CHAIRE DE CYBERDÉFENSE ET CYBERSÉCURITÉ
SAINT-CYR THALES SOGETI

NATO and Cyberdefense[1]

Olivier Kempf

May 2013, article n°III.6

Translated from French

“Cyber” is a word on the lips of many strategists because everyone can see that our world is more and more dependent on, not only information and communication technologies, but their interconnectedness. It seems logical, therefore, to consider the consequences of this new environment in the conduct of war, which is considered both an art and a science. NATO is not the only organization to bring up these questions, as seen in the new Strategic Concept, which it adopted on November 2010 at the Lisbon Summit. One of its key messages was the importance of the fight against these new threats and the new environment. Thus, the cyber domain was regularly cited within this new plan. It seems to be the opportune time to take stock of the system in place and to evaluate its relevance and scope.

1 –NATO’s interest in the cyber environment since the 2000s

The Alliance Strategic Concept prior to 1999, did not mention cyberspace or information systems security anywhere. The first appearance of those ideas in a major document is found in a statement given by Alliance leaders after the Prague Summit in 2002, where they announced their decision to "strengthen [their] defense capabilities against cyberattacks."[2] This was following the first cyberattacks by Serbian activists at the time of the Kosovo conflict. "The NATO public affairs website for the war in Kosovo, where the Alliance sought to portray its side of the conflict via briefings and news updates, was ‘virtually inoperable for several days’ thanks to DDoS[3] attacks. A concurrent flood of email also choked NATO’s email server."[4] Accordingly, the program NCIRC (NATO Computer Incident Response Capability) was established in Brussels and Mons.[5] Although the computer attack itself had no operational impact (as it was a "basic" website) it was unacceptable the organization was handicapped in its communications

[1] This text resumes and updates an eponymous article, published with Arnaud Garrigues and released in the spring of 2012 in Sécurité globale No. 19.

[2] Original passage: “renforcer nos capacités de défense contre les cyberattaques.”

[3] DDoS (distributed denial-of-service): attack perpetrated with many computers that flood the target with traffic to overwhelm it and make service unavailable.

[4] SVERRE MYRLI, “NATO and Cyber Defence,” NATO Parliamentary Assembly report no. 173 DSCFC 09 F bis, 2009. See official report in English: http://www.nato-pa.int/default.asp?CAT2=1765&CAT1=16&CAT0=2&COM=1782&MOD=0&SMD=0&SSMD=0&STA=0&ID=0&PAR=0&LNG=0

[5] It depends on the NATO Communications and Information Agency (NCIA) which succeeded the NATO Communication and Information Systems Services Agency (NCSA). See the website: http://www.ncirc.nato.int/index.htm.

capacity. The NCIRC was thus tasked with the protection of NATO's information and communication systems. “It has a key role in responding to any cyber aggression against the Alliance. It provides a means for handling and reporting incidents and disseminating important incident-related information to security management and users.”[6] “Furthermore, it centralizes and coordinates the handling of incidents to a single place, thereby eliminating the duplication of tasks.”[7]

The press release of the Istanbul Summit in 2004 did not cover these issues, but the one of Riga in 2006 was longer and more detailed because the Allies affirmed their intentions to "work to develop a NATO Network Enabled Capability to share information, data and intelligence reliably, securely and without delay in Alliance operations, while improving protection of [their] key information systems against cyber attack."[8] In fact, it was the attack against Estonia in 2007 that got the attention of leaders, especially because the Baltic republic had become a full ally at the time. Up until then, NATO had mainly focused on protecting itself as an organization, and not helping allies when they were the object of such aggressions. Thus, the change was to move from very classic issues about security of information systems (adapted to a military and ally context) to a more global vision of “cyberdefense.” The question is that of military and violence issues, and if such practices are considered an aggression under international law and the UN Conventions.

