# Stuxnet i folkrättslig belysning

*av Dirk Roland Haupt*

**Résumé**

Based on the case of the Stuxnet computer worm that allegedly targeted uranium enrichment infrastructure in Iran, this article discusses the legality of cyber operations as nuclear counter-proliferation measures. Legally assessing the implications of the creation, installation and control of the Stuxnet software is especially challenging because of the lack of detailed and reliable information relating to its origin, and the physical effects it caused outside the targeted supervisory control and data acquisition systems. Focusing on pertinent aspects in international law (such as: the use of force short of armed attack, preemptive self-defence, countermeasures short of use of force, the law of armed conflict, territorial sovereignty, customary international environmental law, and the principle of non-intervention in matters which are essentially within the domestic jurisdiction of any State), this article argues that the Stuxnet operation as such could constitute a countermeasure, which may or may not be lawful. This depends on how legal commentators assess the availability of feasible alternatives and the impact of the measure in relation to the threat posed by Iran's numerous and deliberate breaches of its obligations to comply with the 1968 Nuclear Nonproliferation Treaty and its safeguard agreements with the International Atomic Energy Agency.

OM ETT SABOTAGEPROGRAM även känt som datamasken W32.Stuxnet, inkom de första rapporterna den 17 juni 2010 då under beteckningen Rootkit.TmpHider.[1] I följden släpptes information om och prover av den skadliga koden till enskilda datasäkerhetsföretag som gjorde stora ansträngningar för att övervaka datatrafiken mellan masken och dess styrningsservrar samt för att förstå och kartlägga utformningen, funktionaliteten och syftet av detta mycket sofistikerade datorprogram.[2]

Av icke-lokala nätverks IP- och domänadresser som protokollförts kunde analytikerna sluta sig till att Stuxnet under tiden mellan juni 2009 och maj 2010 varit målinriktat på datorsystemen i fem anläggningar i Iran. I februari 2010 kunde datasäkerhetsföretaget Symantec samla in 3 280 prover på tre olika varianter av Stuxnet.[3] Datamasken påverkade vissa system för övervakning och styrning av storskaliga industriprocesser (s k Supervisory Control and Data Acquisition [SCADA] system) som utvecklats av företaget Siemens och som uppvisar specifika konfigurationskrav. Spridningen av Stuxnet bortom de datorsystem som datamasken initialt var riktad mot får sannolikt betraktas som en oavsiktlig bieffekt.[4] Det följer av Stuxnets arkitektur att det skapades för att kunna ändra koden för programmerbara styrsystem inom industriell automation i syfte att dels inverka på anläggningarnas verksamhet genom att manipulera system för kontroll av frekvensomvandlare och därmed att kunna bromsa upp eller accelerera motorerna, dels dölja sådana förändringar från respektive utrustnings operatör.[5] Även om de fem iranska anläggningar som varit målen för sabotageprogrammet inte officiellt avslöjades, gjorde otaliga medierapporter snart gällande att Stuxnet hade varit inriktat på

nukleär infrastruktur i Iran, i synnerhet på urananrikningsanläggningen i Natanz och på kärnkraftverket i Bushehr. Det misstänktes att hastigheten av IR-1-centrifugernas rotorer hade manipulerats i syfte att negativt påverka Irans nukleära program.[6]

Att göra en folkrättslig bedömning av konsekvenserna av att utveckla, installera och kontrollera Stuxnet framstår som en viss utmaning på grund av bristen på detaljerade och tillförlitliga uppgifter om datamaskens ursprung och de fysiska effekter den åstadkom utanför de SCADA-system som den varit riktad mot.

Stuxnet har kommit att kallas ”det första cybervapen som kommit till användning”.[7] Frågan har rests huruvida vissa staters underrättelsetjänster kan ha medverkat att utveckla denna skadliga kod.[8] Även om en analys av vem som gynnas av att skapa, installera och styra ett dylikt program mycket väl kan peka i riktning mot folkrättssubjekt som kan vara intresserade av att påverka Irans nukleära program,[9] så ger den inte tillräckligt med juridiskt hållbara indikatorer för att den skadliga cyberaktiviteten ska kunna tillräknas en bestämd individ, en konkret grupp av individer eller även en viss stat.[10]

En folkrättslig analys försvåras dessutom av den omständighet att det fortfarande är oklart huruvida Stuxnet faktiskt har vållat fysiska skador utanför de SCADA-system som det var riktat mot. Trots påståenden i medier och vetenskapliga härledningar[11] kan det inte anses vara styrkt bortom rimligt tvivel att Stuxnet verkligen inverkade på IR-1-centrifugernas eller andra komponenters fysiska integritet i Irans urananrikningsanläggning i Natanz, i kärnkraftverket i Bushehr eller i andra kärnanläggningar. Officiellt bekräftade iranska tjänstemän aldrig någon faktisk skada av fysisk natur orsakad av Stuxnet, och de yttranden som gjorts har snarare försökt bagatellisera dess effekter.[12] Rapporter om utbyte av ett påfallande stort antal centrifuger i anrikningsanläggningen i Natanz utgör inte bevis i juridisk mening för fysiska skador som en direkt följd av Stuxnet, i synnerhet med tanke på att det hade blivit känt långt innan att Iran brottade med mångahanda tekniska problem på senare år på grund av den använda utrustningens dåliga kvalitet, särskilt när det gäller en äldre centrifugmodell som i åratal uppvisat felfunktioner.[13]

## Folkrättsliga överväganden

Därför kan den folkrättsliga analysen av problemet med Stuxnets utveckling, installation, kontroll och verkan endast grundas på hypoteser, av vilka det antas att de med någon större sannolikhet kan ha inträffat på det förmodade sättet.

Om det förhöll sig så att en eller flera stater vore ansvariga[14] för utvecklingen, installationen och kontrollen av Stuxnet, skulle följande folkrättsliga aspekter vara relevanta: (1) bruk av våld som ej motsvarar väpnat angrepp; (2) förebyggande självförsvar; (3) motåtgärd som ej motsvarar bruk av våld; (4) väpnad konflikt; (5) territoriell suveränitet; (6) sedvanerättsliga principer i internationell miljörätt; (7) non-interventionsprincipen. De ska i det följande behandlas i tur och ordning.

## Bruk av våld som ej motsvarar väpnat angrepp

En fråga som ligger nära till hands är om installeringen och de uppgivna effekterna av datamasken Stuxnet skulle kunna kvalificeras som bruk av våld enligt FN-stadgans artikel 2:4.

Enligt den förhärskande uppfattningen i den folkrättsvetenskapliga doktrinen utgör

grundsatsen om förbudet mot hot om eller bruk av våld, som alla FN-medlemsstater ska rätta sig efter i sina internationella förbindelser, en tvingande norm enligt internationell sedvanerätt.[15] Emellertid fastslås härigenom inte mer än förbudets mest grundläggande innebörd, eftersom det annars knappast råder enighet i det internationella samfundet kring tolkningen[16] av begreppet ”våld”.[17] Detta kan ju innefatta en rad olika åtgärder; inte minst har det hävdats att det bl a omfattar politiskt och ekonomiskt tvång. Allt som allt leder dock en närmare granskning av artikel 2:4, sedd i dess sammanhang inom FN-stadgan, till slutsatsen att dess andemening och syfte samt dess tillkomsthistoria ger tydligt stöd åt en tolkning av våldsbegreppet som endast innebärande väpnat våld, d v s bruk av vapenmakt.[18] Denna slutsats understryks av ett flertal resolutioner antagna av FN:s generalförsamling, vilka inte framställer politiskt och ekonomiskt tvång som en uttrycksform för bruk av våld, utan snarare för principen om non-intervention i en annan stats inre angelägenheter.[19] Visserligen är dessa resolutioner inte folkrättsligt bindande. Men de kan anses relevanta såsom efterföljande praxis[20] av FN:s medlemsstater vid tolkningen och tillämpningen av artikel 2:4 i FN-stadgan. Denna slutsats har dessutom bekräftats av Internationella domstolen i sitt avgörande i det s k Nicaraguamålet år 1986, då domstolen inte behandlade ekonomiska tvångsåtgärder vidtagna av USA mot Nicaragua som bruk av våld, utan diskuterade dessa vid uttolkningen av non-interventionsprincipen.[21]

Även om det antas att Stuxnet negativt påverkade kvaliteten på en urananrikad slutprodukt av förmodligen högt ekonomiskt värde vid anläggningen i Natanz och att det hade en negativ inverkan på Irans kärnenergiprogram som en del av denna stats ekonomi, skulle sådan verkan inte tas med i beaktande med avseende på artikel 2:4 i FN-stadgan.

