

## **Global Cyber Security – Thinking About The Niche for NATO**

Eneken Tikk<sup>1</sup>

### **Introduction and Background**

The past few years have been very productive for cyber security thinking – shock attacks against Estonia<sup>2</sup>, Georgia<sup>3</sup> and Lithuania<sup>4</sup> as well as cyber surprises like the Conficker<sup>5</sup>, “Operation Aurora”<sup>6</sup> against Google, Adobe and other companies, have given the international community an opportunity to reconsider their views on global cyber security and make a correction of errors where necessary.

NATO was one of the first international organizations to redefine its cyber defense policy package in 2008 in response to cyber attacks against Estonia, thus re-establishing on the 2002 Prague Summit’s concern for cyber security issues. Other international

---

<sup>1</sup> Eneken Tikk is the legal adviser of the Cooperative Cyber Defense Centre of Excellence (CCD COE). She is a PhD student of Tartu University Faculty of Law. The views expressed in this paper are solely those of the author, meant to promote academic discussions about NATO’s role in global cyber security agenda and do not represent the official position of NATO or the CCD COE. The author highly appreciates the input and comments from Mr. Ulf Häussler (NATO), Mrs. Kadri Kaska (CCD COE) and COL Ilmar Tamm (CCD COE) to this paper.

<sup>2</sup> In the context of political tensions between the Estonian and Russian governments, Estonia faced a large-scale distributed denial-of-service attacks against its governmental and critical private sector web servers in 2007 accompanied with defacement of the prime minister’s party’s website and extensive public propaganda. See more Tikk, E. Et al. *International Cyber Incidents: Legal Considerations*. CCD COE Publishing 2010.

<sup>3</sup> Along with the Russo-Georgian War in August 2008, Georgia was victimised by ditributed denial-of-service attacks against its governmental web servers as well as online media channels. The DDoS attacks were accompanied with defacements and extensive propaganda. See more Tikk, E. Et al. *International Cyber Incidents: Legal Considerations*. CCD COE Publishing 2010.

<sup>4</sup> In summer 2008 tensions broke between Lithuania and Russia over the ban in Lithuania of the use of Soviet Symbols. A Lithuanian communication service provider’s vulnerability was exploited to deface more than 300 websites with sickle and hammer. See more Tikk, E. Et al. *International Cyber Incidents: Legal Considerations*. CCD COE Publishing 2010.

<sup>5</sup> Conficker, also known as Downup, Downandup and Kido, is a computer worm targeting the Microsoft Windows operating system that was first detected in November 2008 and is suspected to having compromised public sector and military information systems in many countries. See more, e.g. Conficker Working Group Home Page: <http://www.Confickerworkinggroup.org/wiki/pmwiki.php/Main/HomePage>.

<sup>6</sup> Operation Aurora is a cyber attack that, using the Internet Explorer’s zero-day vulnerability, hit Google, and a number of other Internet commerce and ICT security stakeholder organizations and others in 2009. ccording to McAfee, the primary goal of the attack was to gain access to and potentially modify source code repositories at these high tech, security and defense contractor companies. See, e.g. [http://www.mcafee.com/us/threat\\_center/operation\\_aurora.html](http://www.mcafee.com/us/threat_center/operation_aurora.html).

organizations have actively engaged in reconsidering cyber security issues: the European Union has introduced a number of amendments in its cyber legal and policy framework, the United Nations has opened discussions on cyber security by forming the Group of Governmental Experts on Information Security. Other organizations, such as OSCE and OECD have initiated revisions of their cyber security agenda.

This paper will examine developments in the legal and policy framework for international cyber security.<sup>7</sup> It will elaborate on major international organizations' stakes in global cyber security efforts and indicate the goals relevant to law and policy making and planning in the field, with emphasis placed on NATO's perspectives and potential role in the global cyber security agenda. The intent of the author is to extract NATO's unique characteristics and position in tackling issues of global cyber security as part of the emerging comprehensive approach.

Before looking at NATO's unique features on the global cyber security arena, this article will set the context and reflect on the roles and responsibilities of other international organisations to look at different segments of cyber security and their current coverage on national and international level. It will then move on to look in more detail at NATO's potential role in the global cyber security picture.

## **I Request for a Global Cyber Security Effort: the “Big Picture”**

No nation or corporation these days is truly in a position to face and manage cyber threats on their own – the global architecture of networks, along with the significant number of agents involved in administering these systems, makes it impossible to limit enforcement within organizationally or territorially-defined jurisdictions, a conclusion that prompted the drafting of the 2001 Council of Europe Convention on Cybercrime.<sup>8</sup>

At the same time, cyber threats are, by their very nature, global. Effective defense therefore requires coordination between nations. Securing information society's way of life requires a balance between national and international measures.

