NATO
OTAN

RESEARCH PAPER

Research Division – NATO Defense College, Rome – No. 103 – July 2014

Semantics Matter

NATO, Cyberspace and Future Threats

by Christine Hegenbart[1]

Contents

Research Paper
ISSN 2076 – 0949
(Res. Div. NATO Def. Coll., Print)
ISSN 2076 – 0957
(Res. Div. NATO Def. Coll., Online)

NATO Defense College
Research Division
Via Giorgio Pelosi, 1
00143 Rome – Italy
web site: www.ndc.nato.int
e–mail: m.dimartino@ndc.nato.int
https://twitter.com/NDC_Research

DEd'A srl
V.le Scalo S. Lorenzo 55, 00185 Rome, Italy
www.dedaedizioni.it

© NDC 2014 all rights reserved

Promoted by the mass media, catastrophic cyber scenarios are omnipresent: "*Cyber-warfare: Hype and fear*", "*Cyber-security: War on terabytes*" and "*Escalating cyber-attacks – It's about time*" are just some of the recent headlines in *The Economist*[2] for prominent articles on cyber topics. The military perspective emerges explicitly from the choice of wording, suggesting a major security challenge for NATO.

Cyberspace is not physical, but virtual. It is more than the Internet: it is an environment formed by computer networks and by everything they connect and control. It is characterized by the use of electronic devices such as computers to store, modify and exchange data, whether on the Internet or on more restricted networks. In this setting, the prefix "cyber-" defines something related to cyberspace.

NATO relies on the security of cyberspace. As in any other public authority or company, nothing runs without the IT infrastructure. NATO has 30 significant communication networks and over 100,000 personal computers. A secure cyberspace environment is essential not only for communication purposes, but also to operate military equipment, especially in combat. According to current reports, eight to ten sophisticated intrusions and many less complex ones are targeted against NATO's computer systems every day.[3] All in all, NATO counts over 2,500 serious cyber incidents every year, but these hostile cyber activities have not caused major disruptions to NATO's network services. In general, low-threshold cyber incidents with the main purpose of intruding and spying on the organization's systems are

[1] Christine Hegenbart works as a Research Assistant at the Academy for Politics and Current Affairs of the Hanns Seidel Foundation in Munich. She was a PfP Fellow at the Research Division at the NATO Defense College in the spring of 2013. The views expressed in this report are the responsibility of the author and do not necessarily reflect those of the NATO Defense College or the North Atlantic Treaty Organization. The author is grateful for the helpful comments and suggestions provided by her colleagues in Rome, and for the advice and thoughtful insight of experts who have commented on the manuscript.

[2] *The Economist*, print edition, December 2012; print edition, February 2013; online, 17 February 2014.

[3] Nick Watts, "The end of the beginning: NATO getting a grip on the cyber threat", *Defense Viewpoints*, 4 February 2013, available online: http://www.defenceviewpoints.co.uk/interviews/the-end-of-the-beginning-nato-getting-a-grip-on-the-cyber-threat (accessed 24 May 2014).

frequent, but major military incidents are either rare or not reported. By their very nature, cyber threats are global and risks emanating from cyberspace are still on the rise. The Internet infrastructure is also crucial to all NATO member states: their societies and economies rely on it. Governments on both sides of the Atlantic are, therefore, concerned about the threats emanating from cyberspace.

The headlines from *The Economist*, quoted above, illustrate a current trend in cyber semantics: it is difficult to talk about the topic in sober, precise language and without exaggeration. The term *cyber war* is both overused and misleading. Cyberspace is inaccurately described through metaphors and analogies as a battleground – not only by the mass media but also in academic and policy circles. However, cyber threats are not predominantly military. Although the Alliance tends to use quite rational language, it has not yet created an official cyber terminology. Because of the persistent lack of consensus, ambiguous terms like *cyber-attack* or *cyber war* have still to be properly defined. As NATO's decisions are reached by negotiation, rhetoric is particularly important. Terminology and language are central to threat representation, and they also shape threat assessment. As an important player in security policy, NATO therefore has to work against this global trend of exaggeration and vagueness in cyber semantics.

This paper will initially discuss three major events which put cyber security on the forefront of NATO's agenda, and examine how the Alliance has addressed the resulting challenges. It will focus on the serious cyber incidents in Kosovo (1999) and Estonia (2007), as well as the occurrence of the malware Stuxnet (2010). NATO's threat assessment changed significantly through these experiences. In addition, the paper will point out the variety of cyber terminology and comment on how NATO is using it. By introducing a cyber conflict escalation ladder, two important questions will be answered. First, how can NATO ensure that its semantics are consistent with a proper threat assessment? Second, what types of cyber conflict have to be addressed by the Alliance? Finally, the paper will draw conclusions about NATO's future policy on cyber defence and will evaluate how proper language is crucial to tighter cyber security.

