Issue 35

December 2014

Legal Gazette

LEGAL ISSUES RELATED TO CYBER

Contents

Publisher:
Monte DeBoer, ACT Legal Advisor
Editor-in-Chief:
Dr. Petra Ochmannova, ACT SEE Deputy Legal Advisor
Editors:
Sherrod Lewis Bumgardner, ACT SEE Legal Advisor
Galateia Gialitaki, ACT SEE Legal Assistant
Mette Prassé Hartov, ACT Deputy Legal Advisor
Kathy Hansen-Nord, ACT Legal Assistance Section Head
Copy Editor:
Shaun Hiller, Legal Intern ACT SEE

www.nato.int

Introduction

Dear Fellow Legal Professionals and Persons interested in NATO,

Autumn brought us a number of interesting developments in the international legal scene. In September the United Kingdom hosted in Wales the NATO summit. Due to Russia's continued aggressive actions against Ukraine, as well as turbulent developments in the Middle East and growing instability in North Africa, the North Atlantic Council met at the Heads of State and Government level to declare the need for a stronger and more effective Alliance.

The world leaders discussed a number of important issues, including greater readiness, the area of cyber, and the need to increase national defence spending. Cyber threats, attacks and fundamental cyber defence responsibility of NATO to defend its own networks and assist Allies received a detailed discussion. You may read about the outcomes of their discussion in four paragraphs focused on cyberspace in the Wales Summit Declaration.

Because of the growing importance of cyber issues we are bringing you the 35th issue of the NATO Legal Gazette topically focused on Legal Issues related to Cyber.

As an introduction to the topic, our colleague from JFC Brunssum CAPT Enrico Cossidente provides you with a snapshot of the legal aspects of cyber and cyber-related issues affecting NATO. The *Jus Ad Bellum* part of cyber is addressed by Ms Florentine de Boer in her article examining the threshold of armed attack in light of collective defence. Our colleagues from NATO Cooperative Cyber Defence Centre of Excellence (CCD COE) Mr Pascal Brangetto, Mr Tomáš Minárik and Mr Jan Stinissen bring you their views on the legal implications of a shift from active cyber defence to responsive cyber defence.

Jus In Bello area is covered by one of the internationally recognised experts on the Law of Armed Conflict, Dr Gary Solis, who contributed with an article about cyber warfare and NATO legal advisors. In addition, Ms

Hanneke Pitters provides her views on the significant differences amongst scholars as to what constitutes direct participation in hostilities in cyber warfare.

As usual, we provide you with an article about a NATO entity. This time our colleague from the CLOVIS team Ms Annabelle Thibault prepared an article about Allied Command Transformation Staff Element Europe (ACT SEE).

Furthermore, because of the importance of better understanding the huge topic of cyber, we bring you two book reviews. One is provided by Mr Vincent Roobaert who examines Marco Roscini's book "Cyber Operations and the Use of Force in International Law" and the second is by Ms Stanila Dimitrova who examines a book edited by our former CCD COE colleague Dr Katharina Ziolkowski "Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy." This is followed by our regular sections like the Spotlight that introduces our new NATO colleagues, the Hail & Farewells, and information about upcoming events of legal interest.

Also, with pleasure we would like to share with you that as of 01 October 2014 Mr Andrés Muñoz Mosquera became the Allied Command Operations (ACO) Legal Advisor. We warmly welcome Mr Muñoz to his new post and provide a short tribute to his predecessor Mr Thomas Randall.

Finally, my assignment at ACT SEE finishes by the end of this year. In January 2015, I am re-assuming my position as a Legal Advisor at International Law Department at the Ministry of Defence of the Czech Republic. Thank you, the readers, for your interest in NATO matters and please allow me to especially thank the authors of the articles who provided the content for the NATO Legal Gazette. Every issue is only as good as its contributors are, and I am grateful that over past two years I had a privilege to edit the six thematically organized issues. I am glad you enjoyed reading the NATO Legal Gazette and look forward to working with you to strengthen our Alliance in the future.

Sincerely yours,

Dr Petra Ochmannova
Deputy Legal Advisor ACT SEE

STAFF ELEMENT EUROPE
MONS - BELGIUM

Questions on
Allied Command Transformation Staff Element Europe
(ACT SEE)

by Annabelle Thibault[1]

Why was ACT SEE created?

When NATO transitioned from a geographically-based to a functionally-based Command Structure in 2003 and as Allied Command Transformation (ACT) and Allied Command Operations (ACO) were created, it became clear that the large geographical and time distances between both Strategic Commands, which are headquartered on different sides of the Atlantic, necessitated a greater organisational presence in Europe to allow ACT to work directly with ACO and other NATO organisations in Europe.

Headquarters, Supreme Allied Commander Atlantic, the predecessor organisation to Headquarters, Supreme Allied Command Transformation (HQ SACT), had a representative element located at NATO HQ starting in 1967 and continuing through 2003. That element continues to exist to this day as the SACT Representative in Europe (commonly referred to as either STRE or SACTREPEUR) with the responsibility to represent SACT at the NAC and other relevant committees, specifically the Military Committee and its working groups.

ACT SEE had no predecessor at SHAPE and was created in 2003 when HQ SACT assumed responsibility from Supreme Headquarters Allied Powers in Europe (SHAPE) for key aspects of NATO defence and resource planning. ACT SEE was to serve as HQ SACT's footprint on the continent for interaction with

[1]Annabelle Thibault is a Franco-British licensed attorney who works as the supervising attorney of the CLOVIS Team. The views expressed in this article are solely those of the author and may not represent the views of NATO, ACO or ACT.

the International Military Staff (IMS), the International Staff (IS), ACO, Nations and other European NATO bodies/agencies, primarily for defence and resource planning issues.

ACT SEE initially consisted of SHAPE J-5 personnel who were transferred to HQ SACT posts to perform similar tasks under similar job descriptions. For instance, the SHAPE Defence Planning Team was transferred from the SHAPE Peacetime Establishment (PE) to the HQ SACT PE for immediate posting to SEE. At the time, the former SHAPE Defence Planning Team simply retained its offices within Building 101, the main building at SHAPE. In the ten years that have followed its creation, ACT SEE has become an entity which now comprises approximately 130 personnel "*performing Transformation functions under ACT command, but in support of the SHAPE and ACO operational missions,*"[2] all located in Building 104, *Live Oak*, behind the main building at SHAPE.

(Photo provided by the author)

Where does the term "*Live Oak*" come from?

In front of the *Live Oak* prefabricated building stands a large piece of the Berlin Wall, commemorating NATO's four decades of endeavouring to protect Western Europe and preserve freedom of access to West Berlin. Two large oak trees, planted when SHAPE moved from France to Belgium, now shade the sidewalk between the fragment of the Berlin Wall and the *Live Oak* entrance, where a poster reveals that *Live Oak* was the code name for a quadripartite military emergency planning group created in 1959.

General Lauris Norstad, then Supreme Allied Commander Europe (SACEUR), served as the first Commander of the Live Oak planning group. His staff was originally located on the U.S. European Command base just outside of Paris, in Fontainebleau. Starting in 1967 at SHAPE, in the very building ACT

[2] Memorandum of Understanding between HQ SACT and SHAPE concerning the HQ SACT Staff Element in Europe (SEE) at Mons, Belgium, 12 May 2005.

SEE is now using, Germany, France, the United Kingdom and the United States formulated responses to possible Soviet actions which could threaten Berlin. This emergency planning group remained in effect until German reunification on 2 October 1990.

What is the legal status of ACT SEE?

The decentralised nature of NATO and the mosaic of entities the Alliance comprises are reflected in the somewhat intricate framework of legal statuses necessary for their functionality. In general terms, NATO Headquarters, its International Staff and NATO Agencies are granted status, privileges and immunities by the Ottawa Agreement.[3] The Paris Protocol[4] provides the status of military organisations belonging to the NATO Military Structure. The Paris Protocol is often supplemented by further agreements entered into with the Host Nation by either HQ SACT or SHAPE to detail the relationship amongst the parties, depending upon which Supreme Command has the preponderance of forces in the country where the NATO entity is located.

ACT SEE illustrates the flexibility and practicality of these agreements. Commanded by the Supreme Allied Commander Transformation (SACT), ACT SEE receives funding, manning, and guidance like any other HQ SACT staff element. However, given its location in Belgium, ACT SEE legally enjoys the status of a military organisation subordinate to SHAPE as described in article 21 of the SHAPE – Belgium Supplementary Agreement of 1967,[5] but without prejudice to the military chain of command which links ACT SEE to HQ SACT. A Memorandum of Understanding (MOU) between HQ SACT and SHAPE concerning the HQ SACT Staff Element in Europe (SEE) at Mons, Belgium signed on 12 May 2005[6] establishes the relationship between SHAPE and ACT SEE for the purpose of administrative and logistic support. This is mainly aimed at guaranteeing efficient daily coordination between SEE and SHAPE as well as at gaining overall efficiencies of scale.

In June 2005, an Exchange of Letters (EOL) was signed between the Belgian Ministry of Foreign Affairs and SACEUR concerning the privileges and immunities to be granted to ACT SEE.[7] Accordingly, ACT SEE and its personnel

[3] Agreement on the Status of the North Atlantic Treaty Organisation, National Representatives and International Staff, 20 September 1951.
[4] Protocol on the Status of International Military Headquarters Set up Pursuant to the North Atlantic Treaty, 28 August 1952.
[5] Agreement between SHAPE and the Kingdom of Belgium on the Special Conditions Applicable to the Establishment and Operation of this Headquarters on the Territory of the Kingdom of Belgium, 12 May 1967, as amended in 2005 and 2013.
[6] Memorandum of Understanding between HQ SACT and SHAPE concerning the HQ SACT Staff Element in Europe (SEE) at Mons, Belgium, 12 May 2005.
[7] Exchange of Letters between BEL MFA and SACEUR on the Privileges and Immunities of ACT-SEE, 30 June 2005.

thus enjoy the very same status, immunities, and privileges, as enjoyed by SHAPE and its personnel under both the Paris Protocol and the 1967 SHAPE-Belgium Agreement.

In practice, and as a matter of example, ACT SEE personnel who are members of a force or civilian component are granted similar tax exemptions in respect to their salaries and emoluments under article 7 of the Paris Protocol. The archives and other official documents in ACT SEE are inviolable and entitled to immunity. The SHAPE-Belgium Agreement provides for a Road Tax exemption for all members of SHAPE: this provision also applies to ACT SEE personnel as does the support provided by Belgium in terms of postal services and telecommunications.

(Photo provided by the author)

What are the activities of ACT SEE?

The transformational functions of ACT SEE primarily relate to defence and resource planning and implementation but also to other ACT missions in the realm of Capability Development, Integrated Resource Management and Training and in coordination with the NATO Headquarters, ACO, and other NATO bodies and agencies in Europe.

The prevalence of defence and resource planning activities within ACT SEE, their co-existence with the functions of the various HQ SACT forward branches in the *Live Oak* building and the location of ACT SEE within ACO explain the quasi triple nature of the Director of ACT SEE's (DIR ACT SEE) post: indeed, DIR ACT SEE also acts as Deputy Assistant Chief of Staff Capability Requirements Targets and Review (DACOS CRTR) whilst being co-assigned as the Supreme Allied Commander Transformation (SACT) representative to the SACEUR.

As DACOS CRTR, DIR ACT SEE is responsible to ACOS Defence Planning (DP) for the management and delivery of the ACT contribution in various

steps of the NATO Defence Planning Process (NDPP). S/He is also intimately involved with the processes related to the transmission to NATO HQ and the nations of the ACT identified capability requirements together with proposals related to their national and multi-national implementation.

As DIR ACT SEE, s/he is responsible for the coordination and support to all HQ SACT Forward Elements located in Mons as well as for the activities of the SEE Coordination and Support Cell.

These Forward Elements include:

- A Joint Education, Training and Exercises (JETE) Branch which acts as JETE representative in appropriate ACO meetings and coordinates all NATO school education and training matters relating to ACO and NATO HQ;

- A NATO Security Investment Programme (NSIP) Section which represents ACT before the Investment Committee and coordinates the Minor Works processes;

- An ACT Crisis Response Operations (CRO) Liaison Team which routes CRO Urgent Requirements (CUR) and Allied Operations and Missions Requirement and Resource Plans (ARRP) to be reviewed by HQ SACT;

- A Command, Control, Deplorability and Sustainment (C2DS FWD) Branch which conducts C2, CIS, Cyber Defence and DS representation and engagement related functions in Europe; and

- A Legal Office, which reports to the ACT Legal Advisor and on whose behalf will engage with legal counterparts on the staffs of SHAPE, NATO HQ, IMS and IS concerning legal transformational initiatives in the areas of education, training and exercises.

What are the functions of the ACT SEE Legal Office?

On behalf of the HQ SACT Legal Office, the ACT SEE Legal Office delivers legal support to all branches of ACT-SEE, for instance through the review of the capability requirement documentation produced by the Capability Requirements (CR) and Capability Target and Review (CTR) branches. It provides general legal assistance concerning Host Nation matters to all ACT SEE personnel. When directed by the ACT Legal Advisor, the ACT SEE Legal Office coordinates Bi-Strategic Commands (Bi-SC) legal issues with the ACO Legal Office, represents HQ SACT, ACT SEE and other ACT entities in various *fora*, such as the NATO Administrative Tribunal or during Defence Policy and Planning Committee meetings. The ACT SEE Legal Office also provides legal support and assistance to the SACTREPEUR and staff.

The Legal Advisor serving as the Head of the ACT SEE Legal Office also is the Officer of Primary Responsibility (OPR) for two courses at the NATO

School: the Legal Advisors' Course which takes place in May and October each year and the Operational Law Course which occurs once a year in May. Additionally, the ACT SEE Legal Advisor is responsible for providing strategic legal support to the NATO exercises that SACT is scheduling on behalf of SACEUR.

Between 2008 and 2012, the ACT SEE Legal Advisor and the Deputy Legal Advisor respectively acted as Chairman and Secretary to the Law of Armed Conflict (LOAC) NATO Training Group Task Group assigned to develop a STANAG in the Training in Law of Armed Conflict (STANAG 2449 ed. 2).[8] Similarly and from January 2013 to March 2014, the LOAC NATO Training Group Task Group held five meetings to develop a STANAG in the Training on Rules of Engagement. The project was successfully completed in March 2014. In July 2014, the NATO Standardisation Agency (NSA) submitted a comprehensive package on the Training on Rules of Engagement to NATO nations to issue ratification responses. This package comprises STANAG 2597 and its corresponding Allied Training Publication.

The ACT SEE Legal Office continues to work on the 3rd version of the NATO Legal Deskbook and on new issues of the NATO Legal Gazette.

From 2009 to 2014, the ACT SEE Legal Advisor sponsored an experiment aimed at improving the sharing of legal information within NATO. The experiment led to the creation of a capability known as CLOVIS (Comprehensive Legal Overview Virtual Information System), which was successfully fielded in support of ISAF in 2013. In 2014, the ACT SEE Legal Advisor managed CLOVIS on behalf of ACO and in 2015, the SHAPE Legal Office will assume direction of the capability.

Conclusion

The continued presence of an HQ SACT forward element at SHAPE and the constant interactions taking place between SHAPE and ACT SEE personnel help answer the question about the means used by NATO's Supreme Military Commands to coordinate defence and resource planning, strategic thinking, and training, education and exercises efforts in the day-to-day strategic conduct of NATO operations.

***

[8] STANAG 2449 Ed. 2 was promulgated in March 2013 – The document can be found at: http://nsa.nato.int/nsa/nsdd/stanagdetails.html?idCover=8217&LA=EN. The corresponding Allied Training Publication can be found at: http://nsa.nato.int/nsa/nsdd/APdetails.html?APNo=1552&LA=EN

www.nato.int

Legal Aspects of Cyber and Cyber-Related Issues Affecting NATO

by Enrico Benedetto Cossidente[1]

Since the mid-1990s international law scholars have increasingly focused their attention on cyberspace.[2] In response to recent developments in the cyber domain, like the hacking activities against Estonia[3] and Georgia,[4] and the Stuxnet virus,[5] International Cyber Law has had to evolve and

[1] Enrico Benedetto Cossidente is an Italian Army Captain currently appointed as a Staff Officer (Rules of Engagement) at the Allied Joint Force Command Brunssum. The views expressed in this article are solely those of the author and may not represent the views of the Allied Joint Force Command Brunssum, ACO, ACT or NATO.

[2] A. Mefford, "Lex informatica: foundations of law on the internet", (1997/1998), v. 5 Ind J Global Legal Studies, 211 and D.R. Johnson and D. Post, "Law and borders – the rise of law in cyberspace", (1996), v. 48 Stanford L Rev, 1367.

[3] The Government of Estonia decided in 2007 to remove a bronze statue that celebrated the victory of the Soviet Army over Nazi Germany in World War II. This caused violent riots in the Estonian capital,Tallinn, and an unprecedented wave of cyber attacks against Estonian public and private sector websites. In regard to the origins of the attacks it has been noted that "some attackers were identifiable by their IP addresses. A number of those were Russian, including some cases where the IP address involved […] belonged to the Russian state institutions. However the Russian authorities denied any involvement, and cyber security experts also pointed out the possibility of spoofing attacker addresses and pointed out the lack of 'evidence of who is behind the attacks supposedly coming from Moscow'", E. Tikk, K. Kaska and L. Vihul, International Cyber Incidents – Legal Considerations, 2010 Cooperative Cyber Defence Centre of Excellence (CCD COE), 23. See also I. Traynor, "Russia accused of unleashing cyberwar to disable Estonia", The Guardian, 17.05.2007 (http://www.theguardian.com/world/2007/may/17/topstories3.russia); Estonia hit by "Moscow cyber war", BBC News, 17.05.2007 (http://news.bbc.co.uk/2/hi/europe/6665145.stm).

[4] During the brief Georgia – Russia War over South Ossetia, Georgia experienced cyber attacks similar to those inflicted to Estonia in 2007. "There is no doubt regarding the involvement of the Russian hacker community in the cyber attacks: the coordination of and support to the attacks took place mainly in the Russian language and was conducted in Russian or Russian-friendly forums. However, there is no evident link to the Russian administration, and the Russian government has denied any involvement in the cyber assaults." E. Tikk, K. Kaska and L. Vihul, supra note 3, 75. See also: Project Grey Goose, Phase I report Russia/Georgia Cyber War – Findings and analysis, 17.10.2008 (alvailable at: https://www.scribd.com/doc/6967393/Project-Grey-Goose-Phase-I-Report).

[5] A malicious program used to slow down the Iranian nuclear program. The US and Israel have been accused of conducting the attack. See M. E. O'Connell, "Cyber Security without Cyber War", Journal of Conflict & Sec Law, 2012, v. 17 No. 2, 188; M.N. Schmitt and L. Vihul, "Proxy wars in Cyberspace",

mature. The mainstream legal analysis has focused on the limitations of international law in handling cyber, and the consequences of cyber attacks/use of force conducted against States.[6] Although this approach has been partially acknowledged recently by an International Group of Experts in the Tallinn Manual[7] it still has some limits due to the different approaches that Nations have to the use of force[8] and the conduct of cyber operations (offensive vs defensive).[9] Yoram Dinstein, on the other hand, is convinced that the current international law is sufficient to regulate cyber warfare.[10] A minority of scholars suggest the return of a Cold War type of deterrence strategy in relation to cyber.[11]

Fletcher Sec Rev, v. I Issue II, spring 2014, 54; M.C. Waxman, "Cyber-Attacks and the use of force: back to the future of Article 2(4)", v. 36 Yale J Intl Law, 2011, 423; K. Dilanian "Iran and the era of cyber war", LA Times,17.01.2011, A1 (http://articles.latimes.com/2011/jan/17/world/la-fg-iran-cyber-war-20110117); D. E. Sanger, "Iran fight malware attacking computers", N.Y. Times, 26.09.2010, 4 (http://www.nytimes.com/2010/09/26/world/middleeast/26iran.html).