Although politically motivated cyber intrusions have occurred frequently in the recent past, it has not overthrown the prevailing consensus that continued development of a robust information society is essential to the advancement of nations.<sup>9</sup> At the same time, the degree to which information and communications technologies (ICT) have penetrated different nations and affected their security differs greatly by country. Thus, the task of securing the cyber domain and information society is both a national and international

---

<sup>7</sup> The background study of this paper (the existing legal and policy instruments of the EU, COE, UN, OSCE, OECD, G8 and ITU in the field of cyber security) is published as Tikk, Frameworks for International Cyber Security: Legal and Policy Instruments. CCD COE Publishing, 2010.

<sup>8</sup> For more information on this, see the Explanatory Memorandum to the Council of Europe Cybercrime Convention (ETS 185). Available <http://conventions.coe.int/treaty/en/reports/html/185.htm>.

<sup>9</sup> Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. Report of the Secretary-General (UN GGE Chairman's draft March 2010).

one. Despite somewhat differing national views on cyber security priorities<sup>10</sup>, cooperation has proved successful among like-minded partners, and there are signs of emerging cyber-coalitions<sup>11</sup>.

To explain NATO’s positioning on the map of international cyber security organizations, it is useful to start with the notion that with the current cyber conflict reaching from internal security breaches to crime to national security relevant incidents and potentially cyber warfare, the responses developed by organizations such as NATO, EU, UN etc need to be put in the context of the segment of cyber threats they are focusing on. Also, international organizations have different quantitative and qualitative potential of improving global cyber security.

The following matrix depicts the areas of attention of different international organizations thereby reflecting the qualitative approach to cyber security. Chart 1 outlines the different dimensions of cyber security, highlighting a specific organization’s input for relevant national law and policy-making domain.

	OSCE	UN	OECD	CoE	EU	G8	NATO
Internet Governance		•	•	•	•		
Cyber Crime	•	•	•	•	•	•	
Cyber Terrorism	•	•				•	•
Cyber Warfare		•					•

Chart 1: Dimensions of Cyber Security

One can see that while Internet and information society governance as well as the fight against cyber crime is in focus of several major international organisations, cyber warfare lies within the area of attention and authority of only the UN and NATO. Although in very broad terms, this understanding will help to define the focus and links between activities of the organizations involved. While collective self-defense in case of a “cyber armed attack” would be something NATO could resolve from legal and policy point of view, the Allies will have to implement cyber crime laws and policies of the EU and Council of Europe.

The level of influence and focus of activity of international organizations heavily depends on their membership. As a forum for cyber security, quantitatively the UN represents the widest possible group of potential consensus, but at the same time also the greatest “cyber security divide”. Like the digital divide, which refers to the disparity of countries, regions and individuals in access to digital and information technology and the unequal availability of relevant skills, the cyber security divide refers to the disparity in the awareness of cyber security, the existence of a relevant legal and policy framework, and availability of the technological solutions for building cyber security.

While a most inclusive forum and thereby uniquely suited to reach a wide consensus on cyber security standards, it is unlikely that the UN would be a forerunner in defining the tools and mechanisms that could serve as the starting point and foundation for such a standard, mainly because of different cyber threat perception and response capabilities of

<sup>10</sup> Russia has advocated the need for cyber arms control, while most European countries and the United States have stressed the need for wider ratification of the Council of Europe Cyber Crime Convention.

<sup>11</sup> NATO CD Policy was proposed jointly by the United States, France, UK and Estonia. In 2008, Russia and China together with 4 more members of the Shanghai Cooperation Organization signed the agreement on Coepration in the Field of International Information Security.

the Member Nations resulting from the divide. Most of the UN's recent activities in the field include the final stage of the GGE discussions and more structured plans to fight cyber crime.<sup>12</sup>

Another relevant point prior to engaging in defining NATO's or any other organization's way ahead in the global cyber security context, is that there are already a number of international instruments in place that either support or potentially contradict with the purposes and means to be developed under any "unique" agenda.<sup>13</sup> Realizing the existing law and policy picture will help to define critical international partnerships and links to national capabilities.

For example, EU is one of the earliest advocates of information society, viewing the cyberspace as integral to our way of life, bringing economic and personal opportunities.<sup>14</sup> Today, the EU has a well-developed legal and policy package for cyber security that contains tens of instruments covering aspects of information society such as electronic signatures, information society services, spam, consumer protection, privacy, copyright and more.<sup>15</sup>

The entry into force of the Lisbon Treaty has strengthened EU's potential as an international security policy actor. The institutional changes brought forth by the Treaty (such as the appointment of the High Representative of the Union for Foreign Affairs and Security and the establishment of the European External Action Service) are expected to ensure better linkages between policy initiatives affecting cyber security and defence. Likewise, commitment by the Member States to act in more coherence (which is expressed e.g. in the solidarity requirements and the obligation to consult among Member States to form common approaches in issues of general interest, as well as the simplified voting requirements in certain issues relating to Common Foreign and Security Policy) will mean a more unified approach among nations. Even more, the Treaty gives authority to the Council to adopt decisions which shall define the approach of the Union to a particular matter which the national policies must conform to. All of the above leads to a strengthened role of the EU as a policy-maker in the international cyber security arena post-Lisbon.