Wake-up Calls for NATO in Cyberspace

One of NATO's core tasks is dealing with current and future threats to its members. Several events have revealed that cyber activities can affect national and transatlantic prosperity, security and stability. The configuration of cyberspace allows covert reading, modification and/or deletion of information on computers or in networks; it can be extremely difficult, even impossible, to attribute responsibility for activities carried out through cyberspace. The main reason is that identities in the virtual world can be easily disguised, allowing those responsible for these activities to remain anonymous.

In general, three different techniques are applied in cyber conflicts: Denial of Service (DoS), malware, and active hacking attacks. DoS is an umbrella term which encompasses malicious attempts to make a server unavailable by inundating it with unmanageable quantities of network traffic.[4] The most common variant is known as Distributed Denial of Service (DDoS): multiple systems and Internet connections, often so-called *botnets* of hijacked computers, are involved in shutting down websites and servers. By contrast, *malware* (short for "malicious software") uses different methods to clandestinely infiltrate a computer with the aim of collecting information as well as changing or deleting files. A common example of malware is the so-called virus, a code that self-reproduces in existing applications: it can perform harmful activities, for example, damaging the hard drive by corrupting information. Worms are specific types of viruses that aggressively transmit themselves across many

[4] The term *DoS attack*, however, particularly describes attempts to interrupt or suspend the Internet service of only *one target by a single attacker*. Catherine Paquet, *Network Security Concepts and Policies*, 5 February 2003; available online at http://www.ciscopress.com/articles/article.asp?p=1998559 (accessed 24 May 2014).

computers and are more independent. In addition to DoS and malware, there are also *active hacking attacks* that use different techniques to penetrate a network, stealing or destroying information and leaving no trace of their presence afterwards. The most common types of active hacking attacks are known as "spoofing" or "sniffing". Spoofing means tricking or deceiving computer systems or other computer users by typically hiding one's identity, or by falsifying the identity of another user on the Internet. Sniffing, on the other hand, entails monitoring network data with the aim of acquiring sensitive information such as login details.

These different types of cyber techniques were used in incidents which served as wake-up calls for NATO. Together with the main stages in the development of NATO's cyber defence policies and capabilities, they are briefly summarized below.[5]

Kosovo 1999: targeting an information campaign

The first, widely reported cyber actions against NATO took place in March 1999, during Operation Allied Force. NATO began a 79-day air bombing campaign, intended to force Serbian military units out of Kosovo and to protect the threatened Albanian civilian population. Numerous pro-Serbian hacker groups reacted to this intervention by attacking NATO's Internet infrastructure. After the bombing of the Chinese Embassy in Belgrade by the US, Chinese hackers entered the conflict, too. A DDoS assault created a flood of incoming emails which paralysed NATO's online communication. For several days the NATO public affairs website reporting on the war in Kosovo was not available. At the same time, several official websites of NATO member states were defaced by the placing of anti-NATO messages on them. For example, the message "Tell your government to stop the war"[6] was found on US government websites. The declared objective of disrupting NATO's military operations was not achieved.

Nevertheless, due to this new cyber dimension of the conflict, NATO saw its information campaign hampered and, for the first time, put the topic on its political agenda. The cyber issue, however, was addressed as a technical problem with limited damage potential. To prevent, detect, and respond to these kinds of cyber occurrences, the NATO Computer Incident Response Capability (NCIRC) was created. It consists of two parts, the NCIRC Coordination Centre at NATO Headquaters in Brussels, and the NCIRC Technical Centre in Mons. The Coordination Centre handles incidents in one centralized structure, thereby eliminating duplication. The Technical Centre, on the other hand, aims at achieving a more effective response to cyber threats and provides services to policy-makers. Its scope includes NATO organizations, as well as infrastructure, and it offers the same support to NATO member countries.

Estonia 2007: targeting a nation

Estonia is one of the most wired and technologically advanced countries in the world. At the end of April 2007, the decision to relocate a Soviet-era World War II monument triggered two nights of violent street riots followed by a spate of DDoS activities. By a series of elaborate cyber operations, networks and websites were flooded and became inaccessible. To a certain extent, these activities seemed to be coordinated under a central command and control. Further disruptions consisted of website defacement, as well as massive posting of comments and spamming. These assaults targeted three types of objective: servers responsible for the Estonian Internet infrastructure; websites owned by the government and by prominent politicians, including the Estonian President; and private sector service providers, particularly those of banks and media corporations. Varying in intensity, the attacks lasted more than three weeks, damaging the political, constitutional, economic and social structure

[5] See also Jason Healy, "NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow", *Atlantic Council Issue* Brief, 27 February, 2012, available online at http://www.atlanticcouncil.org/images/files/publication_pdfs/403/022712_ACUS_NATOSmarter_IBM.pdf (accessed 24 May 2014).