Following the Estonia experience, defense ministers gathered in Noordwijk in October 2007 and favored the adoption of a "NATO policy on cyberdefense"[9] (classified), which was approved a few months later in April 2008 at the Bucharest Summit.[10]

In a statement at the Bucharest Summit in 2008, leaders showed more formal interest in the issue since the concept of a cyberthreat is the subject of a separate article where the prefix "cyber" is used five times: "NATO remains committed to strengthening key Alliance information systems against cyber attacks. We have recently adopted a Policy on Cyber Defence, and are developing the structures and authorities to carry it out. Our Policy on Cyber Defence emphasises the need for NATO and nations to protect key information systems in accordance with their respective responsibilities; share best practices; and provide a capability to assist Allied nations, upon request, to counter a cyber attack. We look forward to continuing the development of NATO’s cyber defence capabilities and strengthening the linkages between NATO and national authorities."[11]

Similarly, NATO announced the establishment of the Cyber Defense Management Authority (CDMA).[12] "[T]he Authority serves as a central command for the technical, political, and information-sharing efforts of Alliance members, as well as directing and managing existing NATO cyber defence entities. On request, the CDMA is also prepared and able to co-ordinate or provide assistance in a concerted effort if an Ally or Allies fall victim to a cyber attack of national or Allied significance."[13] Sometimes forgotten,

[6] NATO website: http://www.nato.int/cps/fr/natolive/topics_49193.htm, last accessed 9 April 2013. See English version, page 11: http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120116_new-security-challenges-e.pdf

[7] NATO website: http://www.nato.int/cps/fr/natolive/topics_49193.htm, last accessed 9 April 2013. Translated into English, original passage: “Par ailleurs, elle centralise et coordonne le traitement des incidents en un point unique, éliminant de ce fait toute répétition de tâches.”

[8] “Riga Summit Declaration,” 29 December 2006, NATO: http://www.nato.int/cps/en/natohq/official_texts_37920.htm?selectedLocale=en

[9] Original passage in French: “politique de l’OTAN en matière de cyberdéfense.”

[10] “La France a largement participé au processus de définition de la politique de cyberdéfense de l'OTAN,” in “Cyberdéfense : un nouvel enjeu de sécurité,” Information Report No 449 (2007-2008) of M. Roger ROMANI, on behalf of the “commission des affaires étrangères” presented on 8 July 2008.

[11] Bucharest Summit Declaration, 3 April 2008, NATO: Full text in English at: http://www.nato.int/cps/en/natolive/official_texts_8443.htm

[12] “NATO sets up cyber defense management authority in Brussels,” Computer weekly, 4 April 2008 : http://www.computerweekly.com/Articles/2008/04/04/230143/Nato-sets-up-Cyber-Defence-Management-Authority-in-Brussels.htm. “*The CDMA will co-ordinate responses to attacks if invited by national cyberdefence authorities. It will also develop and propose standards and procedures for national and Nato cyberdefence organisations to prevent, detect and deter attacks*”

[13] Sverre Myrli, op. Cit. See English version : http://www.nato-pa.int/default.asp?CAT2=1765&CAT1=16&CAT0=2&COM=1782&MOD=0&SMD=0&SSMD=0&STA=0&ID=0&PAR=0&LNG=0

the Office of C3 (C3B) of the former agency NC3A (NATO Consultation, Command and Control Agency)[14] also provides technical expertise in the areas of information technology and communication and has experienced an increase in the volume its activities related to security."[15]

The Strasbourg-Kehl Summit goes even farther into detail, as the prefix "cyber" is used eight times in the final declaration.[16] Everyone recognized that during the conflict in Georgia, in the summer of 2008, attacks were launched against Tbilisi. Though Georgia was a partner that had less capacity in terms of information systems, unlike Estonia, it was clear that the attacks were important because they supported classical conflict.[17]

Confrontation, for hacktivists communities, has been for some years a quasi-conventional means of expressing grievances, especially in zones of tension or conflict. In this way, the cyberattacks in Georgia were not game-changing because the "target," the Georgian internet and networks, were not crucial strategic targets. However, the Georgia case seems to highlight preparation capabilities and the interrelationship with military actions. Despite the lack of proof, common in cyberattack cases, it nevertheless seems that these well-organized groups push one to deeply analyze these types of events and to develop responses and reactions. Thus, the Alliance announced the creation of rapid reaction teams that could be made available to Member States in case of attack. A request sent by non-member states must be approved by the North Atlantic Council.