OECD has been another organization supporting the information society development and thereby somewhat similar to those of EU. Countering cyber crime is included in the cyber security agenda of several major organizations. The chart does not reflect regional organizations outside Europe, several of which have also developed programs to counter cyber crime.<sup>16</sup> Responses to cyber crime have traditionally been in the focus of the Council of Europe – the Cyber Crime Convention has been referred to by many as the key instrument to coordinate international responses to cyber incident. In the light of the politically motivated and national cyber security relevant cyber attacks the convention

---

<sup>12</sup> See [http://www.cybercrimelaw.net/documents/UN\\_12th\\_Crime\\_Congress.pdf](http://www.cybercrimelaw.net/documents/UN_12th_Crime_Congress.pdf).

<sup>13</sup> Tikk, Frameworks for International Cyber Security: Legal and Policy Instruments, CCD COE Publishing, 2010.

<sup>14</sup> From the Report of the high-level seminar on Cyber Security, March 10, 2009.

<sup>15</sup> The collection of relevant EU instruments is available in Tikk, Frameworks for International Cyber Security: Legal and Policy Instruments. CCD COE Publishing, 2010.

<sup>16</sup> Examples include ASEAN and OAS.

has received criticism recently and new players have stepped on the cyber crime arena such as OSCE and UN.

Further, international regimes such as the Ethical Dimensions of the Information Society of the WSIS Geneva Declaration of Principles and Plan of Action<sup>17</sup> and the Shanghai Cooperation Organization have put forth agendas for initiating appropriate policy responses to abusive uses of ICTs.

In sum, it is critical for an international organization part of the global cyber security picture to align and optimize its approaches to cyber security aspects relevant to its mandate and members' immediate concerns. As Chart 1 shows, currently the stakes of organizations often overlap and only rarely result in effective and practical agendas to follow on national level.

Qualitatively, NATO is rather well-positioned in the global cyber security picture in that its focus on international peace and security supports the emerging concerns related to national security relevant cyber attacks that have not been responded to by most cyber security regulations and policies so far. At the same time, this also creates challenges when trying to align this dimension of cyber security with the information society and cyber crime efforts adopted and implemented by other organizations.

Quantitatively, NATO Member Nations are rather like-minded when it comes to cyber threat assessment and priorities. Also, NATO has an opportunity to elaborate and discuss cyber security solutions on two different levels of engagement – the Allies and the Partner Nations. This puts NATO in a very good position to analyze and implement the lessons learned from the Estonian and Georgian cyber attacks.

### **Cyber Security from National Authorities' Perspective**

The prevailing international policy view suggests that the first and foremost steps in securing national cyberspace are to be adopted on the domestic level. In the absence of a national reassessment of threats and available defenses, the debate and remedy package on international level can only be abstract. A critical mass of national understanding and consensus is necessary for the development of common concepts on the international level.

Recently, a few shifts have occurred in implementing cyber security law and policy on national level. Historically, the majority of European nations have drafted their original Information Society Strategies in response to the EU information society agenda and with little or no regard to politically motivated cyber crime and cyber security's national security dimension.<sup>18</sup> This might be so due to the fact that only after the Estonian cyber attacks national security relevant cyber incidents have reached the global security concern

---

<sup>17</sup> Available at [http://www.itu.int/wsis/documents/doc\\_multi.asp?lang=en&id=1161|1160](http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=1161|1160).

<sup>18</sup> E.g. Principles of Estonian Information Policy 2004-2006 ([http://www.epractice.eu/files/media/media\\_259.pdf](http://www.epractice.eu/files/media/media_259.pdf)); The Strategy on the Development of the Information Society in Poland for the years 2004-2006 ([www.mswia.gov.pl/download.php?s=56&id=806](http://www.mswia.gov.pl/download.php?s=56&id=806)); Strategy of the Republic of Slovenia in the Information Society ([unpan1.un.org/intradoc/groups/public/documents/.../UNPAN015723.pdf](http://unpan1.un.org/intradoc/groups/public/documents/.../UNPAN015723.pdf)).

threshold. National strategic approaches since 2007 reflect a more coordinated and balanced approach to the whole spectrum of cyber threats and vulnerabilities.<sup>19</sup>

With the cyber security strategic planning focusing on developing more widely accessible services and supporting the growth of e-commerce and social networking, national authorities responsible for economics and communications have served as the counterparts for implementing EU information society directives and action plans. Ministries of telecommunications (or equivalent) have traditionally been responsible for ensuring the quality and security of communications services and infrastructure, primarily deriving guidance from the EU, OECD and UN WSIS.