[6] One of the most known supporter of this approach is Michael N. Schmitt (see of this author: "Classification of cyber conflict", Journal of Conflict & Sec Law, v. 17 no. 2, 2012, 245-260; see M.N. Schmitt and L. Vihul, supra note 5; "The law of cyber warfare: quo vadis?", v. 25 Stan. L. & Pol'y Rev., June 2014, 269-300).

[7] "In 2009, the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE), an international military organisation based in Tallinn, Estonia, and accredited in 2008 by NATO as a 'Centre of Excellence', invited an independent 'International Group of Experts' to produce a manual on the law governing cyber warfare. […] It is essential to understand that the Tallinn Manual is not an official document, but instead only the product of a group of independent experts acting solely in their personal capacity. The Manual does not represent the views of the NATO CCD COE, its sponsoring nations, or NATO. In particular, it is not meant to reflect NATO doctrine. Nor does it reflect the position of any organization or State represented by observers. Finally, participation in the International Group of Experts by individuals with official positions in their own countries must not be interpreted as indicating that the Manual represents the viewpoints of those countries. Ultimately, the Tallinn Manual must be understood as an expression solely of the opinions of the International Group of Experts, all acting in their private capacity". "Tallinn manual on the international law applicable to cyber warfare", M.N. Schmitt gen. ed., Cambridge University Press, April 2013, Introduction, 16 and 23.

[8] According to the US official position any use of force is considered an armed attack, so there is virtually no difference between art. 2 (4) and art. 51 of the UN Charter (see: at the time US State Dep Legal Adv, H.H. Koh, "International Law in Cyberspace", v. 54 Harvard Int'l Law J Online, 2012, 1-12; M.N. Schmitt, "The Koh speech and the Tallinn Manual juxtaposed", v. 54 Harvard Int'l Law J Online, 2012, 13-37; M.N. Schmitt and L. Vihul, supra note 4, at 67).

[9] In the international community only few nations openly acknowledged their willingness to conduct offensive cyber operations: the UK (see Mr. Philip Hammond,UK Defence Secretary, statement at http://www.ft.com/intl/cms/s/0/9ac6ede6-28fd-11e3-ab62-00144feab7de.html#axzz3BgZxoItw), the US (see the definition of "Offensise Cyber Effects Operations", Presidential Policy Directive-PPD20, 3, http://epic.org/privacy/cybersecurity/presidential-directives/presidential-policy-directive-20.pdf) and the Netherlands in their "Defence Cyber Strategy" (Netherlands Ministry of Defence, 27.06.2012, 5, 6, 8, 11, accessible at http://www.ccdcoe.org/strategies/Defence_Cyber_Strategy_NDL.pdf).

[10] Based on the ICJ advisory opinion on Nuclear Weapons for Dinstein "[..] what counts is not the specific type of ordnance, but the end product of its delivery to a selected objective". So "[..] whatever is permitted (or prohibited) when kinetic means of warfare are used is equally permitted (or prohibited) when the means employed are electronic; the rules of international law are the same whatever the means selected for attack" (Y. Dinstein, "Computer network attacks and self-defense", Int'l Law Studies, v. 76, US Naval War College, 2002,103, 108).

[11] M.C. Waxman, supra note 5, at 421-459. M. McConnell, "How to win the cyber war we are losing", Washington Post, 28.02.2014 (at http://www.washingtonpost.com/wpdyn/content/article/2010/02/25/AR2010022502493.html). Others are against this approach: P. Singer and N. Schachtman, "The wrong war: the insistence on applying cold war metaphors on cybersecurity is misplaced and counterproductive", Bookings

There is also a reverse trend, represented by Mary E. O'Connell,[12] which advocates a change in the way the international community and legal scholars address cyber issues. According to O'Connell, security in cyber space is mainly threatened by crime and espionage and not by military action.[13] She underlines the fact that, by nature, cyber can be used for civil or military purposes, like atomic energy. Therefore the UN should sponsor the creation of international treaties and ad hoc institutions to control and fight the proliferation of crime in cyber space. At the national level this approach requires the involvement of law enforcement units (e.g. police) and special branches of the military to deal with cyber, thus avoiding a situation, like in the US, where a single overarching institution handles these matters.[14] The issue with taking any of the positions mentioned above is that they do not express state practice and opinio juris in the cyber domain. Only time and the action of States will forge a path that the international community will follow.

What is the position of NATO in relation to cyber law? In 2003 the NATO Computer Incident Response Capability (NCIRC) was created to protect NATO's computer networks as the Organisation is responsible for its own computer networks and not for the networks of the Allies. In the aftermath of the 2007 attacks on Estonia, NATO enacted measures to contain the risk of cyber attacks to itself and its member nations. One of the initiatives by NATO members states was to create the NATO Cooperative Cyber Defence Centre of Excellence (CCD COE).[15] In 2010 at the Lisbon Summit NATO endorsed an

---

Institution, 15.08.2011 (accessible at http://www.brookings.edu/research/articles/2011/08/15-cybersecurity-singer-shachtman).

[12] M. E. O'Connell, supra note 5, 187-209.

[13] M. E. O'Connell, supra note 5, at 200.

[14] M. E. O'Connell, supra note 5, at 200. O'Connell's idea is to have cyber space controlled by the Department of Homeland Security (DHS) instead of the United States Cyber Command (USCYBERCOM) as this would de-militarize the internet. On June 23, 2009, the Secretary of Defense directed the Commander of U.S. Strategic Command to establish a sub-unified command, United States Cyber Command (USCYBERCOM). USCYBERCOM plans, coordinates, integrates, synchronizes and conducts activities to: direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to adversaries http://www.defense.gov/home/features/2010/0410_cybersec/docs/cyber_command_gates_memo[1].pdf).

[15] The NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) is an international military organisation accredited in 2008 by NATO's North Atlantic Council as a 'Centre of Excellence'. Located in Tallinn, Estonia, the Centre is currently supported by the Czech Republic, Estonia, France, Germany, Hungary, Italy, Latvia, Lithuania, the Netherlands, Poland, Slovakia, Spain, the United Kingdom and the USA as Sponsoring Nations. The Centre is not part of NATO's command structure, but it is part of a wider framework supporting NATO Command Arrangements. CCD COE is funded by its Sponsoring Nations and not NATO.
The NATO CCD COE's mission is to enhance capability, cooperation and information sharing between NATO, NATO Member States and NATO's partner countries in the area of cyber defence by virtue of research, education and consultation. The Centre has taken a NATO-orientated, interdisciplinary approach to its key activities, including: academic research on selected topics relevant to the cyber domain from legal, policy, strategic, doctrinal and/or technical perspectives; providing education and training, organising conferences, workshops and cyber defence exercises, and offering consultancy upon request. Source: "National cyber security. Framework manual", edited by A. Klimburg, NATO CCD

"in-depth cyber defence" policy. This concept recognises that the cooperation of all the branches of a State's Government are needed to prevent cyber attacks (the so called "Whole Government Approach"[16]).

Despite all the measures taken by NATO there is still no concurrence between the international community and scholars on the threshold upon which a cyber (armed) attack triggers individual or collective self defence.[17]

This lack of common direction of the international community has prevented the definition of an armed cyber-attack in regard to Article 51 of the UN Charter. Nevertheless, NATO as an organisation is addressing issues related to cyber in a number of instances. An example could be the creation of the CCD COE, the Lisbon Summit concept, the recent Wales Summit declaration that the cyber domain still needs more attention. Fragmentation between stakeholders in the Organization has to be minimised and a Cyber Red Team[18] should be created to test its cyber defence capability.

NATO's position has to be compared with the actions of non-NATO actors, specifically Russia and China. These two nations have demonstrated mixed behaviors concerning their perception of international law in cyber space. In 2013 a UN Group of Experts, that included representatives of Russia and China, agreed that international law applies to cyber space; however, both Russia and China did not agree to a reference of international humanitarian law (IHL) with regard to cyber activities.[19] Alternately they are holding this position in regard to IHL while promoting the creation of an international treaty on cyber.[20] Though there have been some Russian actions in cyber space there is no clear evidence of Russian State actors'

COE Publication, Tallinn 2012.

[16] A. Klimburg (Ed.), supra note 15. A new cyber defence policy is circulating in NATO (see last two sentences of http://www.nato.int/cps/en/natohq/topics_78170.htm?selectedLocale=en).

[17] See art. 5 of the North Atlantic Treaty signed in Washington, USA, 4 April 1949, came into force on 24 August 1949 (http://www.nato.int/cps/en/natolive/official_texts_17120.htm). NATO's latest position on the issue was defined after the Wales Summit of September 2014: "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", point 72 of the Official Text of the Wales Summit Declaration (issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales), accessible at http://www.nato.int/cps/en/natohq/official_texts_112964.htm?selectedLocale=en.

[18] A. Klinburg (Ed.), supra note 15, 183.

[19] M. N. Schmitt,"The law of cyber warfare: quo vadis?", supra note 6, 3.

[20] T. Maurer, "Cyber norm emergence at the United Nations-An Analysis of the Activities at the UN Regarding Cyber-security", Harvard Kennedy School-Belfer Center for Science and International Affairs, Sep 2011, 20; J. Lewis interview "International treaty on cyber security is not going to happen-US expert", Voice of Russia,17.05.2013 (accessible at http://voiceofrussia.com/2013_05_17/International-treaty-on-cyber-security-is-not-going-to-happen-US-expert/); "China and Russia surprised the international community last month when they submitted a letter at the UN General Assembly outlining a proposal for an International Code of Conduct for Information Security.", T. Farnsworth, "China and Russia Submit Cyber Proposal", Arms Control Association, Nov 2011 (accessible at https://www.armscontrol.org/act/2011_11/China_and_Russia_Submit_Cyber_Proposal). According to M.E. O'Connell, supra note 5, 205 fn 90, the Russian proposal of a treaty dates back to 1998.

involvement in cyber attacks against Estonia or the US.[21] It is a fact, however, that cyber-attacks were conducted from Russia during its military operations against Georgia.[22] China also has a history of conducting cyber-attacks, but its activities are mainly related to the gathering of military/commercial intelligence.[23] Some of these cyber activities have led to claims being brought against Chinese citizens in US domestic courts.[24]

The aim of this article was to give a brief overview of the interaction between international law and the actions taken in cyber space. The latest legal positions taken by scholars, as well as the activities performed by States and international organisations in this domain portray that, with no coordination in the international community, uncertainty will be the only benchmark of cyber.

***

[21] "The FBI is investigating hacking attacks on 7 of the top 15 banks, including one against JPMorgan Chase […] Hackers from Russia and eastern Europe are often top FBI suspects in cyberattacks. The timing has raised suspicions given the mounting tensions between Russia and the West over Ukraine and economic sanctions" M.Egan, J. Pagliery, E. Perez, "FBI investigating hacking attack on JPMorgan", CNN Money, 27.08.2011 (accessible at http://money.cnn.com/2014/08/27/investing/jpmorgan-hack-russia-putin/).

[22] See supra note 4.

[23] On China's cyber activities see E. Nakashima, "US said to be target of massive cyber-espionage campaign", Washignton Post, 11.02.2013 (accessible at http://www.washingtonpost.com/world/national-security/us-said-to-be-target-of-massive-cyber-espionage-campaign/2013/02/10/7b4687d8-6fc1-11e2-aa58-243de81040ba_story.html).

[24] The Department of Justice charged "five members of the Chinese military [for] hacking into computers and stealing valuable trade secrets from leading steel, nuclear plant and solar power firms, marking the first time that the United States has leveled such criminal charges against a foreign country", E. Nakashima, "U.S. announces first charges against foreign country in connection with cyberspying", Washignton Post, 19.05.2014 (accessible at http://www.washingtonpost.com/world/national-security/us-to-announce-first-criminal-charges-against-foreign-country-for-cyberspying/2014/05/19/586c9992-df45-11e3-810f-764fe508b82d_story.html). On technical evidence of China state actors active involvement in cyber attacks against US targets see: Mandiant Report (Mandiant, "APT1 – Exposing One of China's Cyber Espionage Units", 18.02.2013 accessible at http://intelreport.mandiant.com/).

www.ccdcoe.org

From Active Cyber Defence to Responsive Cyber Defence: A Way for States to Defend Themselves – Legal Implications

by Pascal Brangetto, Tomáš Minárik, Jan Stinissen[1]

Introduction

The Hobbesian *state of nature* is often used to describe the cyber environment which is deemed lawless and full of peril. In order to ensure that computer systems and networks are secure, a wide array of solutions have been developed. "*From the earliest days of the Internet, the basic approach to network security has been to play defense*,"[2] sometimes expressed as "*the best defense is a good defense*."[3] Essentially, one should only deploy defensive means within the network that has to be secured. It is generally acknowledged that the offensive party has the upper hand in cyberspace[4] as it can choose the time and date of a cyberattack, thus, deploying only passive measures might result in a Maginot line situation for the defender.

The mere fact of labelling current defensive tools as passive is a call for a more empowering definition of cyber defence. The use of only passive measures is no longer sufficient to protect networks in the face of rising threat levels. As a way to overcome this, and to be able to hold the high ground, a concept was developed to enable the defending party to play an active

[1] Law and Policy Branch researchers, NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia. The views expressed in this article are solely those of the authors and may not represent the views of NATO, ACO, ACT or the NATO CCD COE.
[2] John Seabrook, "Network Insecurity," *The New Yorker*, May 20, 2013, p. 65.
[3] Josephine Wolff, "The Right to Bear Denial-of-Service Attacks", http://www.slate.com/articles/technology/future_tense/2014/06/second_amendment_right_in_the_cyber_world_is_it_necessary.html. This hyperlink and all those referred to in the following footnotes were last accessed on 10 October 2014.
[4] William Lynn, "In Cyberspace, the Offense Has the Upper Hand," "Defending a new domain" in *Foreign Affairs*, September/October 2010, p. 99.

part in its own cyber defence. The term Active Cyber Defence (ACD) was officially coined by the United States Department of Defense in 2011,[5] and has, since then, become a buzzword. However some concerns have been expressed[6,7] as this notion of active defence[8] gives a somewhat seductive framework that must not be oversimplified or used lightly.[9]

The authors of this article explore, from a legal perspective, the possibility of states taking responsive measures that enhance their cyber defence capabilities. Responsive Cyber Defence (RCD) is seen as a middle-path solution for states around which a clear and robust framework can be constructed. We only consider RCD as an option for states, and will avoid drawing any conclusions for the private sector. The ambition of this article is to provide a general overview of the legal regimes applicable depending on the different cyber incidents and situations which a state entity might be confronted with.

Hence, after defining RCD, the article addresses the deployment of RCD activities from both international and domestic legal perspectives in order to assess their feasibility and to determine their legitimacy.

Responsive cyber defence

The authors of this article define "RCD" as the protection of a designated Communications and Information System (CIS) against an ongoing cyberattack by employing measures directed against the CIS from which the cyberattack originates, or against third-party CIS which are involved. RCD can be seen as a subset of ACD, but the crucial difference is that RCD activities are only conducted in response to an actual and ongoing cyberattack (see *Diagram 1*) and it does not cover pre-emptive or retaliatory

---

[5] "…DoD's synchronized, real-time capability to discover, detect, analyze, and mitigate threats and vulnerabilities. It builds on traditional approaches to defending DoD networks and systems, supplementing best practices with new operating concepts. It operates at network speed by using sensors, software, and intelligence to detect and stop malicious activity before it can affect DoD networks and systems. As intrusions may not always be stopped at the network boundary, DoD will continue to operate and improve upon its advanced sensors to detect, discover, map, and mitigate malicious activity on DoD networks." Department of Defense Strategy for Operating in Cyberspace, July 2011, p. 6, http://www.defense.gov/news/d20110714cyber.pdf.

[6] "When the *Washington Post* publishes a story hyping an ill-considered notion of cyber retaliation misleadingly called "active defense" as a rational idea, we should all worry," Gary McGraw, "Proactive defense prudent alternative to cyberwarfare" http://searchsecurity.techtarget.com/news/2240169976/Gary-McGraw-Proactive-defense-prudent-alternative-to-cyberwarfare.

[7] Paul Rosenzweig, "A typology for evaluating Active Cyber Defenses," 15 April 2013, http://www.lawfareblog.com/2013/04/a-typology-for-evaluating-active-cyber-defenses.

[8] Irving Lachow, "Active cyber defence, a framework for policymakers," February 2013, Center for a New American Security (CNAS). http://www.cnas.org/files/documents/publications/CNAS_ActiveCyberDefense_Lachow_0.pdf.

[9] The comments made in 2012 by Leon Panetta, at the time U.S. Secretary of Defense, hint that this notion could be used to justify pre-emptive cyber actions which could prove counter-productive and dangerous. http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?pagewanted=all&_r=0 .

actions.[10]

For the purposes of this article, and in accordance with NATO documents, a "cyberattack" is understood to be "*[a]n act or action initiated in cyberspace to cause harm by compromising communication, information or other electronic systems, or the information that is stored, processed or transmitted in these systems.*"[11] By "harm", the commentary means not only injury to persons and damage to objects, but also "*direct or indirect harm to a communication and information system, such as compromising the confidentiality, integrity, or availability of the system and any information exchanged or stored.*"[12] Therefore, cyberespionage activities can also be included in this definition. A cyberattack involving the compromise of a CIS is considered to be "ongoing" as long as the defending system is under a certain level of control by the attacker. The mere introduction of a malware into the defending system can already be seen as a compromise of the system and hence, a cyberattack.

It should be well noted that this NATO definition of "cyberattack" is broader than the one provided in the Tallinn Manual for the purposes of *jus in bello*.[13] It also differs from the concept of "cyber operations[14] constituting an armed attack" for the purposes of *jus ad bellum*.[15] This is understandable, because although most cyberattacks take place outside the context of an armed conflict, they still have to be dealt with by domestic and (sometimes) international law.

The main premise of this article is that RCD measures can potentially involve activities which could themselves be qualified as cyberattacks, such as a denial of service attack, responsive honeypots[16] or "hack back". This generates controversy around RCD and prompts political and legal debates regarding its acceptability.

---

[10] Neither RCD nor ACD are defined by NATO. We also noted the US DoD definition of "defensive cyberspace operation response action": "Deliberate, authorized defensive measures or activities taken outside of the defended network to protect and defend Department of Defense cyberspace capabilities or other designated systems." Department of Defense Dictionary of Military and Associated Terms, November 2010 (amended February 2014).

[11] NATO "Report on Cyber Defence Taxonomy and Definitions," Enclosure 1 to 6200/TSC FCX 0010/TT-10589/Ser: NU 0289.

[12] Ibid.

[13] Michael N. Schmitt (gen.ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare,* Cambridge University Press, Cambridge 2013, Rule 30: Definition of Cyber Attack, p. 106.

[14] A cyber operation is "[t]he employment of cyber capabilities with the primary purpose of achieving objectives in or by the use of cyberspace," *Ibid,* p. 258.

[15] Ibid, p. 54.

[16] Honeypots are deception tools (e.g. a fake website) that have the main purpose to analyse the behaviour and intentions of a potential attacker. To render a honeypot responsive would imply, for example, planting a trapped file (beacon, call back functionality…) to be retrieved by the attacker.