[6] Quoted from Dorothy E. Dennig, "Activism, Hacktivism, and Cyberterrorism: the Internet As a Tool for Influencing Foreign Policy", *Networks and Netwars. The Future of Terror, Crime, and* Militancy, ed. by John Arquilla, David Ronfeldt, 2001, available online at http://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1382/MR1382.ch8.pdf (accessed 24 May 2014).

of the state. Communication with the public administration was hindered and the functioning of the domestic economy was perceivably affected. Based in part on technical evidence, the Estonian government accused the Russian government of orchestrating the cyber assaults. Moscow denied any involvement, but refused to help the Estonian investigators identify the perpetrators of the assaults and bring them to justice.[7]

The events in Estonia were widely perceived as the first large-scale cyber-attack on a state, reaching a threshold that marked the phenomenon as a global security concern. NATO, therefore, shifted its focus from an almost exclusively technical perspective to an operational and strategic approach. Consequently, a first Cyber Defence Policy was set up in January 2008: this emphasized not only the need for NATO to secure its own networks, but also the importance of strengthening the Allies' cyber defence capabilities as a whole. Two institutions were created to implement this policy: the Cyber Defence Management Authority (CDMA) in Brussels, and the Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn. The CDMA deploys and coordinates responses to cyber-attacks against NATO and its member states. It has operational capacity and helps improve cyber defence capabilities, providing immediate help if needed and deploying Rapid Reaction Teams (RRTs). The CCDCOE, by contrast, was designed as a research and training centre: amongst other things, it provides concepts that NATO uses to enhance its long-term cyber defence doctrine and runs practical training workshops for up-to-date analysis of lessons learned.

Stuxnet 2010: a new cyber weapon

Stuxnet, the most elaborate malware ever seen, was discovered in summer 2010. Able to control software and electronic industrial equipment, Stuxnet reportedly sabotaged Iran's uranium enrichment facility in Natanz by damaging centrifuges that were critical to the production of nuclear material.[8] The worm is believed to have been developed under the secret operation "Olympic Games", by a team of experts allegedly sponsored by the US and Israel.[9] Stuxnet was described by NATO sources as "the transition from the cyber world to the physical world".[10] It can be seen as a modern tool of indirect intervention to covertly undermine an opponent's network and critical military infrastructure, showing the strategic importance of technological evolution in cyberspace and offering insight into possible future developments of cyber warfare.

Some months later, in November 2010, NATO adopted its new Strategic Concept at the Lisbon Summit. This places greater emphasis than any of the Alliance's previous strategic documents on cyber defence. NATO recognizes that cyber-attacks "can reach a threshold that threatens national and Euro-Atlantic prosperity, security and stability." Therefore, it perceives the need to "develop further our ability to prevent, detect, defend against and recover from cyber-attacks, including by using the NATO planning process to enhance and coordinate national cyber defence capabilities."[11] One step towards achieving this goal was to improve the structure of the NATO Computer Incident Response Capability (NCIRC), so that it is now able to play a key role in responding to any cyber aggression against the Alliance. Furthermore, cyber defence capabilities were incorporated into NATO's Defence Policy and Planning Committee, which provides recommendations to member states in their cyber

[7] *International Cyber Incidents – Legal Considerations*, ed. Eneken Tikk, Kadri Kaska, Liis Vihul, Tallinn 2010, p. 14-35, available online at http://www.ccdcoe.org/publications/books/legalconsiderations.pdf (accessed 24 May 2014).

[8] Gary D. Brown, "Why Iran Didn't Admit Stuxnet Was an Attack", *JFQ* 63 4/2011, p. 70-73. Newer literature questions the damaging effect of Stuxnet on Iranian nuclear facilities, see e.g. Ivanka Barzashka, "Are Cyber Weapons Effective? Assessing Stuxnet's Impact on the Iranian Enrichment Programme", *RUSI Journal* 2/2013, p. 48-56.

[9] David Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran", *New York Times*, 6 June 2012, available online at http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=2&smid=tw-nytimes&seid=auto (accessed 24 May 2014).

[10] NATO, *Rapid Reaction Team to fight cyber attack*, 13 March 2012, available online at http://www.nato.int/cps/en/natolive/news_85161.htm (accessed 24 May 2014).

[11] *Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation adopted by Heads of State and Government in Lisbon*, 19 November 2010.

security efforts. NATO helps Allies secure their networks and offers support and assistance if any of them comes under cyber-attack.

These three examples show the steadily growing complexity and severity of relevant military cyber incidents, though they have been relatively few in number. NATO's mission is defensive in nature; it has no mandate for offensive action in cyberspace. Accordingly, it is dedicated to assuring the security of its member states and high-level cyber threats come within its purview. It prioritizes protection of its own networks, including those of its command structure.