Law enforcement and justice authorities have jurisdiction over national applications for EU activities in the area of freedom, security and justice as well as various cyber crime instruments. The fight against terrorism as well as national security relevant incidents is typically handled by the Ministry of Interior or its equivalent. Thus far, there is no publicly known information involving terrorist attempts to compromise or disable information networks or to execute operations with physical effects. But one cannot rule out the possibility that such intentions or capabilities may emerge in the future (OSCE, UN).

Under some circumstances, a disruptive activity using ICTs could constitute an armed attack and potentially invoke the right to collective self-defense. A response to a cyber attack crossing the threshold of an armed attack falls under the purview of the military and ministries of defense. Although the Estonian attacks in 2007 cannot be regarded as a valid example of a “cyber armed attack,”<sup>20</sup> military authorities around the world have become more actively involved in strategic cyber security planning after the incident.<sup>21</sup> Individual and collective self-defense in case of a cyber armed attack is subject to coordination between UN, NATO and national authorities responsible for the military domain.

The balance between national and international responses to cyber threats is of extra importance when it comes to concerted actions, e.g. offering assistance to a nation that has fallen victim to a cyber attack – the nature and extent of assistance potentially relies on the duty of care standard exercised by the victim. In the event of a cyber attack, a nation that has not developed a legal framework for tackling cyber crime, has not identified its critical infrastructure and elaborated measures to protect its information society against specific cyber threats, is likely to face less cooperation from the international community than nations that have served their equal share in global cyber security. It is both because in a rapid reaction situation an existing procedure better

---

<sup>19</sup> Examples of recently revised national strategic cyber security approaches include the Estonian Cyber Security Strategy (2008), available [http://mod.gov.ee/files/kmin/img/files/Kuberjulgeoleku\\_strateegia\\_2008-2013\\_ENG.pdf](http://mod.gov.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf); Cyber Security Strategy of the United Kingdom (2009) ([www.cabinetoffice.gov.uk/media/216620/css0906.pdf](http://www.cabinetoffice.gov.uk/media/216620/css0906.pdf)); The Strategy for the Development of the Information Society in Poland until 2013 (2008) ([www.mswia.gov.pl/download.php?s=56&id=806](http://www.mswia.gov.pl/download.php?s=56&id=806)); Australian Government Cyber Security Strategy (2009) (<http://www.ag.gov.au/cybersecurity>).

<sup>20</sup> More about the Estonian incident, e.g. Tikk, Kaska, Vihul, *International Cyber Incidents: Legal Considerations*. CCD COE Publishing 2010.

<sup>21</sup> E.g. in Norway and the Netherlands, the MoD-s are taking the leading role in drafting national cyber security strategy.

supports effective interaction and because there is a certain amount of “homework” that can and needs to be done primarily by the victim. Therefore, implementing “peace-time” cyber security solutions such as security measures to protect personal data, basic protections to e-commerce and an overall mechanism for interaction between national authorities and communication service providers can be regarded as “legal common sense” for countries with any significant information society agenda.

For NATO, the challenge will be to exploit and fit into the already existing, somewhat fragmented, cyber security organization implemented by nations. Being linked to primarily national military structures, NATO needs a practical coordination mechanism not only with the authorities mitigating armed attack equivalent cyber incidents but also those involved in national security relevant attack handling. With the relevant authority currently often poorly defined on national level and engaging national authorities from the areas of governance of communications, justice and internal affairs, creating a working national support mechanism to its mission will be a challenge for NATO.

### **The Call for a Comprehensive Approach to Cyber Security**

Based on current role definition and practices, international organizations exercise different perspectives (information society sustainability, cyber crime, national security relevant cyber threats and cyber warfare) to cyber security often in a stove-piped manner, i.e. with no substantive regard to the overlaps or links between the adjacent areas of responsibility. The same is true for national authorities involved in cyber security planning and cyber risk mitigation.

The contemporary nature of cyber threats requires practical reinforcement of national lines of action along with additional instruments to cover the whole spectrum of cyber threats, including those of national security relevance. This can be achieved via an approach that strengthens national security, tackles cyber crime, inhibits terrorist use of internet, is responsive to a wide variety of risks and threats, enables authorities to protect a wide spectrum of targets ranging from critical infrastructure to individual users while balancing the need to safeguard free speech and privacy.<sup>22</sup>

The call for a comprehensive approach to cyber security is driven by the necessity to move beyond a largely inefficient narrow approach in cyber security development and cyber incident handling. This need has been recognised on both the organizational<sup>23</sup> and national<sup>24</sup> level.

There are many factors to consider in developing a comprehensive approach to cyber security. For one, a comprehensive approach is necessary because of the multifaceted nature of the threat landscape: cyber threats vary from politically-motivated mass cyber attacks to highly precise and sophisticated attacks targeting vital national interests. At the

---

<sup>22</sup> An OSCE Strategy for a Comprehensive Approach to Cybersecurity (Draft as of March 1, 2010). Page 3.