Emellertid råder det heller ingen enighet kring frågan om vilka åtgärder som skulle utgöra väpnat våld. Den av FN:s generalförsamling år 1974 antagna ”Definitionen av aggression”, som delvis återspeglar internationell sedvanerätt och som beskriver innebörden av det bredare aggressionsbegreppet som begagnas i artikel 39 i FN-stadgan,[22] åberopas ofta av folkrättssakkunniga och -praktiker när det gäller att bestämma innebörden av väpnat våld. Analysen av de handlingar som räknas upp i artikel 3 i Definitionen av aggression leder till slutsatsen att med bruk av vapenmakt ska förstås användning av konventionellt fysiskt våld genom en stats militära eller paramilitära styrkor mot en annan stats väpnade styrkor (inklusive handlingar utförda av individer eller grupper, om dessa kan tillräknas[23] en stat).

Enligt vedertagen uppfattning kräver bruk av vapenmakt att kinetiska vapen används. Vapen är verktyg för att åstadkomma kinetiska effekter av fysisk karaktär på en kropp eller ett föremål. Stuxnet var förmodligen ämnat åt att ändra, undertrycka, radera eller skicka data, men inte åt att omedelbart orsaka kinetiska effekter. Visserligen betraktas vissa stridsmedel som vapen, även om de inte frigör någon kinetisk energi. De främsta exempel härpå utgörs av biologiska eller kemiska ämnen. Deras bruk anses vara ett av vapenmakt, för även om de inte orsakar fysisk förstörelse, är de ämnade åt att orsaka död eller skada.[24] Detta betraktelsesätt, som är inriktat på verkan snarare än på medlen, motsvarar väl den i folkrätten förankrade synen att metodiskt utgå från åstadkommen verkan.[25] Således torde majoriteten bland folkrättssakkunniga anse att skadlig cyberverksamhet utgör bruk av vapenmakt om dess effekter är jämförbara

med kinetiska, biologiska eller kemiska vapen, d v s med sådana vapen som direkt eller indirekt orsakar dödsfall, kroppsskada eller förstörelse av egendom.[26]

Vissa folkrättsvetenskapliga författare gör gällande att ytterligare kriterier bör uppfyllas för att kunna kvalificera skadlig cyberverksamhet som bruk av vapenmakt, däribland kriteriet på hur allvarliga effekterna ter sig i verkligheten efter det att cyberaktiviteterna genomförts.[27] Denna ansats företräds i den år 2013 publicerade ”Tallinn-manualen i den på cyberkrigföring tillämpliga folkrätten” och utvecklas vidare i kommentaren till manualens regel 11.[28] Den däri utvecklade metoden utgår från att stater, som överväger att lansera cyberoperationer eller som blir till mål för sådana, i avsaknad av tydliga definitionsmässiga trösklar i hög grad är hänvisade till det internationella samfundets bedömning av om dylika operationer strider mot förbudet att bruka våld. Ansatsen består följaktligen i att staterna behöver en handledning för folkrättsligt belastningsbara bedömningar och därför sannolikt kommer att lägga stor vikt vid en uppsättning av kriterier och faktorer, när de kvalificerar vissa aktiviteter som bruk av våld, inte minst när det gäller cyberoperationer. Utan att i formellt hänseende utgöra folkrättsliga kriterier och utan att vara uttömmande, omfattar dessa faktorer för att bedöma ett visst händelseförlopp som bruk av våld bl a

- operationernas allvarlighetsgrad i skadehänseende,
- omedelbarheten av operationernas konsekvenser,
- operationernas direkthet, grad av inkräktande på målstaten och militära karaktär,
- utsträckningen av statlig inblandning som yppas i deras planläggning och utförande,
- mätbarheten av operationernas verkan och
- dessas presumtiva legalitet.[29]

Beroende på de därmed sammanhängande omständigheterna kommer staterna också att tillämpa andra kriterier – i en isolerad betraktelse eller i en samverkande syn –, såsom den rådande politiska omvärldsbilden, prognosen huruvida cyberoperationer bara förebådar ett framtida bruk av militärt våld, angriparens identitet, eventuella kunskaper om angriparens cyberverksamhet och målkategorierna (såsom t ex kritisk infrastruktur).[30]

Således beror bedömningen av om installationen, kontrollen och de påstådda effekterna av Stuxnet utgör bruk av vapenmakt i enlighet med artikel 2:4 i FN-stadgan på om datamasken utlöste ett händelseförlopp som ledde till en förstörelse av egendom av icketrivial omfattning. Det förblir oklart om sabotageprogrammet indirekt förstörde eller inverkade på den fysiska integriteten av (ett betydande antal) IR-1-centrifuger vid anrikningsanläggningen i Natanz eller vid andra kärnanläggningar i Iran.

Men även om fysiska effekter utanför de SCADA-system, som Stuxnet varit inriktat på, inte skulle vara fastställbara, skulle dess installering, styrning och förmodade följder ändå kunna anses utgöra bruk av vapenmakt om de utsatte kritiska infrastruktursystem i Iran för mycket påtaglig och kraftigt kännbar åverkan. Artikel 41 i FN-stadgan skulle inte motsäga en sådan slutsats, trots att bestämmelsen beskriver kritiska infrastruktursystems fullständiga eller partiella avbrott som av FN:s säkerhetsråd beslutade åtgärder, vilka ej innebär bruk av vapenmakt.[31]

Störningar av kritiska infrastruktursystem kan orsakas av att FN:s säkerhetsråd beslutar om inskridande medelst stridskrafter enligt artikel 42 i FN-stadgan (i stället för enligt artikel 41). Bland merparten av folkrättsexperterna råder dock enighet kring uppfattningen att avbrott av datornätverk som stöder kritiska infrastruktursystem endast kan anses vara bruk av vapenmakt om dessas effekter kan likställas med fysisk förstörelse.[32] Således kunde installeringen, styrningen och den förmenta verkan av Stuxnet anses utgöra bruk av vapenmakt bara under förutsättningen att de förorsakade mycket påtagliga och kännbara avbrott av ett eller flera kritiska infrastruktursystem i Iran (t ex av energiförsörjningsstrukturerna som sådana) på ett sådant sätt, att avbrotten skulle vara jämförbara med en fysisk förstörelse av anläggningarna och däri ingående system. Tills idag har Iran inte gjort gällande att dylika allvarliga effekter inträffat.[33]

En minoritet bland folkrättsjuristerna hävdar att förstörelse av data, som är av antingen stor vikt eller avsevärt ekonomiskt värde, bör betraktas som ett bruk av vapenmakt.[34] Denna uppfattning gör gällande att datamängder nuförtiden kan anses ha en betydelse helt i jämnhöjd med vad folkrätten tillmäter fysiska tillgångar. Bedömningen om installationen av Stuxnet då skulle vara att betrakta som bruk av vapenmakt är således beroende på om de raderade eller överskrivna datamängderna i SCADA-systemen varit av stort ekonomiskt värde eller haft väsentlig betydelse. Det hävdas följaktligen att det även inom ramen för artikel 2:4 i FN-stadgan bör tillämpas samma kriterier på och dras samma konsekvenser av radering av data av stort ekonomiskt värde eller väsentlig betydelse som om det vore fråga om fysisk förstörelse av föremål. Det kan dock ifrågasättas om datasabotage utan ytterligare fysisk verkan utanför de angripna datorsystemen skulle vara jämförbart med användning av kinetiska, biologiska eller kemiska vapen. Det skulle vara mycket svårt att i varje enskilt fall av skadlig cyberverksamhet avgöra om de saboterade datamängderna verkligen var av väsentlig betydelse eller i sanningen av ganska trivial natur. Enligt rapporterna ska Stuxnet ha varit inriktat på att frambringa ändringar av data i SCADA-systemen i en eller flera iranska kärnanläggningar. Radering av data är en naturlig del av ändringar av databestånd, vilka ligger till grund för överskrivningsförfaranden.