Variety of Terms and Definitions - NATO's Cyber Semantics

There is a lack of commonly accepted labels for hostile cyber events. So far, there is no universal understanding of key cyber terms and, in the absence of consensus, NATO has no accepted definition.[12] Hence, statements by NATO officials on cyber incidents often fail to use coherent terminology. NATO's coverage of the Kosovo cyber assaults mostly consisted of plain information on the technical aspects and their consequences. But DoS attacks are also qualified as "bombardment strategy".[13] In the case of the Estonian attacks, strategic implications too were mentioned. The unspecific terms "cyber-attack" and "cyber defence" were widely used in commenting on these events, which were seen as harbingers of new security challenges in the 21st century: "It is not any more just about artillery and tanks."[14] It is about cyber resources, one may add. Jaap de Hoop Scheffer, then NATO Secretary General, went even further when he stated: "cyberspace has become a kind of peacetime battleground."[15] Comments like these indicate the tendency, in official statements from the military and defence community, to stop short of the more loaded expression *cyber war*.[16] However, one person who did not hesitate to use it was Estonian Minister of Defence Jaak Aaviksoo: "The cyber-attacks against Estonia were true acts of cyber warfare and cyber terrorism."[17] For him, the outcome of the DDoS attacks "can effectively be compared to when your ports are shut to the sea."[18] This rhetoric of war is quite problematic: representing the conflict in this way increases the risk of escalating non-military cyber incidents into international armed conflicts.

The references to Stuxnet in NATO's external communication showed that the organization had increased its rhetoric using military images to reflect the severe and unprecedented nature of the event. One NATO official spoke of a "cyber-attack on the operating system of its [Iran's] nuclear plant";[19] Stuxnet was described as "[a]n offensive cyber weapon"[20]. The catch-all term, cyber-attack, is frequently used.

The linguistic representation of cyber topics by NATO and its member states is certainly influenced by an US-centric assessment system and narrative. Therefore, it is interesting to examine the cyber semantics of the Alliance's largest and most powerful member. On 11 October 2012, the then Secretary

[12] Only "computer network attack" (CNA) and "computer network exploitation" (CNE) are defined by NATO's Standardization Agency in the *Glossary of Terms and Definitions* listing terms of military significance for use in NATO, available online: http://www.fas.org/irp/doddir/other/nato2008.pdf (accessed 24 May 2014).

[13] *NATO Press conference*, 31 March 1999, http://www.nato.int/kosovo/press/p990331a.htm (accessed 24 May 2014).

[14] *NATO Press briefing*, 23 May 2007, available online at http://www.nato.int/cps/en/natolive/opinions_8313.htm?selectedLocale=en (accessed 31 May 2014).

[15] Speech *by NATO Secretary General Jaap de Hoop Scheffer at the NATO Parliamentary Assembly's Annual Session*, Reykjavik, 9 October 2007, available online: http://www.nato.int/docu/speech/2007/s071009a.html (accessed 24 May 2014).

[16] Only a video on NATO's homepage reporting the Estonian case is headlined "War in cyberspace". In addition, a US Representative at the Cooperative Cyber Defence Centre of Excellence in Tallinn used the classification *cyber war* to describe the 2007 cyber actions.

[17] Speech of Jaak Aaviksoo: *Internet: XXI century battlefield.* 16 June 2007, available online: http://www.kmin.ee/en/1470 (accessed 29 May 2014).

[18] Mark Landler, John Markoff, "Digital Fears Emerge After Data Siege in Estonia", *New York Times*, 29 May 2007, available online at http://www.nytimes.com/2007/05/29/technology/29estonia.html?pagewanted=all&_r=0 (accessed 29 May 2014).

[19] Interview with Jamie Shea, 20 September 2010, available online at http://www.defensenews.com/article/20101220/DEFFEAT03/12200301/Jamie-Shea

[20] Interview, 26 October 2011, http://www.atlantic-community.org/index.php/Open_Think_Tank_Article/Jamie_Shea%27s_Answers_to_Your_Questions (accessed 24 May 2014).

of Defense Leon E. Panetta summed up the US view of cyber security in a paradigmatic speech.[21] He demonstratively presented cyberspace as the "new terrain for warfare" and the "battlefield of the future". Panetta also transferred two of the most traumatic events from US history into the cyber domain: he not only prophesied "a cyber Pearl Harbor", but also spoke of "a pre-9/11 moment." Owing to this threat perception, he concluded, the "most important investment" had to be made "in skilled cyber warriors". This language is definitely ramped up, the intention being to mark cyberspace out as a military domain and underscore the rationale for military solutions, with a view to securing the necessary financial support.

The absence of clear cyber terminology contributes to conceptual vagueness and inaccuracy. This leads to confusion in the debate on cyber conflicts. Different classifications have different meanings and consequences: for example, discourse based on the concept of *cyber crime* places it within the purview of the police, whereas talking about *cyber war* means that it is a problem to be dealt with by the military. The choice of wording can thus affect policy choices, and also help answer the question of how cyber threats can be addressed in the most efficient and appropriate way – and what role NATO has to play in the matter. This is crucially important, since differences in threat assessments can make national and international cooperative efforts difficult.

Attempts to create commonly shared and understood definitions of vital cyber terminology within NATO are therefore needed. As a result of the problem of attribution, the perpetrators of malicious cyber activities cannot always be clearly identified. Nevertheless, one can at least try to distinguish between different types of conflicts by the nature of the actors involved, their intentions and the obvious effects of their actions. The definitions offered below might be imperfect, but they at least represent a basis for future discussions:[22]

(1) Hacktivism and Cyber Vandalism

The word *hacktivism* merges the terms 'hacking' and 'activism'. It describes the activity of state-independent individuals or groups who exploit computers and computer networks through special hacking techniques, thus using cyberspace as a medium for protest and to promote political ends. The intention is to disrupt the legitimate use of information, for example by defacing a website or interrupting a web service. In contrast, cyber vandalism is motivated by the hackers' curiosity and desire for self-affirmation, not by a political agenda.