<sup>23</sup> <http://www.osce.org/item/35613.html>

<sup>24</sup> <http://www.cybersecuritymarket.com/2010/03/03/the-comprehensive-national-cybersecurity-initiative/>;  
<http://edition.cnn.com/2009/POLITICS/05/29/cyber.czar.obama/index.html>;  
<http://www.whitehouse.gov/issues/homeland-security>

same time, cyber threats are also fast-evolving. This makes it impossible to establish a definitive catalogue of cyber threats. Instead, a more inclusive approach is necessary.

Secondly, the environment in which these threats emerge differ from nation to nation. Countries are not equal in terms of their ICT penetration and reliance on communication and information technologies, and they have differing interests and priorities. Yet due to the borderless nature of cyber threats, cross-border cooperation is unavoidable, and this requires a certain level of harmonisation of perceptions and activities. Any incident management regime, including a legal one, must facilitate and support coordination and cooperation.

Building up a secure cyber environment and cyber incident management regime also requires a cooperative effort that brings together different fields of expertise. For example, technological issues are to be solved by technological, not legal measures – but these technological capabilities need to be supported by a legal framework.

Last but not least the threat picture is very broad. Recent risk assessments carried out by international organizations highlight threats like malware<sup>25</sup>, botnets<sup>26</sup>, or even state-sponsored cyber aggression<sup>27</sup>, and draw attention to the need to protect new types of services and online environments (such as online social networks<sup>28</sup> and reputation-based systems<sup>29</sup>). This suggests that the cyber threat spectrum that needs to be covered on the international level is significantly wider than a particular nation's immediate concerns.<sup>30</sup>

In short, a comprehensive approach to cyber security combines the elements of threat, deterrence and response from different areas of authority and responsibility, thereby eliminating gaps between relevant areas and highlighting overlaps of authority. A comprehensive approach thereby reduces the likelihood of a cyber attack resulting in an *ad hoc* reaction or falling into a legal or policy loophole.

Also, a comprehensive approach optimizes the roles and responsibilities of different authorities and stake-holders in securing the cyber domain and managing a cyber incident. It focuses on the substantive measures available for cyber security, using the frameworks of cyber security and individual responsibility areas as the foundation for implementing defenses against individual threat factors such as botnets, spam, malware etc. This allows

---

<sup>25</sup> OECD Ministerial background report DSTI/ICCP/REG(2007)5/FINAL (<http://www.oecd.org/dataoecd/53/34/40724457.pdf>).

<sup>26</sup> ENISA Position Paper „Botnets – The Silent Threat“ (2007) (<http://www.enisa.europa.eu/act/res/other-areas/botnets/botnets-2013-the-silent-threat>).

<sup>27</sup> European parliament Study “Cyber Security and Politically, Socially and Religiously Motivated Cyber Attacks” (2009) ([http://www.isis-europe.org/pdf/2009\\_artrel\\_247\\_09-02-epstudy-cyberterrorism.pdf](http://www.isis-europe.org/pdf/2009_artrel_247_09-02-epstudy-cyberterrorism.pdf)).

<sup>28</sup> ENISA Position Paper “Security Issues and Recommendations for Online Social Networks” (<http://www.enisa.europa.eu/act/res/other-areas/social-networks/security-issues-and-recommendations-for-online-social-networks>).

<sup>29</sup> ENISA Position Paper „Reputation-based Systems: a security analysis“ (2007) (<http://www.enisa.europa.eu/act/it/oar/reputation-systems/reputation-based-systems-a-security-analysis>).

<sup>30</sup> While the use of websites by terrorists may not rank high in the Estonian national cyber threat assessment, there have been examples in the past where Estonian servers have been used to accommodate websites with sensitive political background, viewed as terrorist in some countries' perspectives. Therefore, the ability of the Estonian authorities to investigate and potentially restrict access to such websites affects the interested nations' rights.

for more creativity in tackling individual information security areas such as data and privacy, e-commerce or terrorist uses of Internet.

Table 2 outlines the input of international organizations to different aspects and concern areas of information security, delineating regulation areas and perspectives.

	OSCE	UN	OECD	CoE	EU	G8	NATO
Data & Privacy			•	•	•	•	
Spam			•		•		
E-Commerce			•		•		
General Network Security		•	•		•		
CIIP			•		•	•	
Cyber Crime	•	•		•	•	•	
National Security relevant Cyber Crime	•	•					
Terrorist Uses of Internet	•						
Cyber armed attack response		•					•

Chart 2: Areas of Cyber Security

In a comprehensive approach, every stakeholder and measure will have a certain area of responsibility and authority in the common concern area. The following part of this article will envisage a way for NATO to be engaged in global cyber security.