The responsive cyber defence timeframe

Legend:

-A: Detection of an ongoing cyberattack

-B: End of the cyberattack – termination of its effects on the defended networks.

Diagram 1 – RCD timeframe

(Diagram provided by the author)

Legal considerations : Public International law

It is now generally acknowledged that international law applies to cyberspace,[17] and it is certainly relevant for RCD because of the possible cross-border effects. The question is how it can be applied. Taken from the perspective of a state actor, we will consider how rules of public international law can limit or justify RCD activities.

A) Rules of public international law relevant to RCD activities

Public international law regulates relations between states, granting them rights and imposing obligations towards other states. A breach of such an obligation by a state constitutes an internationally wrongful act.[18] The following paragraphs describe when a cyber operation, including an RCD operation, conducted by state organs or otherwise attributable to states, may constitute an internationally wrongful act.

Cyber operations that include a use of force, as prohibited by Article 2(4) of the UN Charter, are internationally wrongful acts. The question of what type of action can amount to a "cyber use of force" is extensively discussed in the Tallinn Manual, concluding that "*[a] cyber operation constitutes a use*

[17] Indicative is the acknowledgement of the application of international law to the use of Information and Communications Technology (ICT) in the report of the UN General Assembly, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," A/68/98, June 24, 2013. This Group consisted of representatives of 15 states, including the United States, the Russian Federation and China.

[18] See the International Law Commission's *Articles on Responsibility of States for Internationally Wrongful Acts* (2001), Article 2. These *Articles on State Responsibility* are largely deemed to reflect customary international law.

of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force".[19] RCD measures that result in significant physical damage to objects, or injury or death to a person can thus be considered uses of force. Measures that only cause loss of data or financial loss are not uses of force.

A cyber operation that violates a state's sovereignty constitutes an internationally wrongful act.[20] That would definitely include cyber operations that cause physical effects including damage or injury on another state's territory. The question is whether operations that only have non-physical consequences, such as using malware to delete or modify data in a system on another state's territory, or placing malware in a system to monitor its activities, could also qualify as a violation of sovereignty.[21] Few states have taken this position. According to the United States International Strategy for Cyberspace a "disruption of networks and systems" could call for a response.[22,23]

The non-intervention principle - the principle that states shall not intervene in the domestic affairs of another state - is a reflection of sovereignty. If cyber operations coerce a state to take certain actions or refrain from actions, these operations can qualify as unlawful intervention. For example, operations that imply political interference, such as bringing down the online services of a political party on the eve of elections, could qualify as unlawful intervention.[24]

Sovereignty of states also implies that states have an obligation to maintain control over the activities conducted on or from their territory in order to prevent or stop acts that adversely or unlawfully affect other states.[25] The standard of care for monitoring and protection, *due diligence*,[26] implies that states have a duty to monitor cyber infrastructure under their control and prevent harmful or unlawful cyber activities from being performed from it. This

---

[19] Tallinn Manual , *supra* note 13, Rule 11, p. 45.
[20] See for a discussion on sovereignty in cyberspace, Wolff Heintschel von Heinegg, "Legal implication of Territorial Sovereignty in Cyberspace" in *4th International Conference on Cyber Conflict, Proceedings*, NATO CCD COE, Tallinn, 2012, or Benedikt Pirker, "Territorial Sovereignty and Integrity and the Challenges of Cyberspace," in Katharina Ziolkowski (ed.), *Peacetime Regime for State Activities in Cyberspace*, NATO CCD COE, Tallinn, 2013.
[21] The group of experts that drafted the Tallinn Manual did not reach consensus on this (Tallinn Manual, *supra* note 13, p. 16).
[22] The President of the United States of America, *International Strategy for Cyberspace, Prosperity, Security, and Openness in a Networked World* (May 2011), p. 12. http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf
[23] See Heintschel von Heinegg, *supra* note 20, p. 11-12.
[24] Tallinn Manual, *supra* note 13, p. 45.
[25] *Ibid*, p. 26.
[26] ICJ, *Pulp Mills on the River Uruguay (Argentine v. Uruguay)*, Judgment of 20 April 2010, para. 101: The Court points out that the principle of prevention, as a customary rule, has its origins in the due diligence that is required of a state in its territory. It is "every state's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other states."

is crucial; it can mean that a state can commit an internationally wrongful act by not preventing or stopping malicious activity conducted by a private actor from within the state's territory or from a ship or airplane under the control of the state.

Besides the more general aspects just discussed, there are special legal regimes that can be relevant when taking RCD measures. Cyber operations can have an impact on the availability, integrity, and confidentiality of data, possibly impacting international human rights law with respect to privacy or access to information. These operations can also have an impact on the availability of telecommunications services, possibly violating obligations deriving from telecommunications law. They can hamper business transactions, thus perhaps violating trade law obligations, or can even involve air, space, maritime, or diplomatic law.[27] Activities in cyberspace can also affect the obligations deriving from a specific bilateral treaty.

B) Justification for RCD under international law

International law provides states with different options to choose from in order to respond to cyberattacks. Besides protective cyber measures, that only have an effect on their systems or within their own territory, states could take measures against other states that are perhaps unfriendly, but not unlawful. Those actions could qualify as "retortion." An example could be the suspension of services to certain IP addresses.[28] With respect to RCD however, it could be that these measures themselves constitute an internationally wrongful act. Bearing this in mind, the following circumstances precluding wrongfulness might apply.

Under Article 51 of the UN Charter, states have the inherent right of self-defence against an act that amounts to an "armed attack." In the cyber context this threshold is unlikely to be reached. The authors of the Tallinn Manual conclude that cyber operations including a grave use of force can constitute an armed attack. Operations resulting in injuries, deaths, or serious damage to physical objects would qualify.[29] In such a case RCD measures could be employed in self-defence.

Based on a "plea of necessity" measures can be taken to "*protect the essential interests of a state against a grave and imminent peril*."[30] What exactly is an "essential interest" and what is a "grave and imminent peril" is subject to debate. The plea of necessity would likely be relevant when cyber operations threaten the vital functions of a state by targeting its critical

[27] A comprehensive overview of different law regimes relevant to cyber operations is provided in Katharina Ziolkowski (ed.), *Peacetime Regime for State Activities in Cyberspace*, NATO CCD COE, Tallinn, 2013.
[28] See Tallinn Manual, *supra* note 13, p. 40-41
[29] Ibid, p. 54-68.
[30] Articles on State Responsibility, *supra* note 18, Article 25(1).

infrastructures.[31,32] However, necessity is a circumstance that cannot be easily invoked,[33] but should only be considered in exceptional cases: it can be applied when it is "*the only way for the state to safeguard an essential interest*" and may not "*seriously impair an essential interest of the state or states towards which the obligation exists, or of the international community as a whole*."[34]

"*A state injured by an internationally wrongful act may resort to proportionate countermeasures, including cyber countermeasures, against the responsible state*."[35] The purpose of countermeasures is to compel the attacking state to stop the malicious activity and resume compliance with its international legal obligations. Thus, attribution is essential to engage in countermeasures. It must be clear that it is indeed a *state* that is violating its obligations under international law, and at the same time, "*countermeasures are a tool reserved exclusively to states.*"[36] Consider the case when a state suffers a severe cyberattack that does not amount to an armed attack, but nevertheless qualifies as a violation of sovereignty. If the cyberattack is attributable to another state, it constitutes an internationally wrongful act and the injured state could consider cyber and other countermeasures in response. Cyber countermeasures can include blocking electronic traffic, blocking access to financial assets, and in principle even more intrusive measures like a "denial of service attack" against the cyber infrastructure of the attacking state, or a "hack-back." All countermeasures are nevertheless subject to restrictions. Most notably they must be proportionate to the internationally wrongful act and limited to the time during which the wrongful act is ongoing. It can therefore never be a retaliatory measure. Also the state has to give notice that the countermeasure is going to be conducted or, when it is an urgent measure with the aim to safeguard the state's interests,

---

[31] See Robin Geiss and Henning Lahmann, "State Interaction and Counteraction in Cyberspace," in Katharina Ziolkowski (ed.), *Peacetime Regime for State Activities in Cyberspace*, NATO CCD COE, Tallinn, 2013, p. 646.

[32] "'Critical infrastructure' means an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions," *Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection*. In the United States, critical infrastructure is defined as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, February 2013, http://www.nist.gov/cyberframework/

[33] Robert D. Sloane, "On the use and abuse of necessity in the Law of State Responsibility," *The American Journal of International Law*, Vol. 106 (2012), p. 450.

[34] Articles on State Responsibility, *supra* note 18, Article 25(1).

[35] Tallinn Manual, *supra* note 13, Rule 9, p. 36-41. This rule stems from Article 22 of the Articles on State Responsibility, *supra* note 18. The right to use countermeasures is acknowledged by the International Court of Justice, for example in the *Gabčíkovo-Nagymaros Project* (Hungary v. Slovakia) judgment of 25 September 1997.

[36] Michael N. Schmitt, "Cyber Activities and the Law of Countermeasures," in Katharina Ziolkowski (ed.), *Peacetime Regime for State Activities in Cyberspace*, NATO CCD COE, Tallinn, 2013, p. 686.

the other state has to be notified immediately afterwards.

Another justification for responsive actions is when the other state agrees with them. "*Valid consent by a state to the commission of a given act by another state precludes the wrongfulness of that act in relation to the former state to the extent that the act remains within the limits of that consent*."[37] One can imagine that the use of a state's cyber infrastructure could be granted to another state for protective or responsive purposes. Chapter III of the Convention on Cybercrime[38] provides an example of the implementation of consent-based procedures for international cooperation regarding trans-border access to stored computer data.[39] Note that these provisions are only applicable when concerning criminal investigations.[40]

In general, human rights norms, and the norms derived from telecommunications law, trade law and other special legal regimes, are not absolute. Often exceptions are allowed if they protect a legitimate interest such as national security or public safety. Responsive cyber operations that violate a special legal norm, but protect an interest as recognised by the respective regime, could therefore be lawful. For example, an operation that temporarily denies citizens to receive or send messages to and from certain IP addresses affects the freedom to receive and impart information, but might be excused if that operation is necessary to protect national security.[41]

Thus, based on public international law, several solutions may be available to respond to malicious activities, but their application is bound by strict conditions.

www.ccdcoe.org

[37] Articles on State Responsibility, *supra* note 18, Article 20.
[38] Convention on Cybercrime, Budapest, 23 November 2001.
[39] Article 32 paragraph b) of the Convention on Cybercrime: "A Party may, without the authorisation of another Party: access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system."
[40] T-CY Guidance Note n. 3 "Transborder access to data (Article 32)," http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/Guidance_Notes/T-CY(2013)7REV_GN3_transborder_V11.pdf
[41] See also Dinah PoKempner, "Cyberspace and State Obligations in the Area of Human Rights," in Katharina Ziolkowski (ed.), *Peacetime Regime for State Activities in Cyberspace*, NATO CCD COE, Tallinn, 2013, p. 243-246.

Legal considerations : Domestic law

This section provides a general overview of the common features of domestic laws that can be found among NATO member states which, in addition to international law, might have to be taken into account before engaging in any RCD activities.

A) Domestic law and cyberattacks

Modern constitutions adhere to the notion that the executive branch of government is bound by domestic laws. The executive enforces and executes the law created by the legislature as interpreted by the judiciary. This is the fundamental principle of limited government in the legal doctrines of *rule of law* and *Rechtsstaat*, prevalent in both the common and civil law traditions, and is a vital component of the separation of powers in a liberal democracy. The executive can only act if allowed to do so by the law, and RCD activities are not exempt from this principle. [42]

In general, a state's domestic laws, which can limit RCD capabilities or activities, are designed to protect the rights and interests of its citizens. For instance, human rights such as the right to privacy and protection of personal data, the right to property and freedom of expression, information, thought, conscience, religion, assembly and association are often enshrined in a state's constitutional law. More detailed regulations are found in criminal law and other public and private legislation. These also provide for possible limitations on fundamental rights for the purposes of protection of public order, national security or defence.

Most NATO member states have ratified the Convention on Cybercrime (Budapest, 23 November 2001),[43] and are thereby committed to incorporating its provisions into their domestic law. The Convention's primary aim is to harmonise substantive criminal laws of its Parties by providing common elements of the offences. The most important offences for the purpose of this article are those against the confidentiality, integrity and availability of computer systems (Articles 2 to 6 of the Convention).[44] These include illegal access, illegal interception, data interference, system

---

[42] See e.g. Article 20 paragraph 3 of the Basic Law (Grundgesetz) for the Federal Republic of Germany from 23 May 1949: "The legislature shall be bound by the constitutional order, the executive and the judiciary by law and justice.", the English version (as of 21 July 2010) retrieved from http://www.gesetze-im-internet.de/englisch_gg/
and the Tenth Amendment to the United States Constitution: "The powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved to the States respectively, or to the people." http://www.law.cornell.edu/anncon/html/amdt10_user.html

[43] http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm
Except for Canada, Greece and Poland. These countries have not ratified the Convention but all of them have signed it, see
http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG

[44] http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

interference, and misuse of devices.[45] The Parties included the definitions in their criminal and other domestic laws, and the prohibitions apply to their executive branches as well as to private persons. The executive (military, law enforcement, intelligence, surveillance, governmental CSIRT[46] or other designated authority or entity) is only allowed to engage in cyber defence activities which would normally constitute an offence if a legal authorisation or justification exists.

The state authorities are limited in conducting RCD not only by criminal law, but also by other areas of public law. For example, the processing of personal data is regulated by Council of Europe conventions[47] and by EU law, as implemented in domestic law.[48] Also, when considering RCD, telecommunications law has to be taken into account.[49] For example, a sound regulatory framework for data retention and preservation is the prerequisite for a correct identification of the attacker in the attribution stage of RCD. In the EU, the Data Retention Directive[50] obliged the member states to have internet service providers retain all traffic data (but not content) for between 6 months and 2 years, which would allow the countries to use the retained data for RCD purposes, as long as they set clear limits and responsibilities in their domestic laws. However, the Directive was invalidated by a judgment of the Court of Justice of the European Union on 8 April 2014.[51] The Court did not rule out the idea of data retention, it only invalidated the Directive on the basis of its vagueness, so the EU can regulate data retention anew, while the national laws adopted in transposition of the invalidated Directive are mostly still in place.

B) Justification for RCD by self-defence and necessity in domestic law

Regarding the provisions on cyberattacks within domestic law,

[45] For EU Member States, an even stricter harmonisation is provided for by the 2013/40/EU Directive (on attacks against information systems and replacing Council Framework Decision 2005/222/JHA). http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:EN:PDF

[46] Computer Security Incident Response Team.

[47] For example, the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Strasbourg, 28 January 1981), Additional Protocol to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data Regarding Supervisory Authorities and Transborder Data Flows (Strasbourg, 8 November 2001).

[48] See a legal summary at http://europa.eu/legislation_summaries/information_society/legislative_framework/l24120_en.htm

[49] E.g. Constitution and Convention of the International Telecommunication Union, as amended, and other basic documents of the ITU: http://www.itu.int/dms_pub/itu-s/oth/02/09/s02090000115201pdfe.pdf For the NATO member states which are also EU members, see a legal summary at http://europa.eu/legislation_summaries/information_society/legislative_framework/index_en.htm

[50] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32006L0024&qid=1396945634895

[51] Judgment of the Court (Grand Chamber) of 8 April 2014, Digital Rights Ireland Ltd (C-293/12) v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung (C-594/12) and Others, available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62012CJ0293.

prompted by the Convention on Cybercrime, most states recognise two justifications for RCD: self-defence[52] and necessity. These terms have to be distinguished from "self-defence and necessity" in international law.

The notions of self-defence and necessity in domestic law allow the victims of attacks, or of threats, to defend against them by resorting to acts otherwise prohibited by law. However, the exact provisions vary in different jurisdictions. They can vary in their scope (i.e. whether a cyberattack can be considered an attack, or threat, even though it does not cause damage to a physical object), as well as in the underlying conditions (e.g. proportionality and subsidiarity).

Can self-defence and necessity be used to justify state actions? They are primarily meant to exculpate natural and legal persons. The underlying theory is that the state shares its monopoly on violence with private persons in a situation where it is unable to act via its agents due to the urgency of the situation. According to some authors, public authorities cannot directly invoke self-defence or necessity as the basis for their activities, because they are bound by the principle of a constitutionally limited government, which prevents them from taking part in activities which are not specifically allowed by the law.[53]

Although this argument is a powerful one, some countries have developed a more tolerant approach to the application of self-defence and necessity to government activities. According to the prevalent criminal jurisprudence in Germany, it is not easy to separate the private and public spheres. Hence, self-defence and necessity are both considered universal legal principles which can be invoked by public authorities. Constitutional and administrative law both generally recognise that even though the clauses are rather general, they can enable the public authorities to take action based on self-defence or necessity.[54]

The authors of this article take a compromise position. The justification of governmental RCD activities by self-defence or necessity is considered possible but impractical. Their legality would have to be decided by the law enforcement authorities on a case-by-case basis, and the potential liability issues, including those associated with third parties, render this approach rather risky. States that wish to develop RCD capabilities should therefore base them on a more stable foundation by enacting special provisions in their respective domestic laws.[55,56] This approach would allow a constitutional

[52] In some jurisdictions, the notion is labelled more accurately as "necessary defence", because it is commonly applied to a defence of another.
[53] Cf. Rudolphi, H.J., *et al*., *Systematischer Kommentar zum Strafgesetzbuch*. Bonn: Luchterhand, 2003. S7 to § 32 StGB.
[54] See the commentary on necessity ("Notstand") in *Schönke-Schröder, Strafgesetzbuch, Kommentar. 28. Auflage*. Verlag C.H. Beck, München, 2010, page 659.
[55] The need for a regulatory framework for RCD/ACD activities is emphasised by Jay P. Kesan and Carol

review of such provisions by the national judiciary, or other bodies, but it would also improve the predictability of the law for the operators and the public at large.

www.nato.int

A Way Ahead

RCD is not a panacea and requires a thorough examination by states which wish to employ it. Still, it can be considered as one of the available solutions. Implemented within a well-defined framework, RCD can be a middle path for states to retrieve their sovereignty in cyberspace.

International law provides a framework that is relevant for states which plan to conduct RCD activities even though its implementation does still pose a challenge as its spectrum can seem limited. However, used carefully, it remains an appropriate tool to address cyberattacks perpetrated by state-actors. In domestic law, even with a specific basis, it is very likely that RCD will still be considered as an extraordinary measure, and there will be prerequisites regarding its deployment, but such specific legal provisions will likely prove to be more reliable than invoking self-defence and necessity. A certain analogy can also be drawn between RCD and certain law enforcement tasks, e.g. provision of security, protection of life and property or maintenance and restoration of order. The RCD legislation could be crafted in a similar way.