(2) Cyber Crime

Cyber criminals take advantage of cyberspace to promote their illegal activity, sometimes on an organized basis. Cyber crime is motivated by financial gain and includes a broad range of offences like credit card fraud, identity theft and extortion, targeting both individuals and companies.

(3) Cyber Espionage

Companies as well as states and their well-organized and highly professional proxies – that is private hackers acting on their behalf –spy on their targets by sophisticated techniques. Economic espionage has to be distinguished from political and military espionage: the first involves theft of confidential business information and intellectual property of significant economic value; in the second case, the goal is mainly to steal sensitive and classified information from foreign government agencies, on national security issues like military capabilities and strategies. Another potential aim is to test a target computer's defence configuration.

[21] *Remarks by Secretary Leon E. Panetta on Cybersecurity to the Business Executives of National Security*, New York City, 11 October 2012, available online at http://www.defense.gov/transcripts/transcript .aspx?transcriptid=5136 (accessed 24 May 2014). The following quotations are also from this speech.

[22] The definitions are mainly based on Myriam Dunn Cavelty, "The militarization of cyber security as a source of global tension", *Strategic Trends 2012. Key Developments in Global Affairs*, ed. Daniel Möckli. Zurich 2012; James A. Lewis, *The Cyber War Has Not Begun*, Commentary, CSIS, March 2010, available online at http://csis.org/files/publication/100311_TheCyberWarHasNotBegun.pdf (accessed 24 May 2014); Sean Lawson, *NATO & Cyber Conflict: Background & Challenges*. Presented at the Shadow NATO Summit III, Washington D.C, 14/15 May 2012, available online at http://www.basicint.org/sites/default/files/lawson-nato__cyber_conflict.pdf (accessed 24 May 2014).

(4) *Cyber Sabotage*

Here again, it is necessary to distinguish between economic and political-military sabotage. The boundaries between cyber espionage and cyber sabotage are blurred, with the same actors sometimes engaged in both types of activity. The two can also operate in sequence, with cyber sabotage taking advantage of security gaps and vulnerabilities identified by cyber espionage. Cyber sabotage is directed against the integrity and availability of economic or political-military processes and functions of important IT systems, damaging and even destroying equipment or information. Cyber sabotage, unlike hacktivism or cyber vandalism, affects national security, but still remains below the threshold of cyber war.

(5) *Cyber Terrorism*

Terrorist networks and groups, as well as radicalized individuals, might use cyberspace to attract attention, promoting their cause through systematically planned violent actions which inflict physical destruction. Potential targets are usually critical infrastructure sites. Possible results of terrorist cyber-attacks could include plane crashes, water contamination or massive power blackouts. Cyber terrorism can be more than a costly nuisance, since it endangers people and property.

(6) *Cyber War*

National armed forces, as well as state-sponsored and state-authorized militias such as mercenaries, could use cyber techniques to damage, destroy or disrupt an opposing nation state's military capabilities, communication systems or critical infrastructure. Without physical damage and casualties, a cyber conflict is not a cyber war. If the aggressor is not a state actor, it is not cyber war, either. According to many definitions, an act of war has to be instrumental and must involve the use of force for political purposes. This principle also applies to military conflicts in cyberspace.

Cyber war is an ambiguous and controversial term. A more detailed examination is therefore required. To put the question in perspective, it should be specified that cyber war is normally waged in conjunction with military activities and is thus a supporting capability. This means that it is more appropriate to refer to the type of conflict just described here as *cyber warfare*. As in conventional military strategy, *tactical cyber warfare* has to be distinguished from *strategic cyber warfare*. In tactical terms, cyber armed forces aim at achieving dominance in the battlefield through information and communication systems: they facilitate kinetic attacks, for example by penetrating and corrupting guidance system data by means of cyber technology. In other words, cyber capacities serve as an enabler for conventional military operations, or as a means of reducing vulnerability to the opponent's weapons. On the other hand, when a belligerent aims at achieving strategic advantage in the confrontation, the opponent's general ability to function is targeted – for example, by attacking critical infrastructure in the homeland. Both levels of warfare are likely to play a significant role in future armed conflicts.

In contrast, however, a stand-alone cyber war – independent from some larger conflict – seems highly unlikely at present. It is technically possible to conduct crippling cyber-attacks, but major cyber experts do not consider this probable. China, Russia, Israel, France, the United Kingdom and the United States possess the advanced capabilities necessary to launch a cyber aggression, which could cause severe damage and, thus, reach the level of an act of war. Political leaders will most probably not authorize a high-level cyber assault: this is as unlikely as a missile strike. The benefits of a cyber-attack are outbalanced

[23] Bruce Schneier, "When Does Cyber Spying Become a Cyber Attack?", *The Atlantic*, 10.03.2014; available online at http://www.defenseone.com/technology/2014/03/when-does-cyber-spying-become-cyber-attack/80206/ (accessed 12 April 2014).