## II NATO and Cyber Security

NATO is a political-military alliance of long standing and thus could be expected to only look at cyber threats from military perspective. Contrary to such an expectation, the Alliance has indicated in its cyber security policy and concept documents<sup>31</sup> that it will not regard cyber security and cyber defence only in traditional military and defence terms. Thinking about NATO's perspective in the field of cyber security, there are three main fields of focus that are other international organizations and regimes have so far failed to manage effectively. These are a) coordinated response mechanisms for cyber armed attacks (issues relevant to Article 5), b) procedures for information exchange, and security responses invoked in a cyber attack that jeopardizes the Allies' territorial integrity, political independence or national security but does not cross the threshold of an armed attack (issues relevant to Article 4), and c) cyber security under the framework of non-Article 5 crisis response operations.

This perspective delineates a focus area distinct from other international organizations' activities. It is separate from cyber crime aspects (that are dealt with under the Council of Europe convention on cybercrime) and general Internet governance and information society development issues (EU, OECD). Of course, the latter two certainly play a role for cyber security in the national security context, but the approach is not complete

<sup>31</sup> NATO's Cyber Security Concept and Policy are not publicly accessible. Cyber Threats are regarded as part of the concept of Hybrid Threats. See <http://www.afcea.org/events/jwc/10/documents/ACTandJIWCJWCBrief2010v2.1.pdf>.

without involving the focus issues mentioned above: namely warfare, crisis, and peace operations.

Article 5<sup>32</sup> of the North Atlantic Treaty is more familiar to the general public as the deterrent of armed attacks against the Allies justifying the engagement of military in collective self-defence. Article 4<sup>33</sup> provides for coordination and consultation mechanism for cyber threats of a lower threshold, therefore better responding to the contemporary cyber conflict paradigm. Preparing its responses under both provisions, NATO is starting to combine political, military, industrial and technological approaches to cyber-security.

The current policy framework focuses on the security of NATO's systems and the assistance to Allies in case of a cyber attack. According to the Policy NATO is responsible for its own information systems, the Allies are responsible for their networks and infrastructure, and there is a shared responsibility for connections between NATO and nations.<sup>34</sup> Although nations have the prime responsibility for protecting their national networks, NATO has the ability to assist those members who request support against a cyber attack through the dispatch of expert teams.

NATO is currently developing a new Strategic Concept defining the Alliance's mission and purpose for the coming decade. In May 2010, the expert group led by former US Secretary of State Madeleine Albright delivered its analysis and recommendations to the Secretary General, assisting him in drafting the new Strategic Concept.<sup>35</sup> The Group of Experts recognized the significance of cyber threats and concluded that "serious gaps" persist in NATO's cyber defence capabilities. Accordingly, the experts recommended that NATO recognize cyber attacks as a growing threat to the security of the Alliance and its members and accelerate its response efforts by securing NATO's communications and command systems and by helping Allies improve their ability to prevent and recover from attacks. The group also recommended the development of an array of cyber defence capabilities aimed at effective detection and deterrence.<sup>36</sup>

The current NATO Cyber Defence Policy does not address this question beyond noting the potential application of the Washington Treaty "if appropriate." The Group of Experts' report states that the North Atlantic Council will have to decide the applicability of the Washington Treaty based on the nature, source and scope of the particular security

---

<sup>32</sup> The North Atlantic Treaty, Washington, D.C. 4 April 1949, Article 5: The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognized by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area. Any such armed attack and all measures taken as a result thereof shall immediately be reported to the Security Council. Such measures shall be terminated when the Security Council has taken the measures necessary to restore and maintain international peace and security.

<sup>33</sup> The North Atlantic Treaty, Washington, D.C. 4 April 1949, Article 4: The Parties will consult together whenever, in the opinion of any of them, the territorial integrity, political independence or security of any of the Parties is threatened.

<sup>34</sup> See more in Hughes, NATO and Cyber Defence: Mission Accomplished? Ap 2009 No. 1/4 (available <http://www.atlcom.nl/site/english/nieuws/wp-content/Hughes.pdf>); also Myrli, NATO and Cyber Defence (available <http://www.nato-pa.int/default.asp?SHORTCUT=1782>), para 45-55.

<sup>35</sup> [http://www.nato.int/cps/en/natolive/official\\_texts\\_63654.htm](http://www.nato.int/cps/en/natolive/official_texts_63654.htm).

<sup>36</sup> [http://www.nato.int/cps/en/natolive/official\\_texts\\_63654.htm](http://www.nato.int/cps/en/natolive/official_texts_63654.htm)

challenge. The experts also stated that NATO's preparations must correspond to the full range of potential Article 5 threats. As a result, the Group of Experts did not exclude the applicability of Article 5 but recommended its consideration on a case-by-case analysis.