The recent modification of the French legislation regarding the defence of vitally important information systems offers a good example. The provisions

---

M. Hayes, "Mitigative Counterstriking: Self-Defence and Deterrence in Cyberspace," *Harvard Journal of Law & Technology*, Volume 25, Number 2 Spring 2012, page 462, 464, 473, 494 and 521, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1805163

[56] For example, France has introduced the concept of active response to a cyberattack in its Defence Code, Article L2321-2: http://www.legifrance.gouv.fr/affichCode.do?idArticle=LEGIARTI000028342544&idSectionTA=LEGISCTA000028345135&cidTexte=LEGITEXT000006071307&dateTexte=20140127

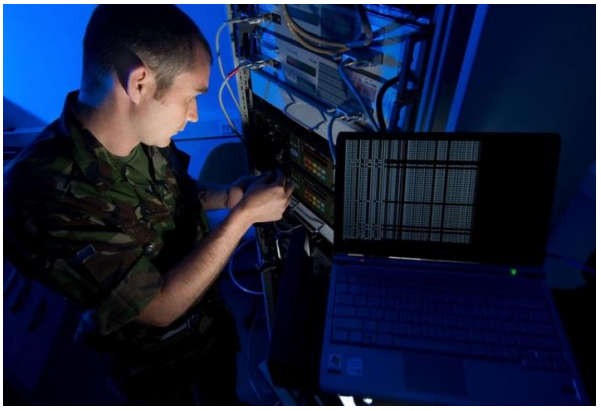
introduced in the Military Planning Act 2014 - 2015[57] are designed to provide French cyber security operators with a clear legal framework and to overcome the shortcomings of the current regulations that do not allow state agencies to intervene actively during a cyber incident.[58] The rationale for this new regulation is to be able to block or stop an attack and it is not intended to constitute an offensive action such as a denial of service. Moreover, it is to be noted that its scope is narrow and there is little doubt that the coming implementation act shall provide for thorough limitations.

In this article, Responsive Cyber Defence was introduced as a time-limited subset of Active Cyber Defence, and its possible justifications were explored. While not ruled out completely, justification, both in international and domestic law, is viewed only as an emergency option, and enacting specific RCD legislation is recommended.

***

[57] "Loi de programmation militaire" – French Military Planning Act of 18th December 2013 in French, http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000028338825&dateTexte&categorieLien=id

[58] Article L. 2321-2 of the Defence Code in French: http://www.legifrance.gouv.fr/affichCode.do;jsessionid=50D91549E234E046C0CC0EAA73C9D07F.tpdjo02v_2?idSectionTA=LEGISCTA000028345135&cidTexte=LEGITEXT000006071307&dateTexte=20140410



www.nato.int

Examining the Threshold of "Armed Attack" in light of Collective Self-Defence against Cyber Attacks: NATO's Enhanced Cyber Defence Policy

by Florentine J.M. de Boer[1]

Introduction

Recently, NATO endorsed its Enhanced Cyber Defence Policy during the Wales Summit on 4 and 5 September 2014. In the Wales Summit Declaration, NATO confirms that "*cyber defence is part of NATO's core task of collective defence.*"[2] The Wales Summit Declaration explicitly recognises that cyber attacks are regulated by international law and that Article 5 of the North Atlantic Treaty[3] can be invoked if the North Atlantic Council (NAC) so decides. In order to trigger Article 5, the cyber attack must reach the threshold of "armed attack."

NATO's new policy adopts the existing threshold of "armed attack" from international law.[4] The policy recognises that cyber attacks could cause

---

[1] Florentine J. M. de Boer was a Legal Fellow at NATO SCHOOL Oberammergau from May - October 2014. She obtained her LL.B. and LL.M. at Leiden University, the Netherlands. I would like to thank Lt Col Brian Bengs for his advice and guidance. The views expressed in this article are solely those of the author and may not represent the views of NATO, ACO, ACT, NATO SCHOOL Oberammergau, or NATO member countries.

[2] Wales Summit Declaration issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales (5 September 2014) para. 72 <http://www.nato.int/cps/en/natohq/official_texts_112964.htm> accessed 22 September 2014.

[3] The official text of the North Atlantic Treaty, or otherwise known as the Washington Treaty, is available at <http://www.nato.int/cps/en/natolive/official_texts_17120.htm> accessed 22 September 2014.

[4] Wales Summit Declaration (n 2); Klara Tothova Jordan, 'Reexamining Article 5: NATO's Collective Defense in Times of Cyber Threats' *The Huffington Post* (13 June 2014) <http://www.huffingtonpost.com/klara-tothova-jordan/reexamining-article-5-nat_b_5491577.html> accessed 22 September 2014; NATO Cooperative Cyber Defence Centre of Excellence, 'NATO Summit to Update Cyber Defence Policy', *International Cyber Developments Review (INCYDER)* Q2 (2014) <https://www.ccdcoe.org/sites/default/files/publications/articles/INCYDER%202014Q2.pdf> accessed 22 September 2014; Steve Ranger, 'NATO updates cyber defence policy as digital attacks become a standard part of conflict' *ZDNet* (30 June 2014) <http://www.zdnet.com/nato-updates-cyber-defence-policy-as-digital-attacks-become-a-standard-part-of-conflict-7000031064/> accessed 22 September

effects equally severe as the effects of conventional armed attacks and could therefore pose a serious threat to the security of States and the Alliance.[5] As usual, it is left to the NAC (member countries) to decide whether the criteria for invoking Article 5 have been met in a particular situation. Member countries' cyber defence policies can and do differ as they try to keep up with the rapid technological developments and some member countries already, or will, support a different threshold of "armed attack."[6] This raises two important questions that will be examined in this article: What is a "cyber armed attack"? What are the implications of NATO's Enhanced Cyber Defence Policy for collective self-defence under Article 5?[7]

Cyber armed attack

Collective self-defence expressed in Article 5 is a well-known fundamental principle of NATO: "*an armed attack against one or more of them in Europe or North America shall be considered an attack against them all* (…)".[8] Therefore, if an armed attack occurs, the right of individual or collective self-defence may be invoked. If the NAC decides to activate Article 5, NATO member countries will assist the attacked State in whatever manner they deem necessary. What attacks reach the threshold of an "armed attack" and trigger the application of Article 5?

Unfortunately, neither the text of Article 5 nor Article 51 of the UN Charter[9] contain an explanation of the threshold required for an armed attack to have occurred, thus there is no clear definition available.[10] Article 5 has only been invoked once in NATO's history, so practice offers little guidance.[11] Additionally, the International Court of Justice (ICJ) did not define "armed attack" when it discussed the right of self-defence. Instead, the ICJ gave a few indications of attacks that qualify or could qualify as

---

2014.

[5] Wales Summit Declaration (n 2) para. 72.

[6] Terry D. Gill and Paul A. L. Ducheine, "Anticipatory Self-Defense in the Cyber Context" (2013) 89 Int'l L. Stud. 438, 444.

[7] The author recognizes that there are also other options available to respond to cyber attacks. Additionally, the right to self-defence is an inherent right of States thus the North Atlantic Treaty is not a prerequisite to exercise this right. It is therefore important to note that this article focuses solely on the threshold of "armed attack" in the context of collective self-defence under Article 5 of the North Atlantic Treaty. Other debates fall outside the scope of this article.

[8] Article 5 North Atlantic Treaty (n 3).

[9] The full text of the Charter of the United Nations, or UN Charter, is available at <http://www.un.org/en/documents/charter/> accessed 22 September 2014.

[10] Article 5 not only refers to Article 51 of the UN Charter, but the majority of the text also derives from that Article. UN Charter (n 9).

[11] Article 5 of the North Atlantic Treaty was for the first time invoked when the terrorist attacks occurred against the United States on 11 September 2001. "NATO and the Scourge of Terrorism" (18 February 2005) <http://www.nato.int/terrorism/five.htm> accessed 20 September 2014; On 12 September 2001 "*The Council agreed that if it is determined that this attack was directed from abroad against the United States, it shall be regarded as an action covered by Article 5 of the Washington Treaty* (…)". "Statement by the North Atlantic Council" Press Release (2001)124 (*NATO Press Releases*, 12 September 2001) <http://www.nato.int/docu/pr/2001/p01-124e.htm> accessed 23 October 2014.

"armed attacks."[12]

The Tallinn Manual on the International Law Applicable to Cyber Warfare ("Tallinn Manual") was produced by an International Group of Experts and provides a thorough analysis of the application of international law to cyber warfare, including the right of self-defence with respect to cyber attacks.[13] The Experts also examined whether the indications the ICJ gave with regard to "armed attack" can apply to cyber attacks. The ICJ indicated in the Nicaragua case that it depends on the scale and effects of an attack to determine whether it amounts to an armed attack.[14] The ICJ concluded that only "*the most grave forms of the use of force* (…)"[15] reach the threshold of "armed attack."[16] An attack must therefore surpass the threshold of "the use of force"[17] to reach the threshold of "armed attack."[18] In short, the focus is not on the type of weapon employed but on the scale and effects of the attack.[19]

Consequently, the International Group of Experts determined that a cyber attack can reach the threshold of "armed attack" if the effects caused are equivalent to the effects of (traditional) kinetic attacks.[20] Put differently, a cyber attack can reach the threshold of "armed attack" if the gravest forms of force have been used and the attack results in physical damage, destruction, injury or death. For example, a cyber attack that involves the

---

[12] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua* v. *United States of America), Merits, Judgment, I.C.J. Reports 1986*, p. 14, para. 191 and 195; *Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, I.C.J. Reports 1996,* p. 226, para. 39; *Oil Platforms (Islamic Republic of Iran v. United States of America), Judgment, I.C.J. Reports 2003*, p. 161, para. 64 and 72.

[13] More specifically, the Tallinn Manual looks at the *jus ad bellum* and the *jus in bello*. The Tallinn Manual does not represent the view of NATO but it was produced at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence. Michael N. Schmitt (ed), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press 2013) 4 and 11.

[14] Nicaragua case (n 12) para. 195.

[15] Nicaragua case (n 12) para. 191.

[16] ibid.

[17] Again, "use of force" is not clearly defined and neither Article 1 of the North Atlantic Treaty nor Article 2(4) of the UN Charter contains an explanation. Nevertheless, the *travaux préparatoires* of the UN Charter provide that 'force' must be more than mere political and economic coercion. Christine Gray, "The Use of Force and the International Legal Order" in Malcolm D. Evans (ed), *International Law* (Third Edition, Oxford University Press 2010)618; M. Schmitt, "Computer Network Attacks and the Use of Force in International Law: Thoughts on a Normative Framework" (1999) 37 Colum. J. Transnat'L. 885, 905 nn 58-59; The ICJ indicated that "force" does not merely have to be "armed force" but that arming and training armed forces could also amount to the threat or use of force. However, merely providing financial support would not reach the threshold. Nicaragua case (n 12) para. 228.

[18] There are two thresholds: one for "the use of force" and one for "armed attack". All armed attacks surpass the threshold of "the use of force" while not all uses of force reach the threshold of armed attack. Nicaragua case (n 12) para. 191; Michael N. Schmitt, "The Law of Cyber Warfare: Quo Vadis?" (2014) 25 Stanford Law & Policy Review 269, 282.

[19] Nuclear Weapons Advisory Opinion (n 12) para. 39.

[20] Schmitt (n 13) 54-56; See also Robin Geiß and Henning Lahman, "Freedom and Security in Cyberspace: Shifting the Focus away from Military Responses towards Non-Forcible Countermeasures and Collective Threat-Prevention" in Katharina Ziolkowski (ed), *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy* (NATO Cooperative Cyber Defence Centre of Excellence 2013) 622 n 3.

infiltration of air traffic control systems and causes planes to crash could reach the threshold of "armed attack" as it results in damage, destruction, injury, and most likely death.[21] Another example of a "cyber armed attack" the Tallinn Manual provides is "*if a group of private individuals under the direction of State A undertakes cyber operations directed against State B, and the consequence of those actions reaches the requisite scale and effects* (…)."[22]

This approach leaves out cyber attacks that have serious consequences without actually causing physical damage, destruction, injury or death. Consider for example a cyber attack that targets the financial system of a State or other critical infrastructure, such as SCADA[23] networks, severely affecting the functioning of a State or even causing a State to be paralysed. It appears disproportionate that these cyber attacks would not reach the threshold of armed attack, while their effects may be more severe, long-lasting and on a greater scale than other effects caused by traditional armed attacks. For example in the Oil Platforms case, the ICJ mentioned that "*the mining of a single military vessel might be sufficient to bring into play the 'inherent right of self-defence'* (…)."[24] Thus if the mining of a single military vessel could reach the threshold, why not a cyber attack that targets critical infrastructure and paralyses a State without causing physical damage, destruction, injury or death?

Several authors and experts support the qualification of disruptive cyber attacks as an "armed attack", albeit they do not cause physical damage, destruction, injury or death.[25] Schmitt, who served as the Director of the Tallinn Manual project, points out that current international law simply does not (yet) allow such cyber attacks to constitute an "armed attack."[26] Nevertheless, it is

---

[21] Jordan (n 4); The International Group of Experts of the Tallinn Manual agreed that in determining whether an attack constitutes an "armed attack", "*all reasonably foreseeable consequences of the cyber operation* (…)" should be considered. Furthermore, the Experts could not all agree on whether intention is required with regard to the effects of an attack. However, "*The majority of the International Group of Experts took the view that intention is irrelevant in qualifying an operation as an armed attack and that only the scale and effects matter*". A response must nevertheless be proportionate and necessary. Schmitt (n 13) 57.

[22] Schmitt (n 13) 58; The example is based on the definition the ICJ provides in the Nicaragua case of an armed attack with the use of Article 3(g) of the Definition of Aggression. Nicaragua case (n 12) para. 195; The ICJ gave another example in the Oil Platforms case. The ICJ held that "*the mining of a single military vessel might be sufficient to bring into play the 'inherent right of self-defence'* (…)". An attack on a ship that is merely owned by a State but that is not flying the flag of that State did not qualify as an armed attack. Oil Platforms case (n 12) para. 64 and 72.

[23] Supervisory Control and Data Acquisition (SCADA). 'Cyber Threats: Issues and Explanations' <http://www.unicri.it/special_topics/securing_cyberspace/cyber_threats/explanations/> accessed 22 September 2014.

[24] Oil Platforms case (n 12) para. 72.

[25] Marco Roscini, Cyber Operations and the Use of Force in International Law (Oxford University Press 2014) 74; See also Nicholas Tsagourias, "Cyber attacks, self-defence and the problem of attribution" (2012) 17 Journal of Conflict & Security Law 229, 231; Gill and Ducheine (n 6) 444-445; Sean Watts, "Low-Intensity Computer Network Attack and Self-Defense" (2011) 87 International Law Studies 59, 60; Schmitt (n 18) 283; Schmitt (n 13) 56-57.

[26] Schmitt (n 18) 283; See also Roscini (n 25) 74.

worrisome that States would not be able to lawfully respond to such attacks with force. The international community already had a preview of the potential of such cyber attacks in the cases of Estonia in 2007 and Georgia in 2008.[27] The disruptive cyber attacks could become increasingly popular since they currently fall below the threshold of "armed attack" and States are unable to respond with force in self-defence.[28] Consequently, this leaves room for adversaries to exploit these types of cyber attacks and it diminishes the deterrent effect of Article 5 in light of cyber attacks.[29]

Authors are not the only ones to advocate for a more progressive view of "armed attacks"; in several NATO member countries interesting developments occurred with regard to their policies on cyber defence.[30] For example, the United States and the Netherlands have been re-examining the threshold. The examples of the United States and the Netherlands indicate the current developments with regard to threshold and demonstrate to what extent national cyber defence policies can differ from the existing threshold. Additionally, it is important to further examine these developments as they indicate what the criteria could be for a cyber attack without physical consequences to constitute an "armed attack."

www.nato.int

Developments in the United States and the Netherlands

In a reply to the Report of the UN Secretary General on "Developments in the Field of Information and Telecommunications in the Context of International Security", the United States found that "*under some circumstances, a disruptive activity in cyberspace could constitute an armed attack.*"[31] Additionally, an assessment of the U.S. Department of Defense ("DoD") explains that,

---

[27] Christian Czosseck, "State Actors and their Proxies in Cyberspace" in Ziolkowski (n 20) 14-15; Watts (n 25) 69-71.
[28] Watts (n 25) 60.
[29] Ranger (n 4).
[30] Schmitt (n 18) 283-284; Roscini (n 25) 74-75; Gill and Ducheine (n 6) 444.
[31] Schmitt (n 18) 283 n 53; Roscini (n 25) 74 n 209.

> *"there may be a right to use force in self defense against a single foreign electronic attack in circumstances where significant damage is being done to the attacked system or the data stored in it, when the system is critical to national security or to essential national infrastructures, or when the intruder's conduct or the context of the activity clearly manifests a malicious intent."*[32]

In the Netherlands, the Advisory Council on International Affairs ("AIV") and the Advisory Committee on Issues of Public International Law ("CAVV") presented a report on cyber warfare to the Dutch government. The report states that "*A serious, organised cyber attack on essential functions of a state could conceivably be qualified as an 'armed attack' within the meaning of Article 51 of the UN Charter if it could or did lead to serious disruption of the functioning of the state or serious and long-lasting consequences for the stability of the state.*"[33] The disruptive attack must be aimed at the State and/or society. Mere annoyance or delay in the exercise of State functions would not amount to an armed attack.[34]

In a response to the report, the Dutch government stated that it largely adopts the report of the CAVV and AIV.[35] Other sources, however, indicate that the Dutch Government has adopted the report.[36]

It appears that the developments in the United States and the Netherlands demonstrate support for a lower threshold of "armed attack" since highly disruptive cyber attacks are described as able to constitute an "armed attack." However, the section in the Wales Summit Declaration implies that NATO's Enhanced Cyber Defence Policy adopts the existing threshold of "armed attack" from international law as it says that the impact of cyber attacks "*could be as harmful to modern societies as a conventional attack.*"[37] What are the implications of NATO's Enhanced Cyber Defence for collective defence?

---

[32] United States Department of Defense Office of General Counsel, An Assessment of International Legal Issues in Information Operations (May 1999) 18 <http://www.au.af.mil/au/awc/awcgate/dod-io-legal/dod-io-legal.pdf> accessed 22 September 2014.

[33] The report provides as examples the targeting of the entire financial system or the entire military communication and command network. Advisory Council on International Affairs (AIV) and Advisory Committee on Issues of Public International Law (CAVV), 'Cyber Warfare No. 77, AIV/No. 22, CAVV' (December 2011) 21 <http://www.aiv-advies.nl/ContentSuite/upload/aiv/doc/webversie_AIV77CAVV_22_ENG.pdf> accessed 22 September 2014.

[34] ibid.

[35] Government of the Netherlands, 'Government response to the AIV/CAVV report on cyber warfare' 5 <http://www.aiv-advies.nl/ContentSuite/template/aiv/adv/collection_single.asp?id=1942&adv_id=3016&page=regeringsreacties&language=UK> accessed 22 September 2014; Schmitt (n 18) 284.

[36] Among them is an article written by Terry D. Gill and Paul A. L. Ducheine. Prof. Gill is also a member of the CAVV, which jointly with the AIV produced the advisory report on cyber warfare. See Gill and Ducheine (n 6) 444 n 9.

[37] Wales Summit Declaration (n 2).

NATO's readiness to respond to cyber attacks

While it is exciting that, according to the Wales Summit Declaration, NATO's Enhanced Cyber Defence Policy for the first time explicitly mentions that Article 5 can be invoked in case of cyber attacks, it is unfortunate that there is no more guidance on criteria for cyber attacks to reach the required threshold. Indeed, there is no definite procedure available with regard to Article 5. The decision to invoke Article 5 is a political decision as it is taken by the member countries through the NAC, NATO's principal political decision-making body.[38] A general challenge for the NAC is to take decisions by consensus as views will differ among 28 sovereign States. Similarly, States have different views on the threshold of "armed attack" in the context of cyber attacks.

The threshold of "armed attack" is generally understood to entail physical damage, destruction, injury or death. However, some States already, or will, support a lower threshold to include highly disruptive cyber attacks without physical consequences.[39] It may require a long debate to reach agreement on whether such cyber attacks constitute an "armed attack" and trigger the application of Article 5. The controversy surrounding the threshold is also demonstrated by the fact that the International Group of Experts, consisting of legal practitioners, academics, and technical experts, could not agree on whether cyber attacks without physical consequences qualify as armed attacks.[40] Likewise, it will be a significant challenge for the NAC to reach agreement on whether the threshold has been reached.