[24] It is essential to note that no single definition of the term 'terrorism' has yet gained universal acceptance. The term implies a moral judgment that poses inherent difficulties; in my opinion, however, there are no better alternatives to this term. The RAND analysis of Brian Michael Jenkins, *The Study of Terrorism: Definitional Problems* (1980), is still fundamental to this discussion: it is available online at http://www.rand.org/pubs/papers/P6563.html (accessed 24 May 2014).

[25] A classic example is Carl von Clausewitz, *Vom Kriege*, Berlin 1832, 1998.

by the risks:[26] the outcome would be uncertain and, additionally, possible combatants share the inability to defend against a sophisticated counter-cyber strike.[27]

This evaluation takes into account the nature of cyber weapons,[28] i.e. cyber tools designed to cause physical or functional harm to targets in the context of a military conflict. They have various advantages – among others, cheapness, high speed, surprise and covertness. Nevertheless, they also harbor several risks. Cyber weapons are not controllable in a military sense: they are not reliable, and they might result in unintended side effects and blow-backs. As the Internet is used for both military and civilian purposes, there is a particularly high risk of affecting non-combatants. In addition, cyber weapons have to be tailored to one particular target and are therefore, in many cases, 'single-use'. However, most importantly, their destructive payload is often exaggerated – for example, by the media, as well as by security consultants and companies. Usually, cyber-attacks cannot be compared to acts of military violence, let alone to a nuclear attack. Cyber weapons are not decisive: they are not destructive enough to subvert an opponent's will and to degrade capacity to resist. This assessment is supported by an in-depth study by the OECD: "[C]ontrary to many assertions and on present information, few single foreseeable cyber-related events have the capacity to propagate onwards and become a full-scale 'global shock'."[29]

All in all, the use of cyber weapons is especially problematic and is a very serious issue. Currently most states, and also NATO as a military alliance, focus on defending against cyber threats. This strategic orientation raises concerns about the ethical and legal implications of using cyber tools. But an increasing number of nation states see cyber capabilities as important instruments, and as weapons to be used in interstate conflicts. However, military and political decision-makers will have to pay close attention to the circumstances under which it is beneficial to use cyber weapons outside the 'classic' theater of military operations. There is the danger of miscalculating the result of cyber-attacks, thereby escalating the conflict and triggering retaliation outside cyberspace with conventional armaments.

Apart from these six types of cyber conflict, the term *cyber-attack* deserves particular notice. The word takes on a variety of meanings, according to the specific security fields. A precise and narrow definition would help de-escalate the rhetoric. In order to reduce confusion and uncertainty in a military context, the term *cyber-attack* should only be used to describe cyber conflicts with a military dimension. Their effects have to be significantly damaging: either disruptive (i.e. drastic, obvious and immediate) or corruptive (i.e. subtle and persistent).[30] Consequently, only instances of cyber sabotage, cyber terrorism and cyber war(fare) should be identified as *cyber-attacks*.

It is important to define, especially for NATO, what constitutes the use of force through cyber technology. The Tallinn Manual on the International Law Applicable to Cyber Warfare, launched by NATO's CCDCOE is not an Alliance directive, but provides guidance on the matter. It defines a militarily relevant cyber-attack as "a cyber operation, whether offensive or defensive, that is reasonably expected

[26] James A. Lewis, *Conflict and Negotiation in Cyberspace. A Report of the Technology and Public Policy Program*, CSIS, February 2013, available online at http://csis.org/files/publication/130208_Lewis_ConflictCyberspace_Web.pdf (accessed 24 May 2014).

[27] Myriam Dunn Cavelty, The militarization of cyber security as a source of global tension, *Strategic Trends 2012. Key Developments in Global Affairs,* ed. Daniel Möckli. Zurich 2012.

[28] The following is mainly based on Thomas Rid, Peter McBurney, "Cyber-Weapons", *RUSI Journal* 157 1/2012, p. 6-13 and James A. Lewis: *Cyber Attack, Real or Imaged and Cyber War,* CSIS, 11 July 2011, p. 12, available online at http://csis.org/files/publication/130208_Lewis_ConflictCyberspace_Web.pdf (accessed 24 May 2014).

[29] Peter Sommer, Ian Brown, *Reducing Systemic Cybersecurity Risk. OECD/IFP Project on "Future Global Shocks",* 2011, available online at http://www.oecd.org/gov/risk/46889922.pdf (accessed 24 May 2014).

[30] Martin C. Libicki, *Cyberdeterrence and Cyberwar*, Santa Monica 2009, available online at http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf (accessed 24 May 2014).

to cause injury or death to persons or damage or destruction to objects."[31] The definition is shaped by the result: if a cyber operation is followed by significant destructive consequences, it qualifies both as a cyber-attack and as use of force. If hostile cyber activity leads only to inconvenience or irritation, it is neither a cyber-attack nor the use of force. The fundamental understandings of this term have to be discussed because, in the end, the evaluation will be a political decision.