Yet, there is an opportunity for an enhanced cyber defence role for NATO beyond existing capabilities. Broader questions of how the Alliance would respond to a large-scale cyber attack have not been fully developed, beyond the limited and largely coordinating role of the Cyber Defence Management Board. It will be important to further refine and test Alliance consultation and reaction mechanisms, for example through more challenging scenarios in NATO exercises. NATO could make a significant contribution in the field of concept development. Formulating coherent and effective cyber security concepts will be a challenging task and cyber attacks are only one aspect of the asymmetric threat catalogue. Responding to cyber attacks in combination with other threat scenarios becomes a far more challenging task requiring an even higher level of coordination and agility. Nevertheless, there is an argument to be made for NATO's enhanced role in cyber defence.<sup>37</sup>

To suggest what this enhanced role could be, it should be noted that a few practical issues inhibit the building and exercise of effective cyber defence – the prevailing reluctance of nations to engage in international binding initiatives, continuing agile and sophisticated cyber intrusions often resulting from or exploiting the infrastructure of countries unwilling or unable to provide cooperation to victims and, last but not least, the current balance between security and freedom of the information infrastructure and services.

There is currently a strong pressure on nations to develop their own strategic approach to cyber security – the emerging national-level conceptual thinking is a prerequisite to determining further international action and coordination. At the same time, national experience with the politically motivated cyber incidents shows that effective restructuring of national cyber security authority and organization is needed. It is difficult to achieve these changes, especially since the (perceived) lack of immediate cyber threat and/or an earlier experience of a large-scale incident makes it difficult to build realistic approaches and justify fundamental changes.

### **Possible Ways Ahead**

While national-level responses are key to the further formulation of cyber security leads on international level, only a few nations and international organizations are able to provide assistance to nations in developing their views to national security relevant cyber incidents. National security relevant cyber intrusions are of particular attention to NATO. Both the first response to the DDoS attack against NATO Public Affairs website in 1999<sup>38</sup> and the 2007 Estonian incidents can be seen as incidents beyond the threshold of an “average” cyber crime as both incidents were politically motivated and involved. Thus, NATO's threshold to tackle cyber security has traditionally been above the economically

---

<sup>37</sup> Author's sum-up of NATO ASG (DI) Peter Flory's concluding keynote speech at the CCD COE Cyber Conflict Conference, Tallinn, June 18, 2010.

<sup>38</sup> See Geers, Cyberspace and the Changing Nature of Warfare. <http://www.scmagazineus.com/cyberspace-and-the-changing-nature-of-warfare/article/115929/>.

motivated cyber crime level. Also, considering NATO's mandate<sup>39</sup> and mission, it would be difficult to justify a focus below that threshold.

When looking at global cyber security in terms of threat levels and appropriate responses, NATO could provide the "higher end" of cyber response capabilities. The daily information security framework is the "normal" state of preparedness where security routines are applied that support the balance between security and human rights as requested by the nature of the network and services provided. This segment is driven by EU and OECD. In case of crime, additional measures for pursuit, investigation and evidence gathering would be applied as well as internal measures to prevent further harm. These measures are elaborated and coordinated by COE and UN. And in case of a "cyber armed attack", the relevant components of military will apply the measures with regard to laws regarding war-waging. In kinetic context, this has been done under the mandates of the UN and NATO.

Different dimensions of cyber security could be regarded as levels of preparedness:

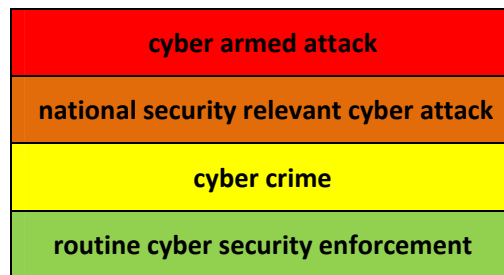


Chart 3. Levels of Cyber security preparedness.

National security relevant attacks are currently least covered on international level. There are a few reasons to this – first, national security is primary the concern for national authorities and thus not overly regulated on international level. Second, this paradigm of cyber conflict is still emerging. Third, balancing the user-oriented information society policy and law against national security concerns is politically very sensitive. It is difficult for any nation to take decisive action in this regard.

Under the presumption that the mission and infrastructure of NATO primarily exist for the purpose of supporting international peace and security, NATO as an organisation is in a good position to develop and apply security measures applicable in case of A4 relevant threat or attack. Applying these measures and procedures on routinely basis, NATO could develop into key partner for state and critical information infrastructure components for defining their "high end" response and coordination mechanisms.

---

<sup>39</sup> The organisation has been set up to safeguard the freedom, common heritage and civilization of the Allies, founded on the principles of democracy, individual liberty and the rule of law. Pursuant to Article 2, the Parties will contribute toward the further development of peaceful and friendly international relations by strengthening their free institutions, by bringing about a better understanding of the principles upon which these institutions are founded, and by promoting conditions of stability and well-being. They will seek to eliminate conflict in their international economic policies and will encourage economic collaboration between any or all of them.

NATO is by its mandate responsible for coordination and consultation in case of national security relevant threats. This places NATO in the position where existing or future cyber security structures of the Allies need to communicate with relevant NATO entities and between themselves.