NATO not only faces general challenges as described above in the case of cyber attacks, but cyber attacks also pose a particular challenge to NATO. National policies on cyber defence will differ even more due to rapid technological developments and growing technological capabilities. States are having a hard time keeping up with all the developments. Some States have more progressive cyber defence policies, whereas other States opt for a conservative policy. Additionally, no cyber attack has thus far been publicly declared as an "armed attack" by a State.[41] A particular issue of the disruptive cyber attacks is that their effects are so remote from the effects of traditional attacks that reach the threshold of "armed attack." Cyber attacks are capable of doing so much more without actually causing physical damage, destruction, injury or death. The effects of disruptive cyber attacks do not correspond with the described effects and examples given by the ICJ. Consequently, States could be or are more reluctant to recognise certain disruptive cyber attacks without physical consequences as "armed attacks."

---

[38] "The North Atlantic Council" (5 March 2012) <http://www.nato.int/cps/en/natolive/topics_49763.htm> accessed 30 September 2014.
[39] Schmitt (n 18) 283.
[40] Schmitt (n 13) 9 and 56-57; Gill and Ducheine (n 6) 444 n 9.
[41] Schmitt (n 13) 57.

By invoking Article 5 in response to the terrorist attacks of 9/11, NATO member countries demonstrated that they could quickly reach an agreement and take a step forward.[42] Nevertheless, taking a step forward with regard to the threshold of "armed attack" may encounter more resistance from individual member countries. It could be "dangerous" to set a precedent with regard to the criteria for highly disruptive cyber attacks to constitute an "armed attack." Both thresholds of "the use of force" and "armed attack" must be preserved and the latter must remain higher. If the threshold is lowered too much, more cyber attacks would reach the threshold and it would become easier for States to use force in self-defence.[43] The standard must remain sufficiently high to ensure that only the gravest forms of cyber attacks can trigger the application of Article 5.

A long debate will be required to determine whether Article 5 can be invoked in the case of a highly disruptive cyber attack without effects equivalent to traditional armed attacks. The envisaged disagreement on the threshold of "armed attack" in cases of cyber attacks could have an adverse effect on NATO's ability to swiftly respond to a cyber attack. There is a significant risk in waiting until such a cyber attack occurs to decide whether the criteria are met to trigger the application of Article 5. NATO's ability to swiftly respond will not only be severely hampered, but it may also entirely prevent NATO to respond collectively with force. When the NAC is unable to reach consensus, the NATO ally that is the object of a serious cyber attack without physical consequences, is left without one of the crucial benefits of being a member of NATO. The member country would be unable to rely on collective self-defence under Article 5.

Conclusion

For cyber attacks to reach the threshold of "armed attack" and trigger the application of Article 5, the cyber attacks would have to cause physical damage, destruction, injury or death equivalent to the effects that traditional armed attacks cause. It is understandable that NATO via its member countries would maintain a threshold that currently exists; nevertheless, a lower threshold of "armed attack" appears to be gaining support in light of the rapid technological developments and growing technological capabilities. If NATO is not able to anticipate the debate on the threshold of "armed attack," NATO's readiness will be adversely affected and NATO may see the value of its cornerstone, Article 5, diminish.

***

[42] Edgar Buckley, "Invocation of Article 5: Five Years On (Invoking Article 5)" (2006) NATO Review summer 2006 <http://www.nato.int/docu/review/2006/issue2/english/art2.html> accessed 21 October 2014.

[43] Michael N. Schmitt, "Attack" as a Term of Art in International Law: The Cyber Operations Context" in C. Czosseck, R. Ottis and K. Ziolkowski (eds), 2012, 4th International Conference on Cyber Conflict (NATO Cooperative Cyber Defence Centre of Excellence, 2012) 288.

www.nato.int

Cyber Warfare and NATO Legal Advisors

by Dr. Gary D. Solis[1]

Introduction

Cyber warfare issues could not have been imagined by the International Committee of the Red Cross's Committees of Experts who wrote the 1949 Geneva Conventions[2] – or those who created the 1977 Additional Protocols I[3] and II[4] that supplement the 1949 Conventions. Today, military commanders may ask their legal advisors, does existing Law of Armed Conflict (LOAC) even apply to cyber issues? It certainly does.

The Statute of the International Court of Justice (ICJ) tells us the sources of International law that the Court looks to: first, international conventions, then international custom. Next the Court considers "*general principles of law recognized by civilized nations*," then judicial decisions and, finally, it looks to "*the teachings of the most highly qualified publicists of the various nations*…."[5] When it comes to cyber warfare, however, there are no international conventions, no custom, and no judicial decisions to look to. For now, we must depend on general principles of law and the writings of publicists and

[1] Gary Solis, a retired US Marine Corps Judge Advocate, directed West Point's law of war program for six years. He teaches the law of war at Georgetown University Law Center, and at Georgetown University Law School. JD, University of California at Davis; LL.M. (criminal law), George Washington University Law; Ph.D. (law of war), The London School of Economics & Political Science. This article draws from his recent longer article on the same topic. The views expressed in this article are solely those of the author and may not represent the views of NATO, ACO or ACT.

[2] Geneva Conventions on protection of victims of armed conflicts I – IV, 1949.

[3] Additional Protocol to the Geneva Conventions of 12 August 1949, and relating to the protection of victims of international armed conflicts (API).

[4] Additional Protocol II to the Geneva Conventions of 12 August 1949, and relating to the protection of victims of non-international armed conflicts (APII).

[5] Statute of the International Court of Justice, Art. 38.1 (June 26, 1945).

scholarly publications.

As the ICJ wrote in its 1996 Nuclear Weapons Advisory Opinion, LOAC applies to "*any use of force, regardless of the weapons employed*."[6] Whether a 500-pound kinetic bomb or a computer's electronic keystroke, a weapon is a weapon, and is subject to LOAC. Still, cyber warfare presents military legal advisors with difficulties because so many aspects of cyber warfare are unsettled or unconsidered by modern LOAC…so far. There are no multinational conventions, no protocols or treaties relating directly to cyber warfare, although they are surely being considered by cyber-aware states. There is no cyber warfare experience that rises to "*international custom*," or "*general principles recognized by civilized nations*" to turn to for unambiguous answers to cyber legal matters. There are no cyber-specific norms, and State practice is slow to evolve. The few judicial decisions that consider cyber delicts relate to domestic cyber crime, rather than violations of international law or its subset, LOAC. American and European law journals are flush with articles on cyber crime but few consider cyber warfare.[7] So far, there is not even agreement as to whether cyber warfare is one word or two.

Despite an absence of specific references in traditional LOAC sources, there are reliable analogous guidelines to the law of cyber warfare found in the 1949 Geneva Conventions and their 1977 Protocols. After the 2007 attack on Estonia involving cyber intrusions,[8] is there a legal advisor to any military commander who doesn't recognise the need to be as current as possible on the rapidly evolving law of cyber warfare? When command networks are regularly hacked by State actors and civilian agents of States?[9] When military aircraft control systems are taken over by unknown intruders?[10] When advanced weapon systems are subject to wholesale theft?[11] Examples of cyber intrusions that threaten combatant forces around the world are numerous and constant.

Good work is being done in capturing basic international cyber warfare legal norms and NATO and NATO Nations have been at the forefront of that work; notably, the NATO Cooperative Cyber Defence Centre of Excellence, based in Tallinn, Estonia. The Tallinn Manual on Cyber Warfare,[12] produced under the expert leadership of Professor Michael N. Schmitt, of the US Naval

---

[6] Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1995, I.C.J. 226-67, ¶ 39, July 8, 1996).

[7] Notable journal exceptions are the *Military Law Review*, published by the US Army's Judge Advocate General's Legal Center & School, and the *International Review of the Red Cross*. Doubtless there are others of which the author is unaware.

[8] Jason Healey, "A Brief History of US Cyber Conflict," in Jason Healey, ed., *A Fierce Domain: Conflict in Cyberspace* (Vienna, VA: Cyber Conflict Studies Assn., 2013), at 14, 68.

[9] J.P. London, "Made in China," *US Naval Institute Proceedings* (April 2011), at 54, 56.

[10] "Virus Hits Networks Used for Drone Flights," *Wash. Post*, (9 Oct. 2011), at A7.

[11] Richard A. Clarke & Robert K. Knake, *Cyber War* (NY: Ecco, 2010), at 233.

[12] Michael N. Schmitt, ed., *The Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge, Cambridge University Press, 2013).

War College, is a leading text on cyber warfare that every military legal advisor would do well to read. This issue of the NATO Legal Gazette is further evidence of NATO's forward thinking in the cyber arena.

Cyber Misunderstandings

There are widespread cyber warfare misunderstandings. Foremost among them is that all cyber intrusions are cyber attacks. The term "cyber attack" is frequently applied in the media to a broad range of cyber conduct that falls outside the boundaries of an attack, as that term is defined in the LOAC.[13]

For either international or non-international armed conflicts, an excellent definition of "cyber attack" is: a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury, or death to persons, or damage or destruction to objects.[14] *"[The definition of cyber attack] should not be understood as excluding cyber operations against data (nonphysical entities, of course) from the ambit of the term attack. Whenever an attack on data results in injury or death of individuals or damage or destruction of physical objects, those individuals or objects constitute the 'object of attack' and the operation therefore qualifies as an attack."*[15] Cyber theft, cyber intelligence gathering, and cyber intrusions that involve only brief or periodic interruption of non-essential cyber services, do not qualify as cyber attacks. Cyber espionage does not constitute a cyber attack. Nor does the hacking of a State's military command network, alone, constitute an attack.

Without a loss of life or injury, or destruction or damage to objects, a cyber manipulation or intrusion, by itself, does not automatically indicate hostile intent. An intrusion may be considered akin to a military aircraft being tracked by enemy radar, but not locked into a missile fire control system.

A "sneak" cyber attack occurring during a period when hostilities were not previously in progress, raises *jus ad bellum* issues; was the conflict-initiating attack a lawful resort to armed force? A cyber attack in the course of an on-going armed conflict, however, is a tactical event that can only raise *jus in bello issues.*

There has been confusion as to whether or not an entry for malicious purposes into the control systems of a State's critical national infrastructure – telecommunications, electrical power systems, gas and oil storage and

---

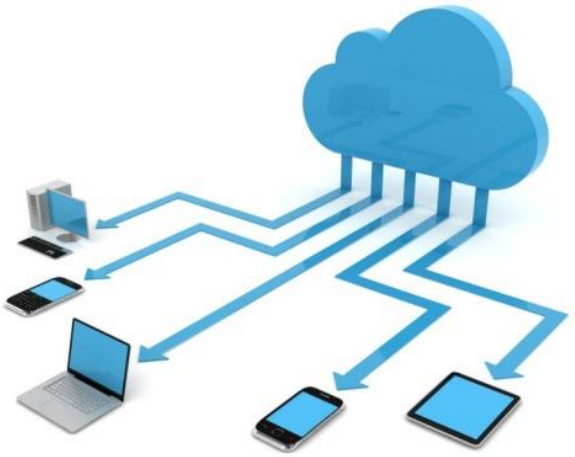
[13] Attack means acts of violence against the adversary, whether in offence or in defence. Article 49 Additional Protocol I to the Geneva Conventions of 12 August 1949, and relating to the protection of victims of international armed conflicts.

[14] Michael N. Schmitt, ed., *The Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge, Cambridge University Press, 2013). A trans-border element is added in the *Manual's* Rule 13, at 54.

[15] Michael N. Schmitt, ed., *The Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge, Cambridge University Press, 2013), Rule 30.6 at 107-08.

transportation, banking and finance, water supply systems, and continuity of government, for example – would constitute an attack.

"*The mere manipulation of a banking system or other manipulation of critical infrastructure, even if it leads to serious economic loss, would probably stretch the concept of armed force...But the disruption of such vital infrastructure as electricity or water supply systems, which would inevitably lead to severe hardship for the population if it lasted over a certain period, even if not to death or injury, might well have to be considered as armed force....*"[16]



www.nato.int

The confusion is, in part, a result of critical infrastructure systems being civilian controlled while corporate civilian entities are beyond the direction of a State's defense officials. Civilian corporations have been resistant to defence officials' pleas to install costly anti-intrusion systems. At the same time, defence authorities have been reluctant to accept responsibility for weakly defended critical civilian systems. That defense authority view seems to be changing. In some countries, such as the US, it seems to be discarded entirely and a cyber intrusion/attack on critical national infrastructure will be viewed as raising a right to armed response, should loss of life, or injury, or damage or destruction of objects, be a reasonably foreseeable result.[17] Legal advisors should particularly be aware of their nation's approach to the protection of critical national infrastructure – and further aware that the approach that could be taken to cyber attacks on critical national infrastructure does not enjoy international agreement.

[16] Cordula Droege, "Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians," 94/886 *Int'l Rev. of the Red Cross*, at 548 (Summed 2012).

[17] This US policy is evidenced in Presidential Policy Directive 20, "U.S. Cyber Operations Policy (Oct. 2012), at 6, as well as Executive Order 13231, "Critical Infrastructure Protection in the Information Age (16 Oct. 2001), at § 1.

Another common error in thinking of cyber attacks is that electric impulses cannot constitute an "armed" attack justifying an armed counter-attack. Whether a cyber attack constitutes a use of armed force matters, because UN Charter Article 51 requires that an armed counter-attack, if any, be a response not to a use of force, but to a use of "armed force."

A surprise cyber attack mounted without actual physical force of arms is an armed attack in the same way that surprise attacks by means of lethal gas or deadly chemicals constitute armed attacks. International law scholar Yoram Dinstein observes, "*[w]henever a lethal result to human beings – or serious destruction to property – is engendered by an illegal use of force by State A against State B, that use of force will qualify as an armed attack. The right to employ counter-force in self-defense against State A can then be invoked by State B…*"[18] Professor Dinstein continues, "*From a legal perspective, there is no reason to differentiate between kinetic and electronic means of attack. A premeditated destructive [computer network attack] can qualify as an armed attack just as much as a kinetic attack bringing about the same…results. The crux of the matter is not the medium at hand (a computer server in lieu of, say, an artillery battery), but the violent consequences of the action taken*."[19]

While appreciating that the answers are not firmly agreed upon, military legal advisors should be prepared to correct these and other common cyber misconceptions of commanders, the media, or elected officials.

Cyber conflict classification

Conflict classification of cyber attacks can be complex. An international armed conflict must by definition be "armed" and must be "international." In considering the international aspect of a common Article 2 of the Geneva Conventions, international conflict, if a cyber attack were launched from Blueland against Redland by an individual, or a group of individuals acting on their own initiative, should a resulting armed conflict be viewed as international? The answer is "yes," but only if the State of Blueland exercised "overall" control of the individual or group, or otherwise endorsed or encouraged the attack.[20] Absent overall control by a State, the attack would be the unlawful act of an individual or group of individuals, subject to

---

[18] Yoram Dinstein, "Computer Network Attacks and Self-Defense," in Michael N. Schmitt and Brian T. O'Donnell, eds., *International Law Studies, Vol. 76: Computer Network Attack and International Law* (Newport, R.I.: Naval War College, 2002), at 99, 100.

[19] Id., at 103.

[20] In the author's opinion, whether the test for State attribution is "overall control" (Prosecutor v. Tadić, IT-94-1, Judgment in Sentencing Appeals (ICTY, 26 January 2000), ¶ 131), or "effective control" (Military and Paramilitary Activities in and Against Nicaragua, ICJ, Judgment of 27 June 1986, ¶ 115), has been settled in favor of overall control by subsequent ICC jurisprudence (Lubanga Decision on the Confirmation of Charges (ICC, 29 January 2007), ¶ 211) and the ICJ itself (Application of the Convention on the Prevention and Punishment of the Crime of Genocide, ICJ, Judgment of 26 Feb. 2007, ¶ 404).

the domestic law enforcement of the State from which the attack was launched.

Might the same attack, launched by the same State-unaffiliated individuals be considered a non-international armed conflict? A cyber-initiated non-international armed conflict would require the participation of an organised armed group, and protracted armed violence of a certain level of intensity.[21] An individual cyber attacker is unlikely to meet such criteria, nor can most opposition groups, particularly those who "organise" on-line without a physical connection between members. These inabilities "*would preclude virtually organised armed groups for the purpose of classifying a conflict as non-international*."[22]

In combination, these impediments raise a high bar that would hinder most cyber operations launched by individuals or groups from achieving non-international armed conflict status. Instead, their acts would be left to domestic law enforcement agencies, guided by human rights norms.

The resolution of conflict status classification issues, of which there are many in LOAC, will continue to evolve through State practice.

Cyber Self-Defence

Self-defence exercised against a cyber attack need not be limited to cyber-on-cyber warfare. A State engaged in armed conflict may lawfully employ all of its military assets, electronic and kinetic. "*For targets of value, however, cyber weapons are difficult to engineer, and delivery is difficult to orchestrate*."[23] The legal challenges, primarily of attribution, and the principles of distinction[24] and proportionality,[25] make an immediate armed counter-attack impractical, if not impossible.[26]

> "*Attribution is one of the most difficult issues in cyber attacks. Rarely is it possible to determine who launched a given attack. The reasons for this are both legal and technical. Virtually every nation has statutes that forbid the unauthorized access into personal computers and Internet service providers' servers, actions that would be necessary to trace-back (hack back) the attack to its origins. The process to seek judicial authorization is*

---

[21] Prosecutor v. Haradinaj, IT-04-84-T (ICTY, 15 July 1999), Judgment, ¶ 49.
[22] Michael N. Schmitt, "Classification of Cyber Conflict," 17 *J. of Conflict & Security L.*, at 245, 248 (2012).
[23] LtCdr. Brian Evans and Rick Lanchantin, "Lifting the Fog On Cyber Strategy," US Naval Institute Proceedings, at 66, 68 (Oct. 2013).
[24] Article 48, Additional Protocol I to the Geneva Conventions of 12 August 1949, and relating to the protection of victims of international armed conflicts.
[25] E.g. see Article 57/2(b) of the Additional Protocol I to the Geneva Conventions of 12 August 1949, and relating to the protection of victims of international armed conflicts.
[26] The principles of distinction and proportionality are also explained in NATO STANAG 2449, Edition 2 and it's ATrainP-2 Training in Law of Armed Conflict. http://nso.nato.int/nso/zPublic/ap/ATrainP-2%20EDA%20V1%20E.pdf

time-consuming and burdensome; by the time it is granted the evidence is gone. And this presumes that this action is even possible."[27]

An immediate counterattack against a presumed source, without significant prior trace-back efforts, or requests for investigative assistance from the state from where the attack originated, would very likely violate the principle of distinction. If a state can aim their counter-attack accurately, however, they will have a target rich environment because, "*in cyber warfare…the physical infrastructure through which the cyber weapons (malicious codes) travel qualify as military objectives…Disabling the major cables, nodes, routers, or satellites that these systems rely on will almost always be justifiable by the fact that these routes are used to transmit military information and therefore qualify as military objectives*."[28] Indeed, at some point in cyber warfare, the LOAC principle of distinction could be in danger of becoming near meaningless in protecting civilian cyber infrastructure.