A Cyber Conflict Escalation Ladder – the Cyber Threat Landscape

As shown above, it is a general phenomenon that cyber semantics are characterized by exaggerated and undifferentiated language patterns. To solve this problem, it helps to visualize the types of cyber conflict described above – hacktivism/ cyber vandalism, cyber crime, cyber espionage, cyber sabotage, cyber terrorism and cyber war – as a cyber conflict escalation ladder. This highlights two of their central characteristics: the frequency of occurrence, and the degree of damage or the severity of effects. The escalation ladder leads from the least to the most damaging conflict type, as well as from the most to the least commonly observed type.-

According to this model, the dominant forms of cyber conflict are hacktivism/ cyber vandalism, cyber crime and cyber espionage. The first two have a limited security impact and do not affect national interests. Considering NATO's mission and mandate, they are not particularly relevant. They influence only the standard level of preparedness and are addressed by the routine security procedures of NATO's Computer Incident Response Capability. These conflict types represent an illegal offence under national law, and their prosecution falls under the remit of civil agencies.

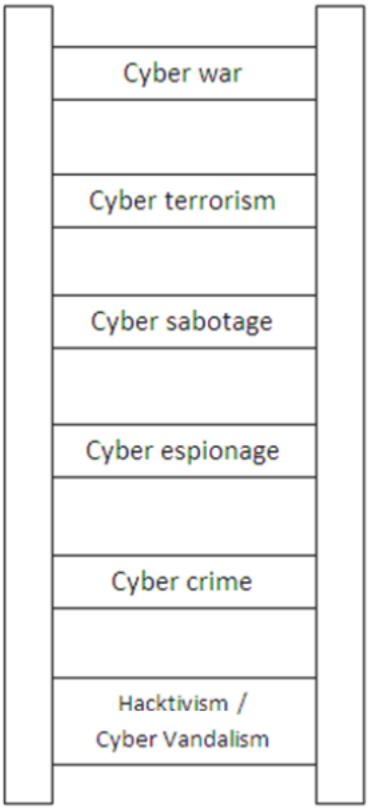

Fig. 1: Cyber conflict escalation ladder

Cyber espionage holds a special position. The indirect damage caused by this prevalent cyber threat might be massive. On the one hand, the transition to cyber sabotage is fluid; on the other hand, the information gained can be used for cyber terrorism and cyber warfare. Therefore, this type of activity potentially has great impact on national security and methods to counter cyber espionage must be given high priority by NATO. The implementation of elaborate security methods is mandatory for the Alliance's classified and operational networks.

[31] *Tallinn Manual on the International Law Applicable to Cyber Warfare*, ed. Michael N. Schmitt, Tallinn 2013.

[32] The model is based on Myriam Dunn Cavelty, "The militarization of cyber security as a source of global tension", *Strategic Trends 2012. Key Developments in Global Affairs*, ed. Daniel Möckli. Zurich 2012; Elgin Brunner, Anna Michalkova, Manuel Suter, Myriam Dunn Cavelty, *Critical Infrastructure Protection. Cybersecurity – Recent Strategies and Policies: An Analysis,* Zurich, August 2009. Available online at http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?lng=en&id=108743 (accessed 24 May 2014).

International law does not prohibit cyber espionage in general. Like conventional espionage, it is a criminal offence and punishable by law in most countries. The responsibility for prosecution lies with civilian authorities. In addition, these cyber activities are dealt with by counter-espionage, for which the security and intelligence services are responsible.

As the conflict escalation ladder illustrates, the other types of cyber conflict – cyber sabotage, cyber terrorism and cyber war – take place infrequently. There are few examples of cyber-attacks causing physical destruction or long-lasting disruption. Stuxnet is the only example of an interstate cyber-attack which caused physical damage. In no instance is a cyber-attack known to have caused casualties. Furthermore, an act of cyber war has never occurred to date. However, NATO has to pay particular attention to these three cyber conflict types, as they have the potential to cause a massive amount of damage. Accordingly, they have high-level security implications, both national and international. Bodies such as ministries of defence, national armed forces and military organizations like NATO have an important role to play in addressing these threats.[33]

With regard to this military dimension of the cyber threat,[34] NATO's interest is twofold. First, cyber-attacks can be relevant to Article IV of the Washington Treaty. As a political-military alliance, NATO consults together with member states whenever "the territorial integrity, political independence or security of any of the Parties is threatened." With regard to cyber security, this is important, as it facilitates procedures for consultation and assistance if cyber-attacks fall below the threshold of an armed attack. Second, cyber-attacks might qualify as armed attacks and thus provide grounds for application of Article V, following the logic that "an armed attack against one or more of them [i.e. the member states] in Europe or North America shall be considered an attack against them all".