## Förebyggande självförsvar

Endast om installationen, kontrollen och de förmodade effekterna av Stuxnet motsvarar bruk av våld i enlighet med förbudet i artikel 2:4 i FN-stadgan, skulle det kunna övervägas om dessa cyberaktiviteter var rättfärdigade som självförsvarsåtgärder.

Enligt artikel 51 i FN-stadgan och tillämplig internationell sedvanerätt omfattas bruk av defensivt och proportionerligt militärt våld mot ett väpnat angrepp, lanserat av en annan stat (eller möjligen av icke-statliga aktörer), av rätten till självförsvar.[35] Även om det kan finnas situationer där det ter sig svårt att med bestämdhet fastlägga vad som faktiskt utgör ett väpnat angrepp,[36] så torde det i allmänhet inte råda något tvivel om att ett sådant föreligger i fall av direkt eller indirekt bruk av vapenmakt av betydande omfattning och verkan. I den folkrättsvetenskapliga litteraturen bekräftas en sedvanerättsligt gällande rätt till självförsvar i situationer, i vilka självförsvarets nödvändighet i enlighet med den s k Caroline- eller Webster-formeln är omedelbar och överväldigande samt är av sådan art att den ej heller lämnar ifrågavarande stat något val av medel eller något rådrum för överläggningar.[37]

Eftersom det inte finns några indikationer på ett väpnat angrepp eller ett överhängande väpnat angrepp från iransk sida mot någon annan stat, kommer endast läran om förebyggande självförsvar i betraktelse som grund för att rättfärdiga den cyberverksamhet som i Stuxnets skepnad riktats mot Irans kärntekniska anläggningar. Detta koncept kräver inte att ett väpnat angrepp faktiskt inträffat eller är omedelbart förestående, utan rätten till självförsvar utlöses, när hotet om ett väpnat angrepp växer fram, motåtgärder som ej motsvarar bruk av våld inte anses tillräckliga för att undanröja hotet och åtgärder beslutade av FN:s säkerhetsråd antingen inte förväntas eller inte förväntas vara effektiva.[38] De folkrättsjurister som stödjer detta koncept betonar behovet av att man effektivt ska kunna försvara sig mot angrepp från terrorister och stater som innehar massförstörelsevapen.[39] Kriteriet på ett omedelbart förestående väpnat angrepp kan emellertid vara relevant; det är lämpligt framför allt i samband med att en annan stat synbarligen mobiliserar sin försvarsmakt, samtidigt som möjligheten till ett effektivt försvar mot ett *angrepp med massförstörelsevapen* skulle hämmas eller omintetgöras, om självförsvarsåtgärden inte fick vidtas preventivt.[40] Emellertid avvisas dessa överväganden av andra som hävdar att en stats spekulativa oro om en annan stats möjliga framtida åtgärder inte kan likställas med ett väpnat angrepp.[41] Dessa sakkunniga hänvisar till artikel 39 i FN-stadgan, enligt vilken endast FN:s säkerhetsråd är behörigt att vidta åtgärder mot latenta hot mot internationell fred och säkerhet, ett konstaterande som stöds av Internationella domstolen i sitt avgörande 2005-12-19 i målet Kongo mot Uganda.[42]

Även om det finns enskilda fall av statspraxis[43] som skulle kunna anses utgöra exempel på förebyggande självförsvar, kan det inte hävdas att konceptet återspeglar gällande folkrätt. Det ska endast nämnas här att innehav av kärnvapen enligt Internationella domstolens rådgivande yttrande år 1996 om folkrättsenligheten av hot om eller bruk av kärnvapen i sig inte strider mot internationell sedvanerätt.[44] Följaktligen kan utvecklingen eller innehavet av massförstörelsevapen endast utgöra en kränkning av *fördragsenliga* skyldigheter, t ex av fördraget den 1 juli 1968 (SÖ 1970:12) om förhindrande av spridning av kärnvapen (icke-spridningsfördraget), som Iran ratificerade år 1970. Det är ganska tveksamt om enbart en sådan kränkning helt utan ytterligare omständigheter skulle utgöra ett framväxande hot om ett väpnat angrepp såsom det omslutes av konceptet för förebyggande självförsvar.

Marco Roscini har framfört den intressanta frågan om inte Stuxnet kunde rättfärdigas som en cyberoperation som förebygger spridningen av kärnvapen eller av vapenfähiga kärnladdningar.[45] Han besvarar frågan nekande på följande grunder: Fördragspartnerna i icke-spridningsfördraget har inte skadats av Irans bristande efterlevnad av avtalen med Internationella atomenergiorganet (IAEA) om kärnämneskontroll eller av relevanta säkerhetsrådsresolutioner och skulle heller inte skadas, om Iran bröt mot artikel II i icke-spridningsfördraget.[46] De verkar sålunda inte ha rätt att vidta motåtgärder enligt artikel 54 i FN:s folkrättskommissions utkast till artiklar om staters ansvar för folkrättsstridiga handlingar. Dessutom äger motåtgärder inte att utgöra brott mot förbudet mot hot om eller bruk av våld. Om Stuxnet utgjorde bruk av våld på grund av att datamasken hade fysiskt destruktiva konsekvenser, skulle åtgärden att installera och styra den vara folkrättsenligt endast om den användes i själv-

försvar mot ett väpnat angrepp från Iran. Emellertid utgör varken förvärvet eller utvecklingen av kärnvapen (och ännu mindre urananrikning) ett väpnat angrepp i enlighet med artikel 51 i FN-stadgan och med internationell sedvanerätt. Slutligen kan enligt Roscinis åsikt kapitel VII i FN-stadgan inte åberopas för att motivera åtgärden, då ingen av sanktionsresolutionerna som av säkerhetsrådet antagits mot Iran gör någon hänvisning till cyberverksamhet eller bemyndigar medlemsstaterna att använda ”alla nödvändiga medel” för att säkerställa efterlevnaden av icke-spridningsfördraget och av kontrollavtalen med IAEA.[47]

## Motåtgärd som ej motsvarar bruk av våld

Installationen, kontrollen och de förmodade effekterna av Stuxnet skulle vidare kunna diskuteras såsom utgörande en motåtgärd, d v s en handling som eljest strider mot folkrätten, men som skulle kunna vara rättfärdigad som reaktion på en annan stats folkrättsstridiga handling. Motåtgärdens syfte är att förmå den stat som handlat i strid med folkrätten att uppfylla sina internationella förpliktelser.[48]

Med tanke på förbudet mot hot om eller bruk av våld i internationella förbindelser samt staternas skyldighet, enligt artikel 2:3 i FN-stadgan och åtskilliga andra traktater,[49] att lösa sina internationella tvister med fredliga medel, är bara sådana motåtgärder lagliga som ej motsvarar bruk av våld.[50] Denna slutsats stöds av artiklarna 49 och 50:1:*a* i FN:s folkrättskommissions utkast till artiklar om staters ansvar för folkrättsstridiga handlingar, av flera resolutioner antagna av FN:s säkerhetsråd,[51] av den av FN:s generalförsamling enhälligt antagna ”Förklaringen om folkrättsliga principer rörande vänskapliga förbindelser och samarbete i enlighet med Förenta Nationernas stadga” (den s k ”Friendly Relations”-deklarationen)[52] samt av Internationella domstolens rättskipning.[53] Därför skulle installationen, kontrollen och de antagna effekterna av Stuxnet endast anses som laglig motåtgärd om den ej motsvarar bruk av våld i enlighet med artikel 2:4 i FN-stadgan.

För att kunna åberopas som rättmätighetsgrund måste en motåtgärd även uppfylla vissa andra kompletterande förutsättningar.[54] I samband med Stuxnet förtjänar två av dessa förutsättningar att granskas närmare: För det första måste en rättmätig motåtgärd vidtas som reaktion på en tidigare folkrättsstridig handling utförd av eller tillräknelig den stat som motåtgärden riktas emot. För det andra måste den stat som vidtar motåtgärden ha åsamkats skada som en följd av den folkrättsstridiga handlingen.