Another pre-counter-attack hurdle is the LOAC principle of proportionality – whether the envisioned counterforce is proportionate to the attack suffered, and the need to repel or deter further attacks. Once distinction, military necessity, and proportionality issues are sorted out, the specifics of a counter-attack may be considered. Satisfying these core requirements clearly narrows a victim State's options. Can a counter-attack oriented on an attacker's reverse azimuth, routed through civilian computer networks, servers, and routers, ever avoid catastrophic damage to a civilian computer network, raising potential violations of distinction and proportionality? Would the damage to the civilian networks be proportional and lawful collateral damage? If a counter- attack is not considered politically feasible or militarily possible, a means other than a cyber counter-attack is required.

A possible lawful response to a confirmed unlawful cyber attack, one carried out as a surprise attack that opens hostilities, for example, is a belligerent reprisal; a specific violation of the LOAC, undertaken in the course of the armed conflict, to encourage an enemy who has violated the law, to refrain from continuing their unlawful conduct.[29] Any belief that reprisals are entirely outlawed by modern LOAC is mistaken, although some

---

[27] Richard Pregent, "Cyber Defense and Counterintelligence," *NATO Legal Gazette*, Issue 26, at 13, 16 (19 Sept. 2011).

[28] Droege, "Get Off My Cloud," supra, note 16, at 564.

[29] Jean S. Pictet, *Commentary, I Geneva Convention 1949* (Geneva: ICRC, 1952), at 341-42. Other sources suggesting the utility of belligerent reprisal: William A. Schabas, *The International Criminal Court: A Commentary on the Rome Statute* (Oxford: Oxford University Press, 2010), 496; Yoram Dinstein, "Computer Network Attacks and Self-Defense," in Michael N. Schmitt and Brian T. O'Donnell, eds., International Law Studies, Vol. 76: *Computer Network Attack and International Law* (Newport, RI: US Naval War College, 2007), at 107; Frits Kalshoven, Belligerent Reprisals (Leiden: Martinus Nijhoff, republished 2005), at 375; and Theodor Meron, *The Humanization of International Law* (Leiden: Martinus Nijhoff, 2006), at 12-13.

commentators and scholars do not share that view.[30] Today, after their grave abuses in World War II, there are specific and narrowly tailored requirements for a lawful reprisal that military legal advisors may determine.

The advantages of a belligerent reprisal in cases of unlawful cyber attack are several: they need not be immediate, giving a victim State time to positively identify the attacker and minimise issues of distinction, they may be carried out in a different, unexpected location, and they can be calibrated to meet the requirement of proportionality.

Belligerent reprisal is a possible response to an unlawful cyber attack in the course of an international armed conflict, but not to every cyber attack. If a State Party were attacked by an opposing State Party in an ongoing international armed conflict, reprisal would not be a lawful option because the cyber attack would simply be another form of lawful attack in the course of an armed conflict.

How might a State lawfully respond to a cyber intrusion not rising to an attack? A category of responses offering lawful options is countermeasures. Essentially, countermeasures are reprisals, such as economic or trade restrictions, without the use or threat of force. Possible countermeasures are varied, each being tailored to the situation giving rise to their use. They may be taken solely to induce, convince, or compel the other State to return a situation to lawfulness. Counter measures, like reprisals, must be preceded by a request that the responsible State remedy its wrongful act. Like reprisals, they may only be taken to induce compliance with international law after an earlier international wrong, attributable to a State, has occurred. They must be proportionate, and they must end when the responsible State returns to compliance with its obligations.[31]

Conclusion

So far, no one is known to have died from a cyber attack anywhere in the world. An experienced cyber expert in the military and civilian communities writes:

> *"The most meaningful cyber conflicts rarely occur at the "speed of light" or "network speed."…[C]yber conflicts are typically campaigns that encompass weeks, months, or years of hostile contact between adversaries, just as in traditional warfare…While some attacks are technically difficult to attribute, it is usually a straightforward matter to determine the nation responsible, since the conflict takes place during an on-going geo-political crisis.*

[30] Prosecutor v. Kupreškić, IT-95-16-T, Judgment (ICTY, 14 Jan. 2000), ¶ 527-36.

[31] Countermeasures proportionality differs from the more familiar proportionality in LOAC. In gauging countermeasures proportionality, the focus is on the injury suffered by the victim State, rather than limiting defensive measures to those required to defeat the armed attack of another State.

> *Despite early fears that nations would strike at each other using surprise…there is no evidence that such conflicts have occurred. Nations seem to be willing to launch significant cyber assaults during larger crises, but not out of the blue...*"[32]

Such reassuring words cannot be the basis of a military legal advisor's awareness of the cyber threat. In a cyber environment that continuously changes and intensifies, continuous awareness and training are key.

Many books have been written about the topics discussed here. A brief paragraph cannot be a substitute for legal research and inquiry, but an awareness of basic issues, however summarily offered, is a basis for further study. As pointed out, the lack of international cyber treaties and adjudicated cases involving cyber issues in the context of armed conflict, render some cyber legal conclusions tentative and subject to disagreement. But what legal topic has ever been entirely clear? Duelling interpretations of evolving law have always been a basis for contested trials – and commentator's opinions. The military legal advisor's considered application by analogy of settled LOAC to novel cyber issues will usually yield a correct and tactically sound result.

***

[32] Healey, "A Brief History of US Cyber Conflict," in Healey, *A Fierce Domain*, supra, note 8, at 21-23.

www.nato.int

Cyber Warfare and the Concept of Direct Participation in Hostilities

by Hanneke Piters[1]

Introduction

The recent NATO Summit Declaration provides that "*[a]s the Alliance looks to the future, cyber threats and attacks will continue to become more common, sophisticated, and potentially damaging.*"[2] Thereby the Summit Declaration directly addresses the fifth "domain of warfare"– cyberspace. Clearly, this is not the first time "cyber" is on NATO's political agenda. Cyber and the need to address defence in cyberspace were tabled already in 2002 at the Prague Summit and were readdressed in 2006 at the Riga Summit; the topic was embedded in the 2010 Strategic Concept, and NATO has developed a governance structure, a response capability, and various partnerships.[3] As such, NATO is dynamically addressing the developments in cyberspace and encountering cyber activities directed at computers used by NATO.[4]

Cyberspace is characterised by being made by man and by its highly technical structure, which lends itself to many different actors and allows the users to mask and conceal their actions and identity. This particular domain trait possesses significant challenges, of which one is the application of existing (legal) norms. The challenge is not specific to NATO, but is relevant to

---

[1] Hanneke Piters obtained an LL.M. in International Human Rights and Humanitarian Law from the University of Essex and an MA in Political Science from Leiden University. She interned in the Office of the Legal Advisor of NATO HQ SACT in 2014. This article is based on a paper written during the LL.M. degree. Special thanks go to Mrs. Mette Hartov and Dr. Petra Ochmannova for their help. The responsibility for the content of this article rests with the author. The views expressed in this article are solely those of the author and may not represent the views of NATO ACO or ACT.

[2] Wales Summit Declaration, 5 September 2014, para. 72.

[3] See http://www.nato.int/cps/en/natohq/topics_78170.htm for a chronological overview of events and steps taken between Prague and Wales.

[4] See for example BBC, "Russian hackers used Windows bug to target NATO", 14 October 2014.

the lawyers addressing cyberspace in the context of NATO and of NATO nations. This article approaches cyberspace in the context of another progressing concept – that of direct participation of hostilities (DPH); a concept that has been subject to extensive studies and discussions, as non-State actors got frequently involved in armed conflicts. The article seeks to summarise the debate on DPH and apply the discussion to actors and their actions in cyberspace. Cyber is a highly specialised area in which the armed forces of NATO member countries employ civilian specialists or outsource tasks. As a result, civilians are becoming increasingly involved in cyber operations.[5] Under International Humanitarian Law (IHL), civilians enjoy protection from attack "unless and for such time" they directly participate in hostilities,[6] and therefore the implications for civilians taking a direct part are significant in terms of losing their protection and thus being legitimately targeted either by cyber or other means, just as they may be punished for their actions.[7] At the inter-State level, NATO nations that allow civilian employees and private contractors to take a direct part in hostilities may violate their obligations under international law.[8]

The question therefore becomes: What actions of civilians participating in cyber operations constitute direct participation in hostilities and for what time may they lose their protection?

Legal Framework and Analysis

The notion "direct participation in hostilities" (DPH) is only applicable to armed conflict (i.e. situations governed by IHL).[9] Article 51(3) of Additional

[5] Harrison Dinniss, Heather, Cyber Warfare and the Laws of War (Cambridge: Cambridge University Press, 2012), p. 160; Turns, David, "Cyber Warfare and the Notion of Direct Participation in Hostilities", Journal of Conflict & Security Law (2012), pp. 291-292; Schmitt, Michael N., "Direct Participation in Hostilities and 21st Century Armed Conflict" in Fischer, H., Crisis Management and Humanitarian Protection: Festschrift fur Dieter Fleck (Berlin: Horst, 2004), p. 527.

[6] Article 51(3) of Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977 (hereafter AP I); Article 13(3) of Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), 8 June 1977 (hereafter AP II).

[7] Melzer, Nils, Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law (Geneva: ICRC, May 2009) (hereafter Interpretive Guidance), p. 65; Melzer, Nils, "Cyber operations and *jus in bello*", Disarmament forum, No. 4, p. 8; Schmitt, Michael N., "Cyber Operations and the *Jus in Bello*: Key Issues", Naval War College International Law Studies (2011), p. 9; Harrison, (n. 5), p. 159; Schmitt, Michael N. (eds.), Tallinn Manual on the International Law Applicable to Cyber Warfare (Cambridge: Cambridge University Press, 2013) (hereafter Tallinn Manual), p. 119. Remark: The Tallinn Manual provides that "*[…] [it] does not represent the views of the NATO CCD COE, its sponsoring nations, or NATO. In particular, it is not meant to reflect NATO doctrine […].*" Tallinn Manual, p. 11.

[8] Watts, Sean, "Combatant Status and Computer Network Attack", Virginia Journal of Law, Vol. 50, No. 2, 2010, p. 423.

[9] Interpretive Guidance, (n. 7), p. 41; Harrison, (n. 5), p. 117. Remark: DPH as a concept is used both in international armed conflicts (IACs) and non-international armed conflicts (NIACs), but experts discussed

Protocol I (AP I) and Article 13(3) of Additional Protocol II (AP II) provide that civilians are entitled to protection against attack "unless and for such time" they take a direct part in hostilities.[10] The concept only applies to persons that participate in hostilities and who are neither members of armed forces or organised armed groups, nor participate in *levée en masse*.[11] Civilian government employees (i.e. technical experts) and private contractors (i.e. those who undertake the work that has been outsourced) who are not members of armed forces or organised armed groups are regarded as civilians and enjoy protection from attack for the time they do not take a direct part in hostilities.[12] Nevertheless, the ICRC "Interpretive Guidance on the Notion of Direct Participation in Hostilitites under International Law" (Interpretive Guidance) points out that "*[t]heir activities or location may, however, expose them to an increased risk of incidental death or injury even if they do not take a direct part in hostilities*".[13]

Several questions arise with regard to cyber activities. First, what qualifies as hostilities? Second, what constitutes taking a direct part? Third, what is the temporal scope of direct participation in hostilities? The Commentaries to the Protocols only shed some degree of light on these questions. The Commentary to AP I states that civilians are entitled to protection when they refrain from hostile acts.[14] It also provides that hostilities include the "*preparations for combat and the return from combat*".[15] It involves the time that civilians use their weapon or carry them, but also when s/he conducts hostile acts without using the weapon.[16] The concept "direct" participation refers to "*acts of war which by their nature or purpose are likely to cause actual harm to the personnel and equipment of the enemy armed forces*" (i.e. "causal relationship").[17] Unsurprisingly, the "ICRC Study on Customary International Humanitarian Law" states that "*[a] precise definition of the term "direct participation in hostilities" does not exist.*"[18] The International Criminal Tribunal for the Former Yugoslavia (ICTY) ruled in Tadiç

---

if there needed to be one or more definitions of DPH. This article is based on the assumption that there is one definition of DPH that applies to both IACs and NIACs. Melzer, Nils, Background paper on Direct Participation in Hostilities under International Humanitarian Law, ICRC Expert Meeting of 25-26 October, 2004, p. 30.

[10] The Israeli Supreme Court held that Article 51(3) of AP I has status as customary international law. The Public Committee Against Torture in Israel v The Government of Israel case (2006) HCJ 769/02 (Targeted Killings case), paras. 23, 29-30.

[11] Interpretive Guidance, (n. 7) pp. 20-36; Tallinn Manual, (n. 7), p. 118; Schmitt, (n. 7), p. 10.

[12] Interpretive Guidance, (n. 7), p. 40; Tallinn Manual, (n. 7), pp. 117-118; Schmitt, (n. 7), p. 10; Melzer (n. 7), pp. 8, 12-13.

[13] Interpretive Guidance, (n. 7), p. 37.

[14] Para. 1942 Commentary to AP I; Para. 4788 Commentary to AP II.

[15] Para. 1943 Commentary to AP I; Para. 4788 Commentary to AP II.

[16] Para. 1943 Commentary to AP I.

[17] Para. 1944 Commentary to AP I; Para. 4787 Commentary of AP II.

[18] Rule 6 of the ICRC Study on Customary International Humanitarian Law. Henckaerts, Jean-Marie and Louise Doswald-Beck (eds.), Customary International Humanitarian Law: Volume I: Rules (Cambridge: Cambridge University Press), 2005, p. 22. Remark: The ICRC Study on Customary IHL is not uncontroversial.

that the status of a person needs to be determined on a "*case-by-case basis.*"[19] The Israeli Supreme Court held in the Targeted Killings case that not only the person who carries out "*the physical act of attack,*" but also the person who sends him/her, makes decisions regarding the act or planned it, is taking a direct part in hostilities.[20] More specifically, the Court ruled that a person who gathers intelligence about the armed forces, and persons who perform, supervise or offer service to the operation of weapons used by "unlawful combatants" take a direct part in hostilities,[21] while persons who spread propaganda do not.[22] This concept of "belligerent nexus" will be addressed below. The Court found that, as with the concept "takes a direct part," no consensus exists as to the scope of the notion "and for such time".[23] It held that a civilian who takes a direct part in hostilities regains protection "*starting from the time he detached himself from that activity.*"[24]

The Interpretive Guidance[25] stipulates that an act needs to meet the following three cumulative conditions in order to amount to direct participation in hostilities: "threshold of harm," "direct causation," and "belligerent nexus."[26]

a. Threshold of harm

The Interpretive Guidance provides that in order to satisfy the "threshold of harm" requirement, an act needs to "*inflict death, injury, or destruction on persons or objects protected against direct attack,*" or must *be likely* to "*adversely affect the military operations or military capacity of a party to an armed conflict.*"[27] The latter implies that an act does not have to bring about physical damage to meet the threshold.[28] The "HPCR Manual on International Law Applicable to Air and Missile Warfare" (HPCR Manual) stipulates that: "*[e]ngaging in electronic warfare or computer network attacks […] which is intended to cause death or injury to civilians or damage to or destruction of civilian objects*" amounts to DPH.[29] Padmanabhan argues that destructing military infrastructure would satisfy the threshold.[30] It is noteworthy that the

[19] Prosecutor v. Dusko Tadiç (1997) 36 ILM 908, ICTY (hereafter Tadiç case), para. 616; Harrison, (n. 4), p. 161; see also the Targeted Killings case, paras. 34-37, 39.
[20] Tadiç case., para. 37.
[21] Ibid., para. 35.
[22] Ibid.
[23] Ibid., para. 39.
[24] Ibid..
[25] Interpretive Guidance, (n. 7); Harrison, (n. 5), p. 165.
[26] Interpretive Guidance, (n. 7), p. 46. Remark: Several aspects of the three cumulative conditions caused controversy amongst the experts that were involved in the study, and proved difficult to reach consensus on. Schmitt, Michael N. "The Interpretive Guidance on the Notion of Direct Participation in Hostilities: A Critical Analysis", Harvard National Security Journal (2010), Vol. 1, pp. 6, 27-39.
[27] Interpretive Guidance, (n. 7), p. 47.
[28] Tallinn Manual, (n. 7), p. 119.
[29] Article 29(iii) of the HPCR Manual on International Law Applicable to Air and Missile Warfare, Program on Humanitarian Policy and Conflict Research at Harvard University, Bern, 15 May 2009.
[30] Padmanabhan, Vijay M., "Cyber Warriors and the Jus in Bello", International Law Studies, Vol. 89,

Tallinn and HPRC Manuals use the wording *intent* instead of *likelihood* as used by the Interpretive Guidance, which could have implications for civilians involved in cyber operations.[31] The Interpretive Guidance stipulates, in relation to adversely affecting the opponent militarily, that "*[e]lectronic interference with military computer networks could […] suffice, whether through computer network attacks (CNA) or computer network exploitation (CNE)…*"[32] Moreover, it states that "*…the manipulation of computer networks […] would not, in the absence of adverse military effects, cause the kind and degree of harm required to qualify as direct participation in hostilities.*"[33] This raises the question as to what adversely affecting the opponent military entails in relation to cyber operations. The Tallinn Manual states that a cyber operation that "disrupts" the opponent's command and control facilities would meet the threshold.[34] Padmanabhan argues that gathering tactical information would suffice.[35] Some members of the International Group of Experts were of the view that the threshold of harm requirement also covers operations that "*enhance one's own (military) capacities,*" because this would in relative terms negatively affect the opponent militarily.[36] Examples given are the development or maintenance of (passive) cyber defences and the identification of vulnerabilities.[37] This would imply that civilians engaged by States that set up an excellent cyber defence run greater risk of losing their protection. Moreover, different States would likely perceive the effect of the identification of vulnerabilities differently, and as a result civilians do not know whether they are taking a direct part in hostilities.

b. Direct causation

According to the Interpretive Guidance the criteria "direct causation" is fulfilled if there is a direct nexus between an act and the harm reasonably expected to follow from it, or a military operation that act is an "integral" part of (i.e. harm has to be caused in "one causal step").[38] Moreover, it states that remotely controlled CNAs meet the condition of direct causation.[39] The Tallinn Manual provides that if a cyber operation brings about the "disruption" of an opponent's command or control network in "one causal step" the condition of direct causation is fulfilled.[40] Nevertheless, Turns argues that the requirement of a direct causal link has significant implications with regard to the application of DPH to cyber operations, as their consequences are often

---

No.288 (2013), pp. 298-299.

[31] Allan Collin, "Direct Participation in Hostilities From Cyberspace", Selected Works (February 2013),p. 26.

[32] Interpretive Guidance, (n. 7), pp. 47-48.

[33] Ibid., pp. 49-50.

[34] Tallinn Manual, (n. 7), p. 119.

[35] Padmanabhan, (n. 30), pp. 298-299.

[36] Schmitt, (n. 7), p. 13; Tallinn Manual, (n. 7), p. 119.

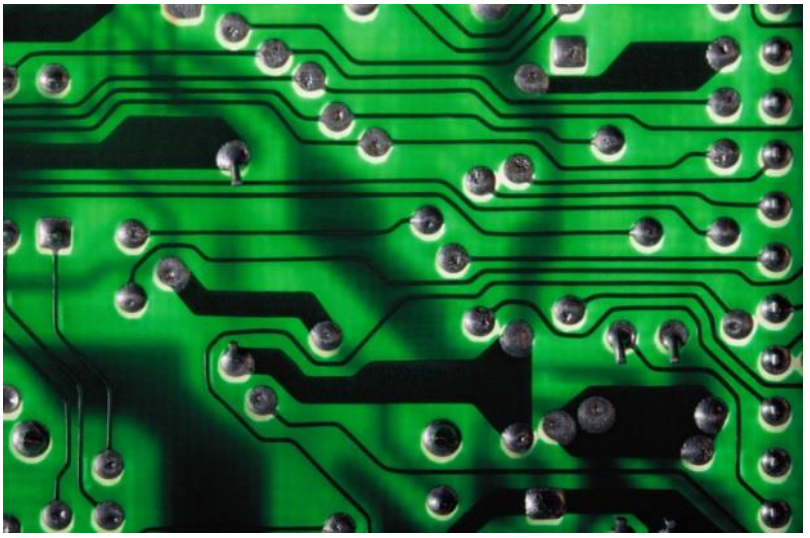
[37] Ibid.