2 -The Lisbon Summit and cyberspace

In 2010, the guidelines were confirmed. First, the Allied Command Transformation drew from subjects covered in the "Multiple Futures Project" (April 2009) to help prepare the drafting of the new Strategic Concept. It recommended writing a strategic concept for cyberdefense, which includes improving the technical capacity to detect, identify, and track cyberattacks and engage attackers, thereby developing cyber-offensive capabilities. Also in preparation for the concept, a high-level conference was held in Tallinn in June of 2009. Lastly, an expert group led by Madame Albright issued a preliminary report on the concept that called for protection against non-conventional threats.[18]

The Strategic Concept illustrates the importance given to the field at the time, elevating it to a top Alliance priority, and to which two articles are dedicated.[19] This innovation is brought about by "using

[14] La NC3A a été intégrée à la NCIA. http://www.ncia.nato.int/Pages/default.aspx

[15] Sverre Myrli, op. Cit. See official document: http://www.nato-pa.int/default.asp?SHORTCUT=1782

[16] Art. 49: "We remain committed to strengthening communication and information systems that are of critical importance to the Alliance against cyber attacks, as state and non-state actors may try to exploit the Alliance's and Allies' growing reliance on these systems. To prevent and respond to such attacks, in line with our agreed Policy on Cyber Defence, we have established a NATO Cyber Defence Management Authority, improved the existing Computer Incident Response Capability, and activated the Cooperative Cyber Defence Centre of Excellence in Estonia. We will accelerate our cyber defence capabilities in order to achieve full readiness. Cyber defence is being made an integral part of NATO exercises. We are further strengthening the linkages between NATO and Partner countries on protection against cyber attacks. In this vein, we have developed a framework for cooperation on cyber defence between NATO and Partner countries, and acknowledge the need to cooperate with international organisations, as appropriate." See NATO website: http://www.nato.int/cps/fr/natohq/news_52837.htm?selectedLocale=en

[17] See Arnaud Garrigues, "Géorgie 2008 : le vrai visage de la cyberguerre ? " in St. Dossé and O. Kempf, Stratégies du cyberespace, Cahier AGS/ l'esprit du livre, June 2011.

[18] "NATO must accelerate efforts to respond to the danger of cyber attacks by protecting its own communications and command systems, helping Allies to improve their ability to prevent and recover from attacks, and developing an array of cyber defence capabilities aimed at effective detection and deterrence." For more see website: http://www.nato.int/cps/fr/natohq/news_64088.htm?selectedLocale=en

[19] Art 12: Cyber attacks are becoming more frequent, more organised and more costly in the damage that they inflict on government administrations, businesses, economies and potentially also transportation and supply networks and other critical infrastructure; they can reach a threshold that threatens national and Euro-Atlantic prosperity, security and stability. Foreign militaries and intelligence services, organised criminals, terrorist and/or extremist groups can each be the source of such attacks.

Art 19: (…) 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, bringing all NATO bodies under centralized cyber protection, and better integrating NATO cyber awareness, warning and response with member nations;(…)

the NATO planning process to enhance and coordinate national cyber-defence capabilities,"[20] which suggests that cyberdefense is included in the planning of defense and possibly in defense plans.[21] This vision is altogether logical since "cyberdefense" includes safeguards and information system security, and is a long-term and complex approach; however, it is not a part of, at first sight, a military vision. It also covers operational aspects, like responses to cyber-crises that NATO could face as an organization. It notes that it is therefore necessary to develop capabilities, plans and response scenarios. Finally, it includes a more military component relating to NATO missions that could be described as a reaction to cyberattacks on a Member State that is the victim of an aggression.

More concretely, leaders issued a statement[22] at the end of the Summit that sets out the short-term objectives for accelerating the development of the NCIRC, establishing a centralized cyber-protection system, and renewing cyberdefense policy.