Huruvida dessa förutsättningar är uppfyllda beror på om Iran har begått en folkrättsstridig handling mot en eller flera stater som installerade och styrde Stuxnet. Irans internationella förpliktelser enligt icke-spridningsfördraget gäller endast i förhållande till de stater som är part i traktaten; internationella förpliktelser i fråga om IAEA:s inspektioner består endast gentemot detta organ. Om Stuxnet således installerats och styrts av en eller flera stater, skulle det vara svårt att hävda att Iran skadade denna stat eller dessa stater genom att bryta mot eller inte fullgöra sina skyldigheter enligt icke-spridningsfördraget.

Med tanke på att motåtgärden ska förmå den stat som handlat i strid med folkrätten att uppfylla sina internationella förpliktelser, skulle också ett koncept av förebyggande motåtgärder vara tänkbart. Ett sådant skulle på sätt och vis återspegla aspekter av läran om förebyggande självförsvar, dock med en avgörande skillnad: Medan fö-

rebyggande självförsvar omsluter bruk av våld för att förhindra ett framtida väpnat angrepp, skulle en förebyggande motåtgärd ej omfatta bruk av våld och i stället syfta till att förebygga förväntade framtida folkrättsstridiga handlingar som ej utgör väpnade angrepp. Endast inom ramen för dylika rent teoretiska överväganden skulle det finnas rum att överväga om inte installationen och kontrollen av Stuxnet skulle kunna utgöra en förebyggande motåtgärd vidtagen mot Iran i syfte att förhindra ytterligare kränkningar av icke-spridningsfördraget, allra främst genom att utveckla kärnvapen. Emellertid har detta koncept varken åberopats av någon stat eller utvecklats i folkrättslig doktrin.

## Väpnad konflikt

En folkrättslig belysning av Stuxnet kan inte undvika frågan huruvida programmets installation och styrning liksom de effekter, som det påstås ha förorsakat, kan ha lett till en internationell väpnad konflikt mellan Iran och den eller de stater som är ansvariga för den här aktuella cyberverksamheten.

Frågan är av betydelse, eftersom en internationell väpnad konflikt utlöser tillämpligheten av krigets lagar, d v s av humanitär folkrätt,[55] mellan parterna i konflikten i enlighet med den gemensamma artikeln 2 i 1949 års Genèvekonventionerna I–IV (SÖ 1953:14–17).[56] I och med att en internationell väpnad konflikt råder gör sig dessutom neutralitetsrättsliga överväganden gällande.

Enligt den rådande uppfattningen uppstår en internationell väpnad konflikt, när en eller flera stater tillgriper vapenmakt mot en annan stat, oavsett lagligheten, skälen eller t o m intensiteten av denna konfrontation.[57] Denna uppfattning bekräftas av kommentaren till Genèvekonventionerna, där det sägs att ”varjehanda motsättning som uppstår mellan två stater och leder till ingripande av väpnade styrkor är en väpnad konflikt enligt artikel 2”.[58] Följaktligen föreligger en internationell väpnad konflikt, när stater brukar väpnat våld mot varandra, och därmed blir krigets lagar tillämpliga.

Begreppet ”bruk av vapenmakt”, vilket medför att stater befinner sig i en internationell väpnad konflikt, måste tydligt skiljas från begreppet ”bruk av (väpnat) våld” i enlighet med artikel 2:4 i FN-stadgan. Det förra uttrycket hänvisar till *jus in bello* som rör den i väpnade konflikter tillämpliga rätten vid utövande av fientligheter och därmed spörsmålet, hur våld folkrättskonformt kan användas inom ramen för en väpnad konflikt, medan det senare är en aspekt av *jus ad bellum*, som avser de folkrättsliga regler, som gäller med avseende på rätten att tillgripa militärt våld. Emellertid är de två termerna nära besläktade. Närhelst en stats handlingar gentemot en annan stat är att anse som bruk av vapenmakt såsom det förstås enligt *jus ad bellum*, indikerar detta ett utbrott av fientligheter på höjd med bruk av våld såsom det förstås enligt *jus in bello* och således att tröskeln till en väpnad konflikt nåtts. Dock har det framhållits att detta konstaterande inte gäller ett snabbt, diskret och närmast ”kirurgiskt” bruk av vapenmakt genom en stat utan ytterligare reaktioner från den stat som bruket av vapenmakten riktas emot (t ex de rapporterade bombardemangen av kärnreaktorn i Osirak i Irak år 1981 eller i Dair Alzour i Syrien år 2007 genom det israeliska flygvapnets försorg).[59]

Då Stuxnet uppges ha påverkat komponenter i Irans kärntekniska anläggningar mellan juni 2009 och april 2010, d v s under en avsevärd tid, kan inte dess installering och styrning beskrivas som en snabb och kirurgisk åtgärd. Därför beror svaret på frågan huruvida installationen och kontrollen

av Stuxnet liksom de effekter, som det påstås ha förorsakat, kan ha lett till en internationell väpnad konflikt mellan Iran och den eller de stater som är ansvariga för datamaskens installation och kontroll på om dessa åtgärder anses utgöra bruk av våld enligt artikel 2:4 i FN-stadgan.

## Territoriell suveränitet

I tillägg till det hittills förda resonemanget finns det anledning att begrunda om installationen och kontrollen av Stuxnet liksom de effekter, som det påstås ha förorsakat, utgör en kränkning av Irans territoriella suveränitet.

Principen om territoriell suveränitet måste skiljas från principen om suverän integritet. Medan den senare kränks när en stat brukar folkrättsstridigt våld på en annan stats territorium, innebär territoriell suveränitet att statens myndigheter har ett maktmonopol inom territoriet, d v s att ingen stat äger utöva jurisdiktion inom en annan stats territorium utan den senares medgivande.[60] Således anses verksamhet av utländska myndighetsföreträdare inom territoriet vara utövande av jurisdiktion som är oförenligt med den berörda statens territoriella suveränitet, och därmed vara folkrättsstridig. För att kränka principen om territoriell suveränitet måste den verkan som orsakas av denna stat på en annan stats territorium vara av antingen fysisk art eller förnimbar som myndighetsutövande av en utländsk stat – helt oansett, vilken omfattning eller intensitet dessa handlingar må ha.[61] Med detta i åtanke skulle man i ett perspektiv inriktat på utövande av en främmande stats myndighet kunna hävda att betydande försämring eller manipulering av datasystemverksamhet genom utländska myndighetsrepresentanter har förmågan att orsaka skönjbara effekter.

Det är fortfarande oklart om Stuxnet åstadkommit fysiska eller förnimbara effekter utanför de SCADA-system det var riktat emot, t ex genom att skada IR-1-centrifugerna i urananrikningsanläggningen i Natanz. Det är heller inte känt om manipuleringen av den datorstyrda driften av IR-1-centrifugerna och i synnerhet deras hastighet verkligen var av betydande omfång.

## Sedvanerättsliga principer i internationell miljörätt

Även om internationellt miljöskydd i huvudsak är traktaträttsligt reglerat, finns det några miljörelaterade regler som erkänns som en del av internationell sedvanerätt. En av dessa grundläggande sedvanerättsliga regler ålägger staterna att inte avsevärt skada den naturliga miljön utanför deras egen behörighet.[62] Denna skyldighet grundar sig på det allmänna antagandet att den territoriella suveräniteten av en stat som tillfogar miljön skador på sitt eget territorium begränsas av den således påverkade statens territoriella integritet. Förbudet att orsaka gränsöverskridande miljöskador uttrycks i talrika traktater[63] och i många staters deklarerade rättsövertygelser samt stöds av Internationella domstolens rättskipning.[64]

Det finns f n inga rapporter om eventuella miljöskador på iranskt territorium som kan ha orsakats av effekterna av installationen och styrningen av Stuxnet-masken.[65]

Emellertid kan det finnas skäl att överväga huruvida Stuxnets installering i iranska kärnanläggningars driftsystem skulle kunna anses ha medfört betydande miljöfara. Trots att FN:s folkrättskommissions år 2001 antagna utkast till artiklar om förebyggande av gränsöverskridande skador från farliga verksamheter[66] anger att det endast finns en skyldighet att minimera risken för gränsöver-

skridande skada (artikel 3), är det allmänt accepterat inom den folkrättsvetenskapliga doktrinen att det inte är tillåtligt enligt internationell sedvänja att framkalla betydande gränsöverskridande risk för skador på den naturliga miljön (när såväl detta är mycket troligt som det finns risk för mycket allvarliga konsekvenser).[67]

Utan detaljerade tekniska kunskaper och precis information om de potentiellt negativa effekterna Stuxnet kan ha haft på operativsystemen för Irans kärntekniska anläggningar och den potentiella fara som masken kan ha utgjort för den naturliga miljön är det omöjligt att bedöma den möjliga faran för miljöskador.