[38] Interpretive Guidance, (n. 7), pp. 51, 53.

[39] Ibid., p. 55.

[40] Tallinn Manual, (n. 7), p. 119.

indirect. The result would be that civilians could participate in cyber operations without losing their protection.[41] Harrison points out that CNAs may even be conducted with the aim of bringing about "secondary" consequences.[42] If an act is part of a coordinated military operation the direct causation test seems to give less room for bringing about indirect effects.[43] This clarifies why Schmitt points out that qualifying the development of software for a specific cyber operation as indirect causation would be criticised.[44] In this light, Padmanabhan claims that the direct causation condition is easier to satisfy in cyber operations as compared to conventional operations.[45] He argues that "cyber weapons" need "constant modifications" during an operation to overcome defences.[46]



www.nato.int

c. Belligerent nexus

The Interpretive Guidance stipulates that in order to satisfy the belligerent nexus requirement "*an act must be specifically designed to directly cause the required threshold of harm in support of a party to the conflict and to the detriment of another.*"[47] The Tallinn Manual only provides that "*the acts must be directly related to the hostilities.*"[48] The example provided is a "*system that is used to direct [i.e. attack] enemy military operations*" meets the condition.[49] It seems that the latter applies a broader approach, although from the example given, can be derived that both approaches are similar: using a system that targets the military operations of

[41] Turns, (n. 5), pp. 287-288.
[42] Harrison, (n. 5), p. 166.
[43] Ibid.
[44] Schmitt, (n. 7), p. 13.
[45] Padmanabhan, (n. 30), p. 298.
[46] Ibid.
[47] Interpretive Guidance, (n. 7), p. 58.
[48] Tallinn Manual, (n. 7), p. 119.
[49] Ibid., pp. 119-120.

an adversary.[50] Some experts are of the opinion that if a person carries out a cyber operation to steal private or public money with the intention to spend it on a specific military operation the condition is fulfilled.[51]

d. Temporal scope

The Interpretive Guidance also examines the temporal scope of DPH.[52] It states that there is no doubt that DPH covers the time that the act is executed.[53] Moreover, it may also include the measures preparatory to the execution of the act.[54] Furthermore, it covers the deployment preceding and the return from the place where the act was executed, provided that it forms an "integral" part of the act.[55] According to this Guidance, civilians involved in an act that constitutes DPH lose their protection for the duration of every act.[56] Thus, as soon as the act ends they regain their protection again.[57] This is also called the "revolving door of civilian protection". [58]

In case of doubt as to whether a person is taking a direct part in hostilities, some experts take the view that the "presumption of civilian protection" needs to be applied.[59] Other experts are of the opinion that all relevant information needs to be assessed and that a person must "act reasonably" when making the decision. [60] The Interpretive Guidance stipulates that *"[w]here the execution of a hostile act does not require geographic displacement, as may be the case with computer network attacks […], the duration of direct participation in hostilities will be restricted to the immediate execution of the act and preparatory measures forming an integral part of that act."*[61] According to Prescott this approach is too narrow for cyber operations, as deployment to and from the location where the operation will take place may not be needed as having a computer is sufficient (i.e. one does not have to be in the vicinity of the target) to conduct the operation, and the execution of the operation may take only a few minutes or even less.[62] Schmitt argues that the right to target a person taking a direct part in

[50] Ibid.
[51] Ibid., p. 120.
[52] Interpretive Guidance, (n. 7), p. 65.
[53] Ibid.
[54] Ibid.
[55] Ibid., pp. 67-68.
[56] Ibid., p. 70.
[57] Ibid.
[58] Ibid., pp. 70-71. Remark: The concept the "revolving door" is not uncontroversial. Schmitt, (n. 26), pp. 37-38; Tallinn Manual, (n. 7), p. 122.
[59] Interpretive Guidance, (n. 7), p. 75.
[60] Tallinn Manual, (n. 7), p. 122.
[61] Interpretive Guidance, (n. 7), p. 68.
[62] Presscott, Jody M., "Direct Participation in Cyber Hostilities: Terms of Reference for Like-Minded States?", in Czosseck C., R. Ottis and K. Ziolkowski (eds.), 4th International Conference on Cyber Conflict (Tallinn, NATO CCD COE Publications, 2012), pp. 258-259; Schmitt, (n. 6), p. 14; Blank, Laurie R., "International Law and Cyber Threats from Non-State Actors", Emory University School of Law Legal Studies Research Paper Series, Research Paper No. 12-234, p. 26.

hostilities is therefore not actually present.[63] The Tallinn Manual provides that civilians lose their protection for the duration that they are involved in the act that constitutes DPH, and "*the actions immediately preceding and subsequent*" to the act.[64] This would include the time when a person is travelling to and from the computer that is used to launch the cyber operation.[65]

Some experts are of the opinion that the duration of taking a direct part should even stretch as far "upstream" and "downstream" as there is a "causal link" with the actual involvement.[66] Schmitt points out that the consequences brought about by a cyber operation may be "long-delayed" to prevent it from being detected (this is comparable to a kinetic operation in which a bomb is planted and explodes later).[67] As a result, those against whom a cyber operation is conducted are not given the possibility to react.[68] Several experts take the view that DPH starts when a civilian engages in the planning of an operation and ceases as s/he stops to have an "active role" in it.[69] This implies that the civilian might already have regained protection at the moment that the damage takes place.[70] Other experts are of the opinion that, to stay in cyber terms, the introduction of a hostile agent and its activation are "separate acts."[71] Harrison took the view that the period should even cover the time that the "effects" of the cyber operation "are being felt."[72]

Experts are divided as to the time that a civilian who conducts "repeated" cyber operations loses his/her protection against attack.[73] Some experts support the approach laid down in the Interpretive Guidance that they must be dealt with as being separate acts.[74] Others take Schmitt's view that "for such time" in a cyber-context can only be defined as covering the whole period that a civilian is participating in "repeated" cyber operations.[75] This paper is in favour of an intermediate approach as it would be dangerous to take away too much protection from or give too many privileges to civilians.

---

[63] Schmitt, (n. 7), p. 14; Padmanabhan, (n. 30), p. 300.
[64] Tallinn Manual, (n. 7), pp. 120-121.
[65] Ibid., p. 121.
[66] Dinstein, Yoram, "The Principle of Distinction and Cyber War in International Armed Conflicts", Journal of Conflict & Security Law (2012) Vol. 17, No. 2, p. 276; Tallinn Manual, (n. 7), p. 121.
[67] Schmitt, (n. 7), p. 14; Tallinn Manual, (n. 7), p. 121; Comments of Dr. Noam Lubell.
[68] Schmitt, (n. 7), p. 14.
[69] Tallinn Manual, (n. 7), p. 121.
[70] Ibid.
[71] Ibid.
[72] Padmanbhan, (n. 30), p. 301.
[73] Tallinn Manual, (n. 7), pp. 121-122.
[74] Ibid., p. 122.
[75] Schmitt, (n. 7), p. 14.

Further applying the concept of DPH to cyber operations

The next step of the article is to illustrate the discussions of DPH against three kinds of actions that regularly occur in the cyber-context: 1) developing programmes; 2) installing and maintaining programmes and computers; and 3) operating programmes.

Research, designing and writing

Turns argues that *general* research related to the development of computer programs does not meet one of the three DPH criteria.[76] He is, however, of the opinion that designing and writing of computer programs (this is comparable to scientists who design weapon systems) meet the threshold of harm and belligerent nexus requirements, provided that it is designed to cause the required foreseeable harm, and the civilians involved know which target or conflict they are designing and writing the program for. Nevertheless, he claims that it does not constitute DPH, because the harm cannot be brought about in "one causal step."[77] Crawford also takes the view that civilians who only write, and not plan the execution of and/or execute the program, are not taking a direct part.[78] In contrast, Harrison argues that coders and systems specialists who are involved in designing programs for a specific CNA are taking a direct part, as it forms an "integral part" of the attack.[79] The Tallinn Manual states that the "*designing of malware in order to take advantage of particular vulnerabilities*" constitutes DPH.[80] However, it also states that designing malware and making it publicly available on the web, so that it can be used by parties to the conflict, does not amount to DPH.[81] The experts that contributed to the Tallinn Manual were split as to whether a civilian that develops and provides malware while knowing that it will be used to execute attacks, but not knowing against which target, meets the direct causation requirement.[82] In short, scholars are divided and the purpose or planned use of the programme is being given weight in determining if civilians are considered to take direct part in hostilities. This position can however be taken too far, and this paper favours the view that civilians who engage in designing a program for a specific cyber operation are taking a direct part in hostilities. If the programme is so specifically tailored to achieving the aim of the operation, the planning and execution add relatively little to the process.

---

[76] Turns, (n. 5), p. 295.
[77] Turns, (n. 5), p. 295; Interpretive Guidance, (n. 7), p. 53 and footnote 122; Comments of Dr. Noam Lubell.
[78] Crawford, Emily, Sydney Law School Legal Studies Research Paper, No. 12/10 (February 2012), pp. 17-18.
[79] Harrison, (n. 5), p. 167; Blank, (n. 62), p. 25.
[80] Tallinn Manual, (n. 7), p. 120.
[81] Ibid.
[82] Tallinn Manual, (n. 7), p. 120; Blank (n. 62), p. 25.

Installing, service and maintenance

The next question is if civilians who install, provide service or otherwise maintain computer programs may be considered to take direct part in hostilities. And, again the scholars disagree: Turns claims that installing a program does not amount to DPH, as the direct causation requirement will not be met.[83] Harrison argues that support and maintenance of computer systems and networks that launch CNAs may be equalled with the maintenance of weapons systems. The civilians involved in the maintenance of weapons systems are believed to take a direct part in hostilities. Nevertheless, several scholars claim that many activities (e.g. routine maintenance and security updates) undertaken by those who support computer systems and networks do not amount to DPH.[84] The Tallinn Manual also argues that general maintenance of computer equipment that may be used in the conflict does not amount to DPH.[85] Whether civilians engaging in the maintenance of defensive cyber operations are taking a direct part is also debated, as preventing a disruption of computer systems and networks negatively affects the enemy militarily.[86] The take-away from this discussion appears to be how to distinguish between routine and non-routine forms of maintenance and if a computer system can be distinguished from a weaponry system.

Operation of computer programs

Another debated area is that of operating computer programs. Harrison claims that civilians who are involved in offensive CNAs directed against the opponent's employees or material take a direct part in hostilities. According to her it is irrelevant whether the attack is conducted to bring about harm on its own, or to support a kinetic attack.[87] Other scholars support the view that carrying out cyber attacks against the opponent by disrupting their networks and manipulating data in their systems, amount to DPH.[88] According to Turns the introduction of a so-called hostile agent by a civilian amounts to DPH if that person previously programmed it to activate at a particular moment in the future, or if it activates instantly.[89] The Tallinn Manual submits that identifying vulnerabilities in the opponent's system in order to use

[83] Turns, (n. 5), p. 295.
[84] Harrison, (n. 5), pp. 168-170; Crawford, (n. 78), p 16; Dörmann, Knut, 'Applicability of the Additional Protocols to Computer Network Attacks', available online http://www.icrc.org/eng/assets/files/other/applicabilityofihltocna.pdf, p. 9; Turns, (n. 5), p. 295.
[85] 'Tallinn Manual', (n. 7), p. 120.
[86] Harrison, (n. 5), pp. 170-171; 'Tallinn Manual', (n. 7), p. 119.
[87] Harrison, (n. 5), p. 167.
[88] Schmitt, (n. 5), pp. 526-527; Crawford, (n. 78), pp. 16-17; 'Tallinn Manual', (n. 7), p. 120; Schmitt, (n. 7), p. 13; Dinstein, (n. 66), p. 276; Dörmann, (n. 84), p. 9; Melzer, (n. 7), 8; Turns, (n. 5), p. 295.
[89] Remark: Turns claims that a civilian takes a direct part if s/he gives oral or written instructions to a combatant to activate a hostile agent. Turns, (n. 5), p. 295.

it for its own benefits also constitutes DPH.[90] However, Turns claims that identifying vulnerabilities in and of itself does not reach the threshold of harm and direct causation requirements.[91] Moreover, he argues that making vulnerabilities publicly known on the internet does not satisfy the direct causation criteria.[92] Several scholars submit that conducting cyber operations to gather intelligence about the opponent's operations amounts to DPH.[93] Nevertheless, Melzer claims that "*general intelligence gathering*" does not qualify as DPH.[94] Several experts argue that carrying out DDoS attacks against the adversary's system qualify as DPH.[95] In short, this category shows a mixed picture of agreement and disagreement amongst scholars.

Conclusion

NATO member countries increasingly employ civilian specialists and outsource tasks to private contractors in the complex cyber domain. The implications for civilian employees and private contractors who are taking a direct part in hostilities can be significant. First, they lose their protection and can be targeted by cyber or other means. Second, they are not included in the proportionality and precautions in attack assessment. Third, they may be held liable and be punished for their actions. Moreover, NATO member countries that let them take a direct part may violate their obligations under international law. Therefore, it is important for legal advisors to know what acts in the cyber domain constitute direct participation in hostilities. This article addresses the three cumulative criteria laid down in the Interpretive Guidance (1) "threshold of harm", (2) "direct causation" and (3) "belligerent nexus", and how they generally apply to the cyber domain and particularly (1) research, designing and writing, (2) installing, service and maintenance, and (3) operation of computer programs.

There is common ground on some DPH aspects, but fierce debate about others. Applying the concept of DPH to cyber operations adds new features and thus disagreement. Examples about which scholars disagree are multiple and most are common facets in the cyber domain: developing and providing programmes that can be used to facilitate malware or to execute attacks; maintenance of defensive cyber operations; identifying vulnerabilities in the opponent's system; and intelligence gathering.

The devil is in the details, and legal advisors have to be mindful of the concept of DPH when providing advice as to whether civilian employees and private contractors can conduct certain tasks, also (or perhaps particularly) in

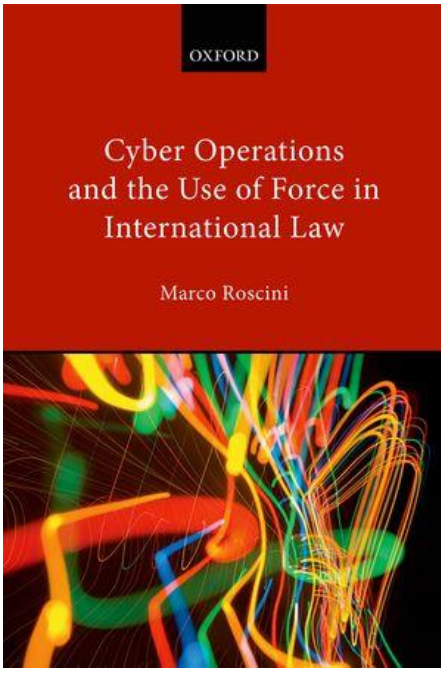
[90] Tallinn Manual, (n. 7), p. 120.
[91] Turns, (n. 5), p. 295.
[92] Ibid.
[93] Tallinn Manual, (n. 7), p. 120; Schmitt, (n. 7), p. 13; Dörmann, (n. 84), p. 9.
[94] Melzer, (n. 7), p. 9.
[95] Tallinn Manual, (n. 7), p. 120; Blank, (n. 62), p. 25.

the cyber domain, without being exposed to the risks of losing their protection under IHL. As the cyber domain attracts wide attention and is being closely explored by legal experts, one could hope that further analysis will be conducted and result in further clarification as to when civilians participating in cyber operations are considered taking a direct part in hostilities and thus a generally accepted approach may be reached.

***

Book Review: Cyber Operations and the Use of Force in International Law by Marco Roscini[1]

by Vincent Roobaert[2]



Since the cyber-attacks on Estonia in 2007 and Georgia in 2008 cyber-attacks have increased in number and visibility. Various nations have developed their own cyber defence policies and have established cyber commands. In the legal field, however, progress has been slightly slower. Despite early declarations that international law, including the law of armed conflict, applies to the cyber domain in principal, practitioners have struggled somewhat to adapt legal texts developed in the 20th century to denial of service attacks, botnets and zero-day exploits.

Legal practitioners have encountered challenges in reconciling rules developed in 1977 with the realities of today's environment. Some of these challenges could be explained, initially, by a lack of awareness of the legal community about the technical characteristics of cyber-attacks and the potential for damages that could derive from them. In recent years, various initiatives have been set up to bring technicians and lawyers together. The training efforts of the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)[3] fall within these initiatives. Increased interest in cyber also derives from evolution in the type of attacks. While early attacks were limited to website defacements or denials of service for certain web-based services such as e-banking, Stuxnet demonstrated that capacities exist for cyber-attacks to cause damages in the physical world as well.

Mr. Marco Roscini's book is among the latest monographs covering the legal aspects of cyber operations. It covers both *jus ad bellum* and *jus in bello* aspects of cyber operations.

---

[1] M. Roscini, Cyber Operations and the Use of Force in International Law, Oxford University Press, 2014.
[2] Vincent Roobaert works as Assistant Legal Adviser for the NCI Agency in Brussels. The views expressed in this article are solely those of the author and may not represent the views of NATO, ACO, ACT or the NCI Agency.
[3] For more information on the CCDCOE, please see their website at www.ccdcoe.org. In addition to publications such as the Tallinn Manual, the centre also organizes exercises and training bringing together technical and legal experts.

With regard to the law governing the use of force, the author recognises that the application of the UN Charter in relation to cyber-attacks is rendered difficult by the requirements of attribution and armed attack.

First, despite improvements in cyber forensics, the identification of the perpetrators of cyber-attacks remains difficult. Secondly, in the absence of actual physical damages, certain States may be inclined to consider that cyber-attacks do not constitute armed attacks under the UN charter.

The author, however, wonders how such a position can be sustained given our increased dependency on IT systems. He then looks at the remedies available to those States that are victims of cyber-attacks either through self-defense, reprisal or counter-measures. Given that many cyber-attacks are designed to be seen as originating from non-state actors, the author argues that lessons should be drawn from States' response to international terrorism, for example the possibility to expand the responsibility of a State harboring hackers which proves to be unable or unwilling to stop the attacks originating from its territory.

The author then turns to an examination of the rules governing the conduct of armed conflicts. He highlights the point that cyber weapons have unique characteristics that call for an adaptation of legal framework. Examples of this are: cyber weapons utilising dual-use infrastructure (i.e. the Internet) to produce their effect and cyber weapons producing a cascade of effects before producing actual physical damage. In such a manner, an attack may target a specific computer in order to affect a system controlled by that computer. This system, in turn, may be led to malfunction, thereby causing damages to individuals or property. The author also underlines the shortcomings of the theory of kinetic equivalence, which requires cyber-attacks to have physical effects to be considered as attacks. In his view, this may not be sustainable in a world heavily dependent on information systems.