Substantially, coordinating responses to national security relevant cyber incidents would not require NATO to create any additional international law and it would not force the organisation to wait until the legal inconsistencies and gaps in adjacent focus areas are solved. Instead, coordination and consultation preparedness under Article 4 requires NATO to have regard to and apply the existing legal and policy framework and the exceptions applicable for national security purposes and then investigate the technically possible and politically preferable approaches to implementing the existing exceptions.

The benefits of such approach include the interdisciplinary solution-development whereby legal framework with its gaps and restrictions would not be the decisive factor of success of cyber defence. It would allow NATO to maintain and further develop a dynamic and agile preparedness and the know-how valuable for Allies. Moreover, it would place NATO into constructive debate with other international organisations as regards necessary improvements and further thinking in their areas of responsibility relating to global cyber security.

For the reasons above, NATO is in a favourable position to discuss cyber security in the context of international peace and security, and promote the debate on the proper balance between national security measures and individual freedoms as it pertains to the Internet. NATO's strategic thinkers and experts have a good ground to work with nations that have thus far focused on existing and recognized threat perspectives (i.e. cyber for the UK, energy security for Eastern Europe nations, and nuclear arms concerns for the US) and, looking at the ensemble of national threat assessments in combination of cooperative security concerns, help develop balanced, optimized and coordinated defence mechanisms.

From a purely cyber perspective, NATO approaches to cyber security as regards NATO's own systems could serve as a model of organisational cyber security measures to be applied in the context of a national emergency or security threats. If proven successful in implementation, the measures envisaged could represent best practices in the area beyond the focus of most other international organizations, and would be relevant to national response applicable in a) the entities that represent a national security relevant target *per se*; b) in case of an incident reaching the national security threshold. Gradually, the introduction of such best practices could lead to a more constructive balance between the security and convenience of information infrastructure and services.

Naturally, solutions developed for NATO will inevitably face criticism when transferred and applied to the national context. NATO's approaches are best transferable for "closed" and classified systems with high confidentiality risk, while national emergencies could easily involve the stoppage of the Internet or public networks or compromise of information integrity. Still, several measures (data exchange, monitoring solutions, log

analysis, cooperation with communication service providers etc.) are relevant for all or most types of incidents.

In the first phase, coordination would support national policy processes leading them to explore and assess the national security threats and responses when developing responses to lower level threats and developing relevant tools and infrastructure. While it takes coordination beyond the military and defence authorities' traditional areas of responsibility to counter emerging and often asymmetric threats, this kind of collaboration would benefit both sides and help integrate the civil/military, national/supra-national, public/private etc. aspects of crisis management.

### **Conclusion**

International organizations have recently reinforced their agendas to tackle cyber security in a more comprehensive setting. However, there are issues and perspectives that a) are not practically part of any current initiative, b) are not coordinated and responded to efficiently and c) are vital to achieving a comprehensive and effective cyber security framework. For example, approaches focusing on global information society development and cyber crime demonstrate a notable commitment to fundamental rights and freedoms; however, certain interpretations of pertinent international as well as constitutional human rights law leave but a narrow margin for effectively ensuring cyber security, since they appear to give the main weight to individual fundamental rights in the process of balancing liberties and security. Despite having developed extensive and thorough information security legal and policy frameworks organizations like the EU and COE are not able to build global information security alone while effectively considering the national security end of it. This goes back to the fact that their mission and authority focuses on different aspects of information infrastructure and threats.

There appears to also be a gap in horizontal, cross-organisational coordination of measures and responses – often, international organizations' input to national level tends to be “stove-piped”, focusing on and materializing in only certain areas of responsibility and authority and thereby not forming a comprehensive and coordinated response mechanism.

For these reasons, NATO is in a unique position since a) it is not bound by a substantial earlier heritage of information society law and policy (and is thereby less affected by some of the tensions around the balance between security and fundamental freedoms), b) it focuses on the most sensitive areas of cyber security and c) it could engage in coordination and collaboration that remains outside the area of direct influence and restrictive effects of cyber security deriving from privacy and freedom of information concerns.

NATO offers a forum suitable for coordination and consultation with regard to national security threats that are not considered outright threats to international peace and security. This places NATO in a position where existing or future cyber security structures of the Allies need to be structurally connected with relevant NATO entities and between themselves.

Focusing on the current cyber security paradigm, i.e. national security relevant cyber attacks rather than “cyber armed attacks” would allow NATO to focus with cyber defence

and countering hybrid threats initiatives without being affected by pending national strategic decisions regarding the establishment of cyber commands and other practicalities that over time need to be resolved for Article 5 coordination. It would also relieve the need for assistance on the national level where calls for strategic approaches require immediate action.

To take action at the international level, there is no absolute need to develop or wait for a new international treaty law to be agreed upon. No further instruments are immediately required on the international level, as cyber security of national relevance is primarily to be resolved on the national level. At the same time, for national approaches necessitating coordination and possibly harmonization, a new niche for an international organization has emerged—one that NATO seems well suited to fill.