## Non-interventionsprincipen

Om man ponerar att Stuxnet skapades, installerades och styrdes av en eller flera stater, kan den sedvanerättsliga principen om non-intervention i en annan stats interna angelägenheter, en logisk följd av principen om staters suveräna likställdhet, bli tillämplig. Principen är traktatfäst i artikel 2:7 i FN-stadgan med avseende på FN-organ samt i vissa regionala fördrag.[68] Vidare återspeglas den i vissa staters deklarationer[69] och i resolutioner antagna av FN:s generalförsamling.[70] Dessutom har Internationella domstolen bekräftat att denna princip utgör en beståndsdel av internationell sedvanerätt.[71]

En otillåten inblandning äger rum när en stat i syfte att tvinga en annan stat till ett visst beteende inkräktar på den senares inre eller yttre angelägenheter, d v s på dennas rätt till maktutövning (*domain réservé*).[72]

Allmänt sett kan det hävdas att en stats inre angelägenheter omfattar alla dessa frågor som inte regleras av internationella normer. Det kan diskuteras om installationen och kontrollen av Stuxnet och den efterföljande återverkan på Irans nukleära program skulle utöva inflytande på en inhemsk angelägenhet i Iran. Sedan år 1958 har Iran varit medlem i IAEA. I november 2010 hade IAEA 151 medlemmar, vilket motsvarar c:a 80 % av det internationella statssamfundet. År 1970 ratificerade Iran icke-spridningsfördraget, vilket gör Irans kärnprogram till föremål för IAEA:s kärnämneskontroll och verifikationer. I skrivande stund är 189 stater parter i detta nästintill universella fördrag. Följaktligen kan det ifrågasättas om Irans kärnprogram är en fråga om inre angelägenheter eller snarare en fråga av internationaliserad karaktär som inte omfattas av Irans *domain réservé*.[73]

Vid en närmare granskning uppvisar Stuxnet-operationen de klassiska förutsättningarna för att kvalificeras som intervention. Den utövade ett visst mått av tvång[74] och syftade till att hindra en stat från att fortsätta följa en bestämd handlingslinje. Denna betraktelse får inte sammanblandas med frågan om ifrågavarande stats politik var ett folkrättsenligt tillvägagångssätt eller inte, då detta spörsmål rör ett annat sakförhållande. Med hänsyn till operationens uppläggning, struktur och komplexitet ligger det nära till hands att anta att den utfördes av en stat eller av stater i samverkan snarare än av en grupp individer. Den överskred inte tröskeln till ett väpnat angrepp, eftersom den inte ledde till mänskliga offer, betydande långsiktiga skador eller störningar av kritisk infrastruktur, d v s av infrastruktur av avgörande betydelse för statens funktionsduglighet. Operationen kan mycket väl ha utgjort bruk av våld utan att överskrida tröskeln till ett väpnat angrepp, ty enligt uppgift lär den ha orsakat en viss materiell skada och var tillräckligt intrusiv för att eventuellt ses som ett bruk av våld av vissa folkrättsliga kommentatorer, även om uttalandena från den iranska regeringen

inte innehöll referenser till *jus ad bellum*.[75] Trots att enstaka röster ur regeringsapparaten velat göra gällande annat, har den iranska regeringen inte hävdat att operationen var att likställa med bruk av våld eller att den t o m utgjorde ett väpnat angrepp.

Det är en öppen fråga, om installeringen, styrningen och de angivna effekterna av Stuxnet var en folkrättsenlig form av intervention. Å ena sidan ledde operationen uppenbarligen till att ifrågavarande stat fick fatta inrikespolitiska beslut, som den annars inte skulle ha fattat, och till att den åtminstone tillfälligt hindrades från att utföra kärnteknisk forskning för vad som uppgavs vara fredliga ändamål.[76] Å andra sidan rådde allvarliga tvivel om den rent icke-militära karaktären och inriktningen av Irans nukleära politik, och det fanns tydliga tecken på att Iran som fördragspart har handlat i strid med icke-spridningsfördragets regim.[77] Denna stat har onekligen systematiskt vägrat att samarbeta eller har undanglidit diplomatiska ansträngningar för att försöka förmå den att uppfylla dess förpliktelser enligt icke-spridningsfördraget. Som sådan skulle Stuxnet-operationen kunna utgöra en motåtgärd, som är folkrättskonform eller ej, beroende på hur man bedömer tillgängligheten av lämpliga alternativ och åtgärdens verkan i förhållande till det proliferationshot som Irans bristande uppfyllelse av de gällande bestämmelserna på icke-spridningens område har utlöst.[78]

Katharina Ziolkowski[79] diskuterar huruvida Stuxnet utgjorde ekonomiskt tvång eller ett brott mot non-interventionsprincipen och drar slutsatsen att det är tveksamt om Stuxnet-operationen bröt mot den senare principen. Slutsatserna uppnås till stor del genom en tolkning av punkterna 244 och 245 i Nicaraguamålet,[80] i vilka Internationella domstolen avvisade Nicaraguas påstående att USA brutit mot non-interventionsprincipen som en följd av vissa ekonomiska åtgärder som införts av USA:s regering (nedskärning av ekonomiskt bistånd, minskade importkvoter för socker och införande av ett handelsembargo). Det är åtminstone inte alldeles uppenbart att detta också bevisar att Stuxnet inte skulle kunna kvalificeras som en form av intervention, framför allt med tanke på att det knappast finns någon likhet mellan de ekonomiska åtgärder som varit föremål för domstolens avgörande i Nicaraguamålet och installationen och styrningen av ett sabotageprogram i iranska kärncentrifuger, vilket enligt uppgift resulterat i att de kan ha åsamkats viss fysisk skada.

När det gäller de av USA:s regering vidtagna ekonomiska åtgärder som påtalats i Nicaraguamålet, rör det sig till stor del om retorsioner[81] (nedskärning av bistånd, minskade importkvoter) som inte bröt mot någon rättslig skyldighet, medan ett selektivt – och potentiellt folkrättsstridigt – handelsembargo förmodligen av Internationella domstolen inte hade bedömts nå upp till den nödvändiga nivån av tvång för att utgöra en intervention, även om det orsakat ekonomisk skada eller uttryckte ogillande av Nicaraguas politik. I motsats därtill var Stuxnet inte utformat på ett sätt att orsaka ekonomisk skada eller att uttrycka politiskt ogillande, men för att förhindra eller fördröja den av den iranska regeringen valda politiska handlingslinjen när det gäller att bedriva kärnteknisk forskning för påstått fredliga ändamål.

## Slutsats

Eftersom fakta om Stuxnet delvis fortfarande är oklara, kan den folkrättsliga analysen av datorprogrammets skapelse, installation, styrning och effekter baseras på enbart antaganden. Det finns starka skäl för

att nå slutsatsen att Iran har agerat i strid med icke-spridningsfördragets system och att Stuxnet kan kvalificeras som en motåtgärd, folkrättskonform eller ej. Det väsentliga för den i detta bidrag förda diskussionen är emellertid att Stuxnet-operationen var en åtgärd som innebar tvång, avsedd att hindra staten från att utföra en vald politisk handlingslinje, och eftersom den sannolikt vidtagits av en eller flera stater mot en annan kan den på tillräckliga grunder kvalificeras som en form av intervention, om än en som efter allt att döma är försvar- och godtagbar.

De som utvecklade, installerade och styrde Stuxnet vidtog i vart fall långtgående åtgärder för att förhindra eller åtminstone för att minimera oavsiktliga skador på andra mål än urananrikningsanläggningen i Natanz:[82]

1) Datamasken aktiverades endast inom miljön av den specifika Siemensprogramvara som användes i Natanz.
2) Varje infekterad dator kunde sprida sabotageprogrammet till endast tre andra datorer.[83]
3) Även när en dator var smittad, självreplikerade datamasken inte i tillräckligt hög utsträckning för att hämma datorfunktioner och åstadkom därför bara hanterbara störningar.
4) Programmet innehöll ett kommando som deaktiverade datamasken den 24 juni 2012.