Mr. Roscini should be praised for writing a book that goes beyond existing analysis of the law of armed conflict applied to cyber. Earlier legal monographs on cyber warfare restated the principles of laws and attempted to awkwardly apply them to cyber, with varying degrees of success. Many lacked an understanding of the technical aspects of cyber. Mr. Roscini, on the other hand, has clearly spent time studying the legal but also the technical aspects of cyber. The result is a monograph that does not merely repeat legal principles in an abstract manner but rather presents the legal rules with a technical hindsight, highlighting their potential flaws and gaps in the cyber area.

***

Book Review: Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy, by Katharina Ziolkowski (ed.)[1]

by Stanila Sv. Dimitrova[2]

States are the leading players on the international scene, and as such they set up the rules of the game. In recent years, States have faced a struggle in securing their control in the realm of cyberspace as, the non-physical nature of, power grows across the globe. "*Peacetime Regime for State Activities in Cyberspace*" sets out to explore the limitations of State power in cyberspace and to define its place within the international legal framework.

Realising that cyberspace is a relatively novel area, which is something of a *terra incognita* for many legal professionals, Katherina Ziolkowski's volume begins with an overview of the technological capabilities and challenges involved. Despite the specialised topics and technical information, the language of these chapters is easy to understand and conveys the ideas without in-depth prerequisite knowledge. This first part equips the reader with the understanding of what cyberspace is, who the actors within it are, its use and specific properties.

Following in Part II, the volume focuses on the influence and applicability of international law in cyberspace. The chapters provide a general-to-specific dissection of (general) international law and its ability to put a frame around the cyberspace realm. The authors have explored the applicability of international law to cyberspace in various areas such as territorial sovereignty, non-intervention, human rights, civil and military aviation, protection of submarine cyber infrastructure, etc. The last chapter of this part is dedicated to the "*Responsibility of States and International Organisations in the Context of Cyber Activities with Special Reference to NATO*," which could present a particular interest to the audience of this Legal Gazette.

In Part III, the authors have adopted a forward-thinking approach in

[1] K. Ziolkowski (ed.), Peacetime Regime for State Activiities in Cyberspace: International Law, International Relations and Diplomacy, NATO CCD COE Publication, Tallinn, 2013.
[2] Legal Intern, SHAPE Legal Office (March – September 2014). The views expressed in this article are solely those of the author and may not represent the views of NATO, ACO or ACT.

identifying future missions, setting up a forum for discussion of possible reactionary responses to legal deficiencies in cyberspace, emphasising the growing need for developed cyber diplomacy, analysing trends in international policy to cyber emergencies, proposing de-militarising the response to a cyber-attack, among other topics. The latter is, in fact, a topic in two of the chapters, and represents an interesting shift away from the concept of responding to a cyber-attack under self-defence (Art. 51 UN Charter). It proposes that countermeasures taken in response to an internationally wrongful act, pursuant to the International Law Commission Articles on Responsibility of States for Internationally Wrongful Acts, can be a viable means of responding robustly, but short of the provocative use of force.

The volume is a comprehensive and informative compilation of articles containing opinions of respective authors on current issues related to cyber. Its main objective is to identify the *status quo* and to stir discussion in order to provide a reactionary response and develop legal certainty. Being a product of the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCDCOE), it often has references to NATO and its legal order, which makes it a must-read for the NATO legal community.

***

Thomas E. Randall, SHAPE and ACO Legal Advisor, 2005-2014
An Appreciation

By Sherrod Lewis Bumgardner[1]

Tom Randall became a NATO International Civilian (NIC) in May 2005 when he accepted the post as the Legal Advisor for Supreme Headquarters Allied Powers Europe (SHAPE). By happy circumstance, I also became a NIC in June 2005 working for Headquarters Supreme Allied Commander Transformation (HQSACT) at Allied Command Transformation Staff Element Europe (ACT-SEE), and was able to continue my professional relationship and friendship with Tom Randall.

My relationship with then Captain Randall, US Navy, began in 1993 when he was in London as the Staff Judge Advocate for the Command-in-Chief, U.S. Naval Forces Europe and I was serving as a junior Legal Advisor in Stuttgart at the Office of the Staff Judge Advocate, U.S. European Command (EUCOM) responsible for action-officer legal support for operations. Captain Randall's hands-on approach to operational matters enabled me to establish an effective working relationship with him and his office. In small part it helped that I had inherited his former EUCOM legal portfolio, his desk, and his very well organised files; but mainly it was his professional courtesy and willingness to help push issues through the, sometimes turgid, U.S. joint military staffing process that made him a supportive colleague. Our working relationship strengthened upon his military retirement in 1995 and arrival as the civilian legal advisor in the EUCOM legal office where we continued working together until I left EUCOM at the end of 1996.

Tom left EUCOM in 2001 for other senior U.S. government civilian attorney assignments in Washington, D.C. He first went to the International and Operational Law Division of the U.S. Navy Judge Advocate General's Corps (Code 10). In 2003 he became the Special Assistant for International Law to the Judge Advocate General of the U.S. Air Force. Tom then moved from the Pentagon to Mons, Belgium, after being selected by General Jim Jones, USMC, the 14th Supreme Allied Commander Europe (SACEUR) to

[1] Sherrod Lewis Bumgardner serves as the ACT Staff Element Europe Legal Advisor since June 2005.

become the SHAPE Legal Advisor.

As the SHAPE Legal Advisor (and, after the 2012 re-organisation of the NATO Command Structure, the Allied Command Operations (ACO) Legal Advisor) Tom Randall continued to apply his pragmatic approach to law to enhance the ability of the Alliance to carry out its mission.

Well-spoken and possessing great dignity, Tom disliked needless formality and always encouraged straightforward conversation. He favoured those lawyers who had learned to express themselves clearly and succinctly. He wanted practical solutions and used a team approach to answering the legal questions posed to his office. He championed the use of mind-mapping software for legal problem-solving so that all aspects of the many complex legal problems SHAPE faced were captured and considered.

Under Tom's leadership, SHAPE, ACO, and NATO handled momentous challenges. These challenges included the legal consequences of: the International Security Assistance Force (ISAF) in Afghanistan as a NATO mission and, after 2012 the planning for ISAF's transition to Operation Resolute Support; the air and maritime actions to protect the civilian population of Libya in Operation Unified Protector; the 2013 NATO deployment of Patriot missiles to Turkey; adjustments to the NATO Training Mission in Iraq, Kosovo (KFOR), and Bosnia-Hercegovina (NATO HQ Sarajevo); multiple restructurings of the NATO Command Structure NATO Agencies, and host-nation agreements between NATO nations and NATO entities; NATO-EU relations; and what Tom saw as the never-ending battle to preserve the legal status and prerogatives of SHAPE and its personnel.

On Tuesdays, when operational tempo permitted, Tom hosted a weekly legal meeting at ACT-SEE for legal personnel from the nine legal offices located at SHAPE.[2] This was to ensure the personnel of these offices were informed of the current legal developments SHAPE and NATO were facing. National legal advisors visiting SHAPE were always welcome, as were the legal advisors from the International Staff and International Military Staff at NATO Headquarters. These meetings were usually attended by 10-15 people, but depending upon events and visitors to SHAPE, as many as 25 legal personnel could be there. Tom would begin the meeting by providing an update describing the issues about which he and the SHAPE legal office were most engaged. He would then go around the room so that the meeting's participants could share items of common interest with the group. Tom kept the discussions substantive and lively making all attendees (whether interns or senior colleagues) feel like full members of a large SHAPE legal community.

[2] The nine organizations that have legal offices located aboard the SHAPE military base are: SHAPE, NATO Communication and Information Systems Group (NCISG), Allied Command Counter-Intelligence (ACCI), NATO Special Operations Headquarters (NSHQ), ACT-SEE, NATO Communications and Information Agency (NCIA) the German National Military Representative, the European Union Staff Group, and the U.S. Army Northern Law Center.

While Tom's support of SHAPE's senior officers and officials left him little time for academic pursuits, he always found time to support legal training and education. In 2007 when the ISAF mission was becoming the primary focus of ACO, Tom attended the NATO Operational Law Course and spent a full week in the classroom ensuring the ACO legal perspective was clearly understood by the course attendees. He authored three article for the **NATO Legal Gazette**, "*The Ends and Outs of the Use of Contractors during Operations*," Issue 17, 2008; "*The Evolving Role the Legal Adviser in Support of Military Operations—Some Tips for 'Up-and-Coming' Legal Advisers*," Issue 21, 2012 and; "*Legal Authority of NATO Commanders*," Issue 34, 2014.

In sum, the SHAPE Legal Office accomplished much during Thomas E. Randall's nine-year tenure. He leaves behind a legacy of openness, engagement, and professionalism. Those of us that had the opportunity to be his colleagues will long remember him and warmly wish him all the best in his future endeavours.

***

CLOVIS PROJECT UPDATE

Dear Readers,
Dear CLOVIS Users,

Please note that as of January 1st 2015, there will be a transition in management and that after that date CLOVIS will be operated by the SHAPE Legal Office.

For access to CLOVIS and assistance, you are now invited to contact Ms Francesca Trivoli (SHAPE Legal Office) at: francesca.trivoli@shape.nato.int.

We wish to take this opportunity to thank you for your contribution and support in our endeavour to build the platform that aimed at better sharing legal information and bringing NATO legal advisers together. It has been a real pleasure working with you.

Yours Sincerely,

Jessica Johnson
Thomas Mertens
Allende Plumed Prado
Annabelle Thibault

NATO SPOTLIGHT

Name: Patrick McCarthy

Rank/Service/Nationality: Captain/Navy/USA

Job title: HQ ISAF Legal Advisor

Primary legal focus of effort: Prepare legal authorities for the Resolute Support Mission.

Likes: Playing lacrosse.

Dislikes: People who do not have the imagination to "get to yes."

When in HQ ISAF everyone should: Enjoy Mexican night!

Best NATO experience: Singing karaoke with the whole NATO team during the San Remo NATO Legal Conference.

My one recommendation for the NATO Legal Community: Smile and don't forget that teamwork makes the dreamwork.

NATO SPOTLIGHT

Name: Thomas Schiffer

Rank/Service/Nationality: Lieutenant Colonel/Army/United States

Job title: Chief Legal Advisor, NATO LANDCOM, Izmir, Turkey

Primary legal focus of effort: I do a little bit of everything.

Likes: Running/marathons, travel, spending time with my wife and three daughters, anything involving strapping something to your feet and going down a snow covered mountain (skiing/snowboarding/telemark skiing).

Dislikes: Arrogance, selfishness, and olives.

When in Izmir, Turkey everyone should: Try a glass of Raki (at least once), visit the wealth of nearby ancient sites (see photo above!), and eat seafood—the fish is amazing here.

Best NATO experience: These past few weeks on our LANDCOM battle staff training in Grafenwoehr, Germany. We had a genuine, headquarters-wide bonding experience.

My one recommendation for the NATO Legal Community: Being new to NATO, I have been treated throughout the community with a lot of patience and a lot of mentorship. I have appreciated everyone's willingness to "show the new guy" how things are done in NATO."

NATO SPOTLIGHT

Name: Rudolph Stamminger

Rank/Service/Nationality: Lieutenant-Colonel/Air Force/France

Job title: Legal Advisor / Staff Officer

Primary legal focus of effort: Operational Law / New Weapon System/ New Method of Warfare, Centres of Excellence.

Likes: Military history, strategy, geopolitics, military airplanes, Ancient Greece (Επαμεινώνδας, Ξενοφών, Περικλής, Θουκυδίδης...).

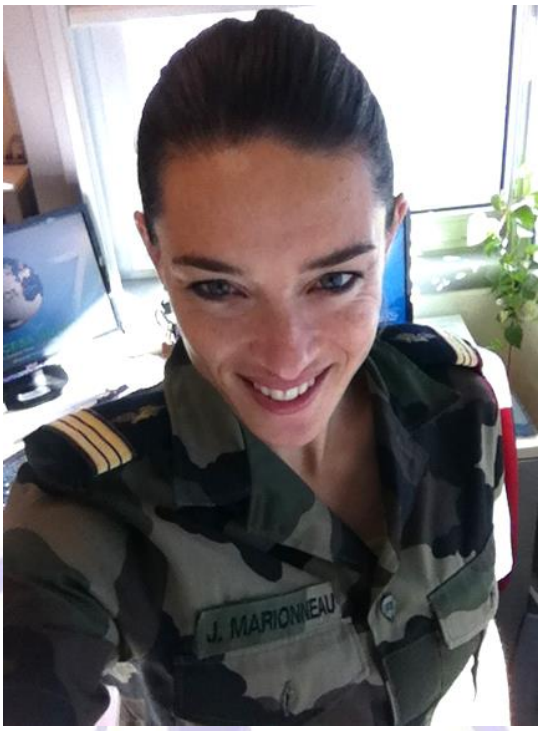
Dislikes: Carthago ("Carthago delenda est").

When in Virginia everyone should visit the Historic Triangle (Yorktown, Jamestown, and Williamsburg) and feel the American history (and a bit of France…).

Best NATO experience: Being a Legal Advisor for Operation Unified Protector. It was an intense experience and satisfying professionally.

My one recommendation for the NATO Legal Community: Learn from the others. Share your experience and thoughts.

NATO SPOTLIGHT



Name: Julie Marionneau

Rank/Service/Nationality: Captain/ Air Force/France

Job title: JFC Naples Legal Advisor

Primary legal focus of effort: International law and Operational Law. NATO's presence in the Balkans region and in Africa (NS2AU).

Likes: Travelling, discovering new places, inviting friends to dinner, practicing all sorts of sports, reading every night.

When in Naples everyone should go to the Opera San Carlo for an amazing night and continue the night with a nice walk on Margellina's pedestrian water front towards Castel dell'Ovo.

Best NATO experience: Being involved as a LEGAD in the Targeting cycle during Operation Unified Protector.

My one recommendation for the NATO Legal Community: Get to know each other. Do not hesitate to share relevant documents and exchange thoughts, new ideas on a particular subject of interest.

HAIL & …

Bienvenue…

ARRC	Maj Harris, John
CAOC Uedem	Maj Van Beem-Van der Laan, Kim
HQ KFOR	Col Ferrucci, Salvatore
	LtC Plöchl, Hans
HQ SACT	LtC Stamminger, Rudolph
JFC Brunssum	Wg CDR Sanger-Davies, Mark Anthony
	Mrs Janseen-Kuijpers, Marian
JFC Naples	CPT Marionneau, Julie
	SFC Parker, William
NATO HQ / IMS	LtC McCollom, Terence J
NHQ Sarajevo	LtC Bennett, Christopher
	MSgt Harden, Twana
NMIOTC	Maj Balis, Nikolaos
NRDC-GER/NDL	Maj Van den Hurk, Emilie
NRDC-ITA	CPT Galbiatti, Marta
	Maj Seghetta, Giovanni
SHAPE	Mr Muñoz Mosquera, Andrés (ACO Legal Advisor)
	Ms Armengou, Helena
	Ms Zarco Lens, Caridad
	Mr Fonseca Lindez, Ignacio
	Mr Garcia Pozo, German
STRIKFORNATO	CDR Harvison, Melissa

www.nato.int

FAREWELL

Bon Voyage…

ACT SEE	Mr Lockwood, Philip
HQ KFOR	Col Arpaia, Bruno
	Maj Stieglbauer, Stefan
HQ SACT	LtC Tuset Anres, Frederic
	Ms Piters, Johanna "Hanneke"
JFC Brunssum	Wg CDR Steele, Allan
JFC Naples	LTC Troiville, Wilfried
NRDC-ITA	Maj Rubino, Luigi
NHQ Sarajevo	LtC Patyski, Lyn T.
	TSgt Franjul, Rafael A.
SHAPE	Mr Randall, Thomas (ACO Legal Advisor)
STRIKFORNATO	LCDR Whittemore, Luke

www.nato.int

UPCOMING EVENTS OF LEGAL INTEREST…

…at the NATO School, Oberammergau, Germany:

The **NATO Legal Advisors Course** will occur from **30 March to 3 April 2015.** The course aims to provide military and civilian legal advisors, in national or NATO billets, an understanding of legal basis for establishing the Alliance, NATO Organisations, International Military Headquarters and other NATO entities. It is focused on the administrative aspects of the Alliance and the NATO functions. The course covers issues such as the International Agreements, the financial aspects of NATO and the role of Commanders and Legal Advisers in NATO.
The Legal Advisors Course takes place twice per year. The second one for 2015 will be the week of **5 to 9 October 2015**.

The **NATO Operational Law Course**, from **11 to 15 May 2015**, aims to provide in-depth training and practical exercises focused on legal issues faced during NATO military operations. The course focuses on operational issues such as the legal aspects of NATO operations, International Humanitarian Law, International Human Rights Law, detention, NATO ROE, targeting, Command limits etc.

***

…at the Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia:

The CCD COE in Tallinn, Estonia organises a course on **International Law of Cyber Operations,** from **19** to **23 January 2015.** The course is an invaluable educational opportunity for military and civilian legal advisors to obtain an in-depth overview of the application of the jus ad bellum and international humanitarian law to cyber operations. The course is offered by the CCDCOE in cooperation with the United States Naval War College and the University of Exeter. The course takes place twice per year with the second one being from 18-22 May 2015.
For more information on how to register for the courses, please visit: **https://www.ccdcoe.org/events.html**

***

…at the Headquarters NATO Rapid Deployable Corps Greece (HQ NRDC-GR), Thessaloniki, Greece:

The Office of the Legal Advisor of HQ NRDC-GR, in Thessaloniki, Greece, organises a Legal Conference on **Innovation in the Law of Armed Conflict: New Challenges, New Perspectives,** the **14-15 January 2015**. The aim of the Conference is to bring together academics and legal advisors, both from the NATO Command and Force Structure, in order to exchange opinions and share views on the contemporary challenges of the Law of Armed Conflict.
For more information on the conference, please contact:
Maj Karatzias, Vasileios, Senior LEGAD, v.karatzias@hrfl.grc.nato.int or
Cpt Zalidis, Vasileios, Legal Advisor, v.zalidis@hrfl.grc.nato.int or
Cpt Pantzou, Irini, Legal Advisor, i.pantzou@ hrfl.grc.nato.int.
(Tel: +30 2310 882428 or +30 2310 882460)

***

…at the University of Adelaide, Australia:

The University of Adelaide, in partnership with the McGill University Institute of Air and Space Law (Montreal, Canada), is offering **a Masters Level course on Strategic Space Law**. The course gives a unique opportunity for lawyers and other professionals to study space law in both its military and commercial aspects in a strategic context. This course examines the legal aspects of space security, globally and domestically.
For more information, please visit:
http://www.adelaide.edu.au/course-outlines/107722/1/sem-1/2014/

***

…of NOTE

The **Canadian Forces Support Unit Europe**, CFSU (E), located in Selfkant-Kaserne, Niederheid, Germany is recruiting a **Liaison Officer – Legal Affairs (paralegal)**. Candidates should be citizens of a NATO country, Law University graduates or professionally trained in similar positions and speak English and German.
For further information on post, please use the following link:
http://www.europe.forces.gc.ca/Resources/Ger-All/GK_Selfkant/rcpo-brpc/_doc/Posters/008-GG-06-14%20-%20Poster%20-%20Assist%20LO%20E%20-%201114.pdf
You can contact the CFSU (E)Regional Civilian Personnel Office at:
rcpo_europe@forces.gc.ca, (Tel: +49(0)2451 717 219).

More information on NATO Cyber related issues can be found on the NATO Multimedia Library web page: http://www.natolibguides.info/cybersecurity

This LibGuide is intended to provide a few starting points to assist you with your research on issues related to cyberspace security, in particular, in the NATO context.

The NATO Legal Gazette can also be found on the official ACT web page: http://www.act.nato.int/publications