The Chicago Summit confirms that the cyber domain is receiving attention. Thus, Article 49 of the Declaration Issued by the Heads of State and Governments, published May 20, 2012, stated: “Cyber attacks continue to increase significantly in number and evolve in sophistication and complexity. We reaffirm the cyber defence commitments made at the Lisbon Summit. Following Lisbon, last year we adopted a Cyber Defence Concept, Policy, and Action Plan, which are now being implemented. Building on NATO’s existing capabilities, the critical elements of the NATO Computer Incident Response Capability (NCIRC) Full Operational Capability (FOC), including protection of most sites and users, will be in place by the end of 2012. We have committed to provide the resources and complete the necessary reforms to bring all NATO bodies under centralised cyber protection, to ensure that enhanced cyber defence capabilities protect our collective investment in NATO. We will further integrate cyber defence measures into Alliance structures and procedures and, as individual nations, we remain committed to identifying and delivering national cyber defence capabilities that strengthen Alliance collaboration and interoperability, including through NATO defence planning processes. We will develop further our ability to prevent, detect, defend against, and recover from cyber attacks**.** To address the cyber security threats and to improve our common security, we are committed to engage with relevant partner nations on a case-by-case basis and with international organisations, inter alia the EU, as agreed, the Council of Europe, the UN and the OSCE, in order to increase concrete cooperation. We will also take full advantage of the expertise offered by the Cooperative Cyber Defence Centre of Excellence in Estonia.”[23]

Other actions demonstrated Ally interest in the cyber domain. In August of 2010, NATO’s International Secretariat in Brussels created the new "Emerging Security Challenges Division,"[24] which notably includes an office dedicated to cyberconflict. Finally, on March 10th, 2011, NATO Defence Ministers

[20] See the English version: http://nato.int/cps/en/natohq/official_texts_68580.htm?selectedLocale=en

[21] See the NATO website http://www.nato.int/cps/fr/natolive/topics_49193.htm: NATO will also use its defense planning process to promote the development of cyberdefense capabilities of the Allies, to help the Allies at their request and optimize information sharing, collaboration and interoperability. The Allies also work to support the development of international norms on conduct in cyberspace.

[22] Art 40 : Cyber threats are rapidly increasing and evolving in sophistication. In order to ensure NATO’s permanent and unfettered access to cyberspace and integrity of its critical systems, we will take into account the cyber dimension of modern conflicts in NATO’s doctrine and improve its capabilities to detect, assess, prevent, defend and recover in case of a cyber attack against systems of critical importance to the Alliance. We will strive in particular to accelerate NATO Computer Incident Response Capability (NCIRC) to Full Operational Capability (FOC) by 2012 and the bringing of all NATO bodies under centralised cyber protection. We will use NATO’s defence planning processes in order to promote the development of Allies’ cyber defence capabilities, to assist individual Allies upon request, and to optimise information sharing, collaboration and interoperability. To address the security risks emanating from cyberspace, we will work closely with other actors, such as the UN and the EU, as agreed. We have tasked the Council to develop, drawing notably on existing international structures and on the basis of a review of our current policy, a NATO in-depth cyber defence policy by June 2011 and to prepare an action plan for its implementation.

[23] See the official publication: http://www.nato.int/cps/fr/natohq/official_texts_87593.htm?selectedLocale=en

[24] See the official publication: http://www.nato.int/cps/en/SID-ED0F7AEC-2EF6EC44/natolive/news_65107.htm.

approved a new concept paper on cyberdefense.[25] They approved a new NATO cyberdefense policy[26] and an action plan at a meeting in June of 2011 (the action plan was approved by the Ministers in October of 2011). As the NATO website explains,[27] " …[the new] policy offers a coordinated approach to cyber defence across the Alliance with a focus on preventing cyber attacks and building resilience. All NATO structures will be brought under centralised protection, and new cyber defence requirements will be applied. The policy clarifies political and operational mechanisms of NATO's response to cyber attacks, and integrates cyber defence into NATO's Defence Planning Process…It also sets out the framework for how NATO will assist Allies, upon request, in their own cyber defence efforts, with the aim to optimise information sharing and situational awareness, collaboration and secure interoperability based on NATO agreed standards. Finally, the policy sets the principles on NATO's cyber defence cooperation with partner countries, international organisations, the private sector and academia."[28] Also, "in February 2012, a contract worth €58 million euros was awarded for the upgrade of the NATO Computer Incident Response Capacity (NCIRC), which was to achieve full operational capability by the end of 2012. A cybernetic monitoring cell, which will have the role of strengthening intelligence sharing and knowledge of the situation, is also about to be established."[29]