Category of Cyber Activity		Level of Security Impact	
		Low	High
	Theft	Hacktivism / cyber vandalism cyber crime	Cyber espionage
	Disruption	Hacktivism / cyber vandalism cyber crime	Cyber sabotage, cyber terrorism, cyber war

Fig. 2: Ordering Cyber conflict types

NATO's Way Ahead in Cyberspace

With regard to the challenges emerging from cyberspace, NATO has to play a relevant role, given that this will be an increasingly contested area in the future. All major militaries are arming in the cyber realm – literally and semantically. Cyber capacities will certainly be deployed in every future military conflict. According to major cyber experts, there is only a small chance of having a devastating cyber war. However, there is a high probability of strategic and tactical cyber warfare in the context of traditional warfare. NATO's mission as a political-military alliance is defensive in nature, and this also applies to cyber security. Nevertheless, NATO has to consider

[33] Cyber terrorism and cyber sabotage have this civil and public responsibility component, too, especially if critical infrastructure or business companies are targeted.

[34] Eneken Tikk, "Global Cybersecurity – Thinking About the Niche for NATO", *SAIS Review of International Affairs*, 30 2/2010, pp. 105-119.

[35] *The North Atlantic Treaty*, 4 April 1949.

cyber threats from a military perspective. This does not mean, however, militarizing non-military cyber threats, such as the numerous low-impact cyber intrusions that NATO is currently facing.

For a proper risk analysis, the Alliance has to take into account the potential and the motivation of possible opponents. The decisive question has to be: "Who has an interest in attacking the cyber environment of NATO or its members, and the capability to do so?" − not "Where are we vulnerable?" For the military, it is of course legitimate to plan for worst-case scenarios. However, using too many resources for the very remote chance of a catastrophic incident makes neither strategic nor financial sense. As this paper concludes, NATO's biggest task is to prepare, in both technical and semantic terms.

(1) Securing IT infrastructure
Given the nature of cyber threats measures to achieve technical assurance are the most important elements of cyber defence. These measures should cover NATO's administrative and operational network systems. The majority of risks can be dealt with in this way. Moreover, better vetting procedures can be adopted to prevent targeted attacks by insiders or through "baiting" techniques. It is unlikely that cyber intrusions can be avoided completely, but it is essential to work on the capabilities to mitigate their effects. Systems should have the ability to recover quickly and – if necessary in the realm of military conflict – to withstand attacks.

NATO's key communication systems are necessarily interconnected; therefore, weakness in any one of them leads to weakness in them all. The member states are responsible for their own cyber security, and hence for implementing sufficient protective measures. Nevertheless, in order to secure these crucial systems NATO should help individual Allies strengthen their cyber defence capabilities for protection of military and civilian cyber infrastructure.

(2) Getting the semantics right
Apart from these technical measures, a proper semantic representation of cyber threats is the most crucial cyber security requirement. In a securitized cyberspace, a vague conception and an imprudent use of the terms *cyber wa*r and *cyber-attack* could be dangerous. NATO should accelerate efforts to set up appropriate cyber conflict classifications and a detailed cyber terminology, which would provide guidance for Allies and Partner countries. Introducing common definitions like those described above, as well as the conflict escalation ladder, is crucial.

The escalation ladder model suggests that only cyber sabotage, cyber terrorism and cyber war are threats that should be depicted as relevant for NATO as a defence alliance. It is not desirable to lower this threshold. Cyber crime and cyber espionage should not be mistaken for cyber war. The term *cyber war* should be used only to describe a severe cyber conflict between or among states, with a destructive impact in the real world. In the context of an international defence organization, the term *cyber-attack* should be used only for cyber activities intended to harm people or property.

Use of language from the military domain – including overuse of the term *cyber war* – potentially triggers fear of possible opponents' cyber capabilities. An overt rhetoric of deterrence could also increase tensions, causing an escalation in the militarization of cyberspace and in cyber conflict, rather than avoiding it. Clear definitions and delimitations would definitely limit this risk. At the same time, they would help prevent escalation of non-military cyber incidents into armed conflicts. NATO, thus, should be in charge of de-escalating rhetoric. Of course, this does not mean that the current challenges faced by governments and organizations like NATO should be played down; it is simply a question of keeping the cyber threat in perspective.

NATO has great potential for discussing and implementing cyber security measures with its members and Partners. Appropriate choice of language will foster an environment for creating the urgently needed norms and international conventions for cyberspace management. The current grey area in international law has to be addressed by a clear definition of what cyber activities should be considered permissible for (non-)state actors.

When it comes to NATO, the military dimension of cyber threats has to be qualified. The nature and the threshold of damage that could trigger an Article V response should be clearly stated for cyber conflicts. In the end, it will be a political choice whether a specific cyber conflict is evaluated as cyber war. For the sake of reliability, this decision should be based on a precise – and, most important, shared – linguistic foundation.

NATO should promote an overarching objective in cyber security: the reduction of threats emerging from cyberspace. In this realm, cyber semantics are essential, with a view to facilitating the de-escalation of potential conflict originating from virtual space. NATO should work against omnipresent cyber-doom scenarios based on vague threat assessments, sensationalism and rhetorical dramatization, whether by the mass media or by decision-makers.