Författaren är jur lic.

## Noter

1. Knapp, Eric D och Langill, Joel Thomas: *Industrial Network Security. Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems*, Syngress, Waltham 2015 (andra uppl), s 301.
2. Falliere, Nicolas; O'Murchu, Liam; Chien, Eric: "W32. Stuxnet Dossier. Version 1.4 (Februari 2011)", Symantec, Cupertino 2011, s 4, *http://www.cse.psu.edu/~smclaugh/cse598e-f11/papers/falliere.pdf* (2015-07-05).
3. Ibid, s 7.
4. Ibid, s 2, 4-7.
5. Ibid, s 39-43.
6. Zettler, Kim: *Countdown to Zero Day. Stuxnet and the Launch of the World's First Digital Weapon*, Crown, New York 2014, s 195, 245-246; Barzashka, Ivanka: "Are Cyber-Weapons Effective? Assessing Stuxnet's Impact on the Iranian Enrichment Programme", *The RUSI* [Royal United Services Institute for Defence and Security Studies] *Journal*, band 158, 2. häftet 2013, s 50, *http://www.tandfonline.com/doi/pdf/10.1080/03071847.2013.787735* (2015-07-05).
7. Op cit, Zettler, Kim, se not 6, s 52, 404-405; Ziolkowski, Katharina: "Stuxnet – Legal Considerations", *Humanitäres Völkerrecht – Informationsschriften | Journal of International Law of Peace and Armed Conflict*, 3. häftet 2012, s 140.
8. Op cit, Zettler, Kim, se not 6, s 65-68, 187-188, 247-248.
9. Om Irans nukleära program se Bernstein, Jeremy: *Nuclear Iran*, Harvard University Press, Cambridge MA/London 2014, s 76-93 och 153-190.
10. Foltz, Andrew C: "Stuxnet, Schmitt Analysis, and the Cyber 'Use-of-Force' Debate", *Joint Forces Quarterly*, 4. häftet 2012, s 44, *http://www.au.af.mil/au/awc/awcgate/jfq/foltz_stuxnet_schmitt_oct2012.pdf* (2015-07-05); Roscini, Marco: "Cyber Operations as Nuclear Counterproliferation Measures", *Journal of Conflict and Security Law*, 1. häftet 2014, s 134. Motsatt åsikt före-

träds av Gill, Terry D: ”Non-Intervention in the Cyber Context”, i Ziolkowski, Katharina (utg): *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy*, NATO Cooperative Cyber Defence Centre of Excellence, Tallinn 2013, s 235.

11. Geers, Kenneth; Kindlund, Darien; Moran, Ned; Rachwald, Rob: *World War C: Understanding Nation-State Motives Behind Today's Advanced Cyber Attacks*, FireEye, Milpitas 2014, s 14, *http://www.fireeye.com/resources/pdfs/fireeye-wwc-report.pdf* (2015-07-05). Se även Schmitt, Michael N, och Vihul, Liis: ”Proxy Wars in Cyber Space: The Evolving International Law of Attribution”, *Fletcher Security Review*, 2. häftet 2014, s 55.
12. Vid ett högnivåmöte om bekämpning av nukleär terrorism den 28 september 2012 kritiserade Irans utrikesminister Ali Akbar Salehi i allmänna ordalag de cyberangrepp som hade riktats mot iranska kärnanläggningar, vilka han beskrev som ”manifestation av nukleär terrorism och därmed en allvarlig kränkning av principerna i FN-stadgan och folkrätten”. Han relaterade inte dessa till urananrikningsanläggningen i Natanz eller till någon annan kärnanläggning i Iran. Se ”Statement by H. E. Dr. Ali Akbar Salehi, Minister of Foreign Affairs of the Islamic Republic of Iran, at the High Level Meeting on Countering Nuclear Terrorism (New York, 28 September 2012)”, *http://iran-un.org/en/2012/09/28/28-september-2012-2/* (2015-07-05). Jfr även Kerr, Paul K; Rollins, John och Theohary, Catherine A: *The Stuxnet Computer Worm. Harbinger of an Emerging Warfare Capability*, Congressional Research Service, Washington 2010, s 3-5.
13. Op cit, Ziolkowski, Katharina, se not 7, s 140.
14. Op cit, Gill, Terry D, se not 10, s 235.
15. Bring, Ove och Mahmoudi, Said: *Internationell våldsanvändning och folkrätt*, Norstedts Juridik, Stockholm 2006, s 19. Se även Brown, Gary och Poellet, Keira: ”The Customary International Law of Cyberspace”, *Strategic Studies Quarterly*, band 6, 3. häftet 2012, s 126-145.
16. Op cit, Bring, Ove och Mahmoudi, Said, se not 15, s 16-19.
17. Randelzhofer, Albrecht och Dörr, Oliver: ”Article 2(4)”, i Simma, Bruno; Khan, Daniel-Erasmus; Nolte, Georg; Paulus, Andreas (utg): *The Charter of the United Nations. A Commentary*, band I, Oxford University Press, Oxford/New York 2012 (tredje uppl), s 208-213 §§ 16-28.
18. Dörr, Oliver: ”Use of Force, Prohibition of”, i Wolfrum, Rüdiger (utg): *The Max Planck Encyclopedia of Public International Law* (citeras i det följande som *MPEIL*), band X, Oxford University Press, Oxford/New York 2012, s 609 f §§ 12-13.
19. Jfr exempelvis (1) första principen i Förklaringen om folkrättsliga principer rörande vänskapliga förbindelser och samarbete i enlighet med Förenta Nationernas stadga (den s k ”Friendly Relations”-deklarationen; bilagan till den av FN:s generalförsamling den 24 oktober 1970 antagna resolutionen 2625 [XXV]) att staterna ska i sina internationella förbindelser avhålla sig från hot om eller bruk av våld, vare sig det är riktat mot någon annan stats territoriella integritet eller politiska oberoende eller på annat sätt oförenligt med Förenta Nationernas ändamål, (2) operativa §:en 2 i Förklaringen om otillåtligheten att ingripa i staters inrikes angelägenheter och om skyddet av dessas oberoende och suveränitet (FN:s generalförsamlings resolution 2131 [XX] den 21 december 1965), (3) principerna 2:I:*b* och 2:II:*a* i Förklaringen om otillåtligheten att ingripa och att blanda sig i staters inre angelägenheter (bilagan till den av FN:s generalförsamling den 9 december 1981 antagna resolutionen 36/103) samt (4) § 1:I:8 i Förklaringen om att förbättra effektiviteten av principen om att avhålla sig från hot om eller bruk av våld i internationella förbindelser (bilagan till den av FN:s generalförsamling den 18 november 1987 antagna resolutionen 42/22).
20. Efterföljande praxis utgör ett tolkningskriterium enligt artikel 31:3:*b* i Wienkonventionen den 23 maj 1969 (SÖ 1975:1) om traktaträtten. Se närmare härom Linderfalk, Ulf: *Om tolkningen av traktater*, Lunds universitet, Lund 2001, s 194-201.
21. International Court of Justice [ICJ]: *”Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America): Merits. Judgment of June 27, 1986”*, ICJ Reports of Judgments, Advisory Opinions and Orders 1986, s 126 § 245, *http://www.icj-cij.org/docket/files/70/6503.pdf* (2015-07-05) (citeras i det följande *Nicaraguamålet*).

