ansvar för folkrättsstridiga handlingar jämte kommentaren till dessa artiklar i International Law Commission (utg): *Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries [2001]*, United Nations, New York 2008, s 40-54, *http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf* (2017-06-13). Jfr även Crawford, James: *State Responsibility. The General Part*, Cambridge University Press, Cambridge 2014 (första uppl, tredje tryckning), s 81-83.
16. Op cit, Schmitt, Michael N (red), se not 8, s 111-116. Till följd av förbudet i FN-stadgan mot hot om eller bruk av våld har motåtgärder en snävare innebörd än den äldre rättsfiguren repressalier. Medan en folkrättskonformt vidtagen motåtgärd ej får omfatta bruk av våld, kunde repressalieåtgärder omfatta handlingar, där militärt våld brukades.
17. Ibid, s 82-83.