22. Bilagan till den av FN:s generalförsamling den 14 december 1974 antagna resolutionen 3314 (XXIX). Se närmare härom Bring, Ove: *Aggression, självförsvar och non-intervention. Tre studier i internationell rätt*, Iustus, Uppsala 1982, s 9-21.
23. 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* (2015-07-05). Jfr även Kees, Alexander: "Responsibility of States for Private Actors", i op cit, *MPEIL*, se not 18, band VIII, s 961-964 §§ 11-22 och 25, och Crawford, James: *State Responsibility. The General Part*, Cambridge University Press, Cambridge 2014 (första uppl, tredje tryckning), s 81-83.
24. Diniss, Heather Harrison: *Cyber Warfare and the Laws of War*, Cambridge University Press, Cambridge 2012, s 59-61.
25. Brownlie, Ian: *International Law and the Use of Force by States*, Oxford University Press, Oxford 1991, s 362; Hellman, Cecilia: *IT-krigets lagar*, Försvarshögskolan, Stockholm 2004, s 32 f.
26. Dinstein, Yoram: "Computer Network Attack and Self-Defense", i Schmitt, Michael N, och O'Donnell, Brian T (utg): *Computer Network Attack and International Law*, Naval War College, Newport 2002, s 103.
27. Redan år 1999 hävdade professor Michael N Schmitt i artikeln "Computer Network Attacks and the Use of Force in International Law: Thought on a Normative Framework", *Columbia Journal of Transnational Law*, band 37, 3. häftet 1999, s 914 f, att en differentierad uppsättning av kriterier bör formuleras som ska vara inriktad på sannolikheten att staterna kommer att kvalificera en cyberoperation som bruk av våld.
28. Schmitt, Michael N (utg): *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press, Cambridge 2013, s 48-51. Se även Dinstein, Yoram: "International Humanitarian Law and Modern Warfare", i Byström, Karin (utg): *International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law, 17–19 November 2004, Stockholm, Sweden. Proceedings of the Conference*, Försvarshögskolan, Stockholm 2004, s 19 f.
29. Op cit, Dinniss, se not 24, s 63 f; op cit, Foltz, Andrew C, se not 10, s 42 f; op cit, Hellman, Cecilia, se not 25, s 33. Se även Wingfield, Thomas C: "CNA and the Jud ad Bellum: An Introduction", i op cit, Byström, Karin (utg), se not 28, s 97-100; Palojärvi, Pia: *A Battle in Bits and Bytes. Computer Network Attacks and the Law of Armed Conflict*, Erik Castrén Institute of International Law and Human Rights, Helsingfors 2009, s 62-74.
30. Tallinn-manualens metod kritiseras av Fleck, Dieter: "Searching for International Rules Applicable to Cyber Warfare – A Critical First Assessment of the New *Tallinn Manual*", *Journal of Conflict and Security Law*, 2. häftet 2013, s 336 f, med argumentet att den inte är lämplig för att besvara huvudfrågan, nämligen om ett cyberanfall är en operation som inte når upp till tröskeln av bruk av våld eller som utgör ett bruk av våld eller som t o m är att betrakta som ett bruk av våld som ska likställas med ett väpnat angrepp.
31. Schulze, Sven-Henrik: *Cyber-„War" – Testfall der Staatenverantwortlichkeit*, Universität Trier, Trier 2014, s 114 f ; Woltag, Johann-Christoph: "Cyber Warfare", i op cit, *MPEIL*, se not 18, band II, s 990 § 8, gör gällande att artikel 41 i FN-stadgan snarare avser ekonomiska åtgärder såsom sanktioner eller embargon.
32. Op cit, Woltag, Johann-Christoph, se not 31, s 990 § 8.
33. Se även op cit, Barzashka, Ivanka, se not 6, s 52 f.
34. Barkham, Jason: "Information Warfare and International Law on the Use of Force", *New York University Journal of International Law and Politics*, band 34, 1. häftet 2001, s 88.
35. Shaw, Malcolm N: *International Law*, Cambridge University Press, Cambridge 2014 (sjunde uppl), s 820-829. Se även Ruys, Tom: *"Armed Attack" and Article 51 of the UN Charter. Evolutions in Customary Law and Practice*, Cambridge University Press, Cambridge 2013, s 91-125 och 528-532;

Valo, Janne: *Cyber Attacks and the Use of Force in International Law*, Helsingfors universitet, Helsingfors 2014, s 57-62.

36. För en mycket åskådlig behandling av detta problem se Bring, Ove: *FN-stadgan och världspolitiken. Om folkrättens roll i en föränderlig värld*, Norstedts Juridik, Stockholm 2011 (fjärde uppl), s 156-186.
37. Noyes, John E: "'The Caroline': International Law Limits on Resort to Force", i Noyes, John E; Dickinson, Laura A; Janis, Mark W (utg): *International Law Stories*, Foundation Press, New York 2007, s 263-305.
38. Greenwood, Christopher: "Self-Defence", i op cit, *MPEIL*, se not 18, band IX, s 111-113 §§ 41-51. Jfr även Stürchler, Nikolas: *The Threat of Force in International Law*, Cambridge University Press, Cambridge 2009, s 252-274.
39. Sofaer, Abraham D: "On the Necessity of Pre-emption", *European Journal of International Law*, 2. häftet 2003, s 214.
40. Se Haupt, Dirk Roland: "Ballistiskt missilförsvar i Europa och folkrätten. Jus ad bellum, jus in bello och staters folkrättsliga ansvar ex delicto", *KKrVAHT*, 4. häftet 2014, s 63-67.
41. Ziolkowski, Katharina: "General Principles of International Law as Applicable in Cyberspace", i op cit, Ziolkowski, Katharina (utg), se not 10, s 160-161 jämte not 194 på s 160; Eek, Hilding; Bring, Ove; Hjerner, Lars: *Folkrätten.* Norstedts, Stockholm 1987 (fjärde uppl), s 300.
42. International Court of Justice [ICJ]: *Case Concerning Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda)*, ICJ Reports of Judgments, Advisory Opinions and Orders 2005, s 59 f § 148, *http://www.icj-cij.org/docket/files/116/10455.pdf* (2015-07-05).
43. Gray, Christine: "The US *National Security Strategy* and the New 'Bush Doctrine' on Preemptive Self-defense", *Chinese Journal of International Law*, 2. häftet 2002, s 440-444, *http://chinesejil.oxfordjournals.org/content/1/2/437.full.pdf* (2015-07-05).
44. International Court of Justice [ICJ]: *Advisory Opinion of July 8, 1996, on 'Legality of the Threat or Use of Nuclear Weapons'*, ICJ Reports of Judgments, Advisory Opinions and Orders 1996, s 267 § 105(2)(F), *http://www.icj-cij.org/docket/files/95/7495.pdf* (2015-07-05) (citeras i det följande *Rådgivande yttrande om lagligheten av hot om eller bruk av kärnvapen*).
45. Op cit, Roscini, Marco, se not 10, s 157.
46. Artikel II lyder:
Varje icke-kärnvapenstat som är fördragspart förbinder sig att icke från någon som helst överlåtare mottaga kärnvapen eller andra kärnladdningar eller kontroll över sådana vapen eller laddningar, vare sig direkt eller indirekt; att icke tillverka eller på annat sätt förvärva kärnvapen eller andra kärnladdningar; samt att icke söka eller mottaga något bistånd för tillverkning av kärnvapen eller andra kärnladdningar.
47. Op cit, Roscini, Marco, se not 10, s 157.
48. Bring, Ove: *FN-stadgans folkrätt*, Norstedts Juridik, Stockholm 1992, s 275.
49. Här bör främst nämnas konventionen den 18 oktober 1907 (SFS 1910:153) för avgörande på fredlig väg af internationella tvister, artikel II i det internationella fördraget den 27 augusti 1928 (SÖ 1929:23) rörande fördömande av krig samt konventionen den 26 december 1933 rörande staters rättigheter och skyldigheter (den s k Montevideokonventionen).
50. Op cit, Brownlie, Ian, se not 25, s 281 f. Se även Franck, Thomas M: *Recourse to Force. State Actions Against Threats and Armed Attacks*, Cambridge University Press, Cambridge 2004, s 131-134.
51. Jfr i synnerhet följande resolutioner: (1) operativa §:en A:1 i resolutionen 101 (1953), antagen den 24 november 1953; (2) operativa §:en 2 i resolutionen 111 (1956), antagen den 19 januari 1956; (3) operativa §:en 2 i resolutionen 171 (1962), antagen den 9 april 1962; (4) operativa §:en 1 i resolutionen 188 (1964), antagen den 9 april 1964; (5) fjärde §:en i ingressen till samt operativa §:en 3 i resolutionen 270 (1969), antagen den 26 augusti 1969.
52. Se ovan not 19, nr (1).
53. International Court of Justice [ICJ]: (1) *Corfu Channel Case, Judgment of April 9, 1949*, ICJ Reports of Judgments, Advisory Opinions and Orders 1949, s 35, *http://www.icj-cij.org/docket/files/1/1645.pdf* (2015-07-05) (citeras i det följande *Korfusundsmålet*); (2) op cit, *Nicaraguamålet*, se not 21, s 127 § 249; (3) op cit, *Rådgivande yttrande om lagligheten av hot om eller bruk av kärnvapen*, se not 44, s 246 § 46.
54. International Court of Justice [ICJ]: *Gabčikovo-Nagymaros Project (Hungary/*

*Slovakia), Judgment of September 25, 1997*, ICJ Reports of Judgments, Advisory Opinions and Orders 1997, s 55-57 §§ 83-87, *http://www.icj-cij.org/docket/files/92/7375.pdf* (2015-07-05) (citeras i det följande *Gabčikovo-Nagymaros-målet*).

55. Richardson, John Charles: *Stuxnet as Cyberwarfare. Applying the Law of War to the Virtual Battlefield*, JMR Portfolio Intelligence, Washington 2011, s 13 f, *http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1892888* (2015-07-05).
56. Artikel 2 lyder:
Förutom de bestämmelser, som skola träda i tillämpning redan i fredstid, ska denna konvention tillämpas i varje förklarat krig eller annan väpnad konflikt, som uppstår mellan två eller flera av de höga fördragsslutande parterna, även om en av dem icke erkänner att krigstillstånd föreligger.
Konventionen ska likaledes tillämpas vid ockupation av hela eller en del av en av de höga fördragsslutande parternas territorium, även om ockupationen icke möter något militärt motstånd.
Även om en av de i konflikten inbegripna makterna icke biträtt denna konvention ska den likväl vara bindande för de makter, som biträtt densamma, i deras inbördes förhållanden. Konventionen ska vidare vara bindande för dem gentemot nämnda makt, därest denna antager och tillämpar dess bestämmelser.
57. Corn, Geoffrey S; Hansen, Victor; Jackson, Richard B; Jenks, Chris; Jensen, Eric Talbot; Schoettler, James A, Jr: *The Law of Armed Conflict. An Operational Approach*, Wolters Kluwer Law & Business, New York 2012, s 14 f.
58. Pictet, Jean S: *Commentary on the Geneva Conventions of August 12, 1949. Band 1: Geneva Convention [I] for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field*, International Committee of the Red Cross, Genève 1995, s 32 [författarens översättning].
59. McCormack, Timothy L H: *Self-Defense in International Law. The Israeli Raid on the Iraqi Nuclear Reactor*, St. Martin's Press, New York | The Magnes Press, The Hebrew University, Jerusalem 1996, s 109 f och 301 f.
60. Op cit, Eek, Hilding m fl, se not 41, s. 403.
61. Se det av Tysklands expert i "Regeringsexpertgruppen för utvecklingar på informationens och telekommunikationernas område inom ramen för internationell säkerhet" vid gruppens första möte i New York den 22 juli 2014 distribuerade icke-officiella dokumentet med titeln "International Law Pertinent for Territorial Sovereignty in Cyberspace", s 3 § 6. – Expertgruppen som utarbetade Tallinn-manualen kunde emellertid inte enas kring frågan om det föreligger en suveränitetskränkning, när ett sabotageprogram installeras och det sedan inte förorsakar någon fysisk skada; op cit, *Tallinnmanualen*, se not 28, s 16.
62. Ebbesson, Jonas: *Internationell miljörätt*, Iustus, Uppsala 1993, s 46.
63. För en översikt över detta folkrättsliga område som kännetecknas av en påtaglig traktatdynamik se Beyerlin, Ulrich och Grote Stoutenburg, Jenny: "Environment, International Protection", i op cit, *MPEIL*, se not 18, band II, s 461-484; Sands, Philippe: *Principles of International Environmental Law*, Cambridge University Press, Cambridge 2003, s 125-143.
64. Op cit, *Rådgivande yttrande om lagligheten av hot om eller bruk av kärnvapen*, se not 44, s 241 f § 29; op cit, *Gabčikovo-Nagymaros-målet*, se not 54, s 41 § 53.
65. Bland de meddelade grunderna för de skadeståndskrav som Iran enligt chefen för presidentämbetets centrum för folkrättsliga ärenden, Majid Jafarzadeh, ville rikta mot USA och EU fanns inga miljöskador. Se Cohen, Tamir: "Iran: Nithba' eth kol hame`oravim be-mitkafoth ha-sayber" [Iran: Talan mot alla inblandade i cyberangreppen], *Ha-aretz* 2012-08-15, *www.haaretz.co.il/captain/net/1.1801964* (2015-07-05). Skadeståndskraven gjordes aldrig gällande.
66. Se härom Ebbesson, Jonas: *Nordiska ministerrådets rapport (TemaNord 2003:522) Den nordiska miljöskyddskonventionens relevans och framtid*, Nordiska ministerrådet, Köpenhamn 2003, s 106 f.
67. Drott, Daniel: *Gränsöverskridande föroreningar och statssuveränitet*, Lunds universitet, Lund 2004, s 37 f, *http://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=1556972&fileOId=1564166* (2015-07-05). Mera återhållsam till en dylik rättssats är Malanczuk, Peter: *Akehurst's Modern Introduction to International Law*, Routledge, London/New York 1998 (sjunde uppl), s 246.
68. T ex i artiklarna 3, 4 och 8 i 1933 års Montevideokonvention, i artiklarna 1 och 3:*e* i stadgan för Organisationen för de ame-

rikanska staterna, i artikel 3 i stadgan för Organisationen för afrikansk enhet samt i artikel 4:*a* och *g* i Afrikanska unionens konstituerande rättsakt av den 11 juli 2000.

69. Såsom exempelvis i principerna I och VI i 1975 års slutdokument från Helsingfors.
70. Se ovan not 19.
71. Op cit, *Korfusundsmålet*, se not 53, s 5; op cit, *Nicaraguamålet*, se not 21, s 106 § 202.
72. Op cit, Schulze, Sven-Henrik, se not 31, s 122 f; op cit, *Nicaraguamålet*, se not 21, s 106 f §§ 202-203.
73. Op cit, Ziolkowski, Katharina, se not 7, s 147.
74. Det kommer alltid att vara ett utmanande åtagande att skilja mellan utövande av illegalt tvång och av helt lagligt (politiskt, ekonomiskt o s v) inflytande. Varken statspraxis eller doktrin tillhandahåller några användbara kriterier för en sådan åtskillnad. I folkrättsvetenskapen hävdas det att olagligt tvång består i att utöva massivt inflytande, som förmår den drabbade staten att ta beslut med hänsyn till sin politik och praxis, som den inte skulle fatta som en fri och suverän stat. Se närmare härom dels Kunig, Philip: ”Intervention, Prohibition of”, i op cit, *MPEIL*, se not 18, band VI, s 289-299, dels Thorarensen, Björg och Leifsson, Pétur Dam: *Þjóðaréttur* [Folkrätt], Codex, Reykjavik 2011, s 114 f och 230-232; Roscini, Marco: ”Cyber Operations as a Use of Force”, i Tsagourias, Nicholas och Buchan, Russell (utg): *Research Handbook on International Law and Cyberspace*, Elgar, Cheltenham/Northampton 2015, s 233-254.
75. Op cit, Roscini, Marco, se not 10, s 151.
76. Op cit, Gill, Terry D, se not 10, s 235.
77. Seward, Amy; Mathews, Carrie; och Kessler, Carol: ”Evaluating Nonproliferation *Bona Fides*”, i Doyle, James E (utg): *Nuclear Safeguards, Security, and Nonproliferation. Achieving Security with Technology and Policy*, Elsevier/Butterworth-Heinemann, Burlington/Oxford 2014, s 274 f och 278 f.
78. Op cit, Roscini, Marco, se not 10, s 140 f; op cit, Gill, Terry D, se not 10, s 236.
79. Op cit, Ziolkowski, Katharina, se not 7, s 146 f.
80. Op cit, *Nicaraguamålet*, se not 21, s 125 f §§ 244-245.
81. Op cit, Eek, Hilding m fl, se not 41, s 308.
82. Roscini, Marco: *Cyber Operations and the Use of Force in International Law*, Oxford University Press, Oxford 2014, s 229.
83. Richmond, Jeremy: ”Evolving Battlefields: Does Stuxnet Demonstrate a Need for Modifications to the Law of Armed Conflict?”, *Fordham International Law Journal*, band 35, 3. häftet 2012, s 856.