At the same time, in the new conceptual project, the "Global Commons"[30] ACT enumerates four spaces that deserve future action from the Alliance: the sea, air, space and cyberspace. The Supreme Allied Commander Transformation (SACT) explains: "First and foremost, we do not presume that the "Global Commons" are the places where conflicts will necessarily take place in the future. But these are areas where any infringement of free access to them has a considerable impact, not only on the possibility of implementing practices of the military but also of our societies, their security and global economic prosperity. [T]oday, these spaces are increasingly vulnerable. No nation is able to respond alone to these threats. This study aims to help us better understand future challenges. It works to bring about, in time, a more in-depth discussion surrounding ideas like employment, doctrines and capabilities."[31]

3 Alliance action

The Alliance actions today are organized into four categories: coordination (CDMA), aid to allies (rapid reaction teams), research and training, and cooperation with partners.

Coordination

The North Atlantic Council supervises cyberdense actions on a political level, and it is the primary level of political decision-making in a cyberdefense crisis. It is assisted by the Defence Policy and Planning Committee (DPPC). On an operational level, the Cyber Defense Management Board (CDMB), is responsible for coordinating cyberdefense activities throughout NATO's civilian and military agencies. It

[25] http://www.nato.int/cps/fr/SID-CC3D342A-5F1A90A5/natolive/news_71432.htm?selectedLocale=fr

[26] See NATO, "la politique de cyberdéfense en un coup d'œil," NATO site, September 2011, http://www.nato.int/nato_static/assets/pdf/pdf_2011_09/20111004_110914-policy-cyberdefence-fr.pdf

[27] See http://www.nato.int/cps/fr/SID-C4621EB1-D3267419/natolive/topics_78170.htm

[28] See official publication in English: http://www.nato.int/cps/en/natolive/news_75358.htm

[29] Translated into English, original quote in French "en février 2012, un marché d'une valeur de 58 millions d'euros a été attribué en vue de OTAN de réaction aux incidents informatiques (NCIRC), qui devrait être pleinement opérationnelle d'ici fin 2012. Une Cellule de veille cybernétique, dont le rôle sera de renforcer le partage du renseignement et la connaissance de la situation, est également sur le point d'être mise en place."

[30] http://www.act.nato.int/activities/seminars-symposia/the-global-commons

[31] To see more on Global Commons, see O. Kempf, « *Introduction à la cyberstratégie* », Economica, 2012. Original passage in French: "Tout d'abord, nous ne prétendons pas que les « Global commons » soient le lieu où se dérouleront obligatoirement les conflits dans le futur. Mais ce sont des espaces où toute atteinte au libre accès a un impact considérable, non seulement sur la possibilité de mise en oeuvre des moyens militaires mais aussi sur nos sociétés, leur sécurité et la prospérité économique mondiale. Or, aujourd'hui, ces espaces sont de plus en plus vulnérables. Aucune nation n'est à même d'y répondre seule à des menaces. Cette étude a contribué à mieux visualiser les défis du futur. Elle devrait se traduire à terme par une réflexion plus élaborée en matière de concepts d'emploi, de doctrines et de capacités. "

is placed within the Emerging Security Challenges Division in the international Secretariat. For technical things, it consults the C3 Board (C3B). The statement of requirements is provided by military authorities (Chiefs of Staff, SHAPE and SACT) and the NCIA.

The latter, thanks to the NCIRC, provides technical and operational services ensuring cybersecurity of the organization. "The top level of the NCIRC is the NCIRC Coordination Centre situated in the NATO Headquarters and is composed of NHQC3S personnel. The NCIRC Coordination Centre is an element of the Chiefs of Staff responsible for coordinating cyberdefense activities carried out within NATO and with other countries, with the administrative support of CDMB, planning the annual Cyber Coalition exercise and for liaising (regarding matters of cyberdefense) with international organizations such as the EU, OSCE and the UN / ITU. The Cyber Threat Assessment Cell (CTAC) is also located with the NCIRC Coordination Centre."[32]

Assisting Allies

Some mechanisms have been developed, per the request of an allied country, so that NATO can send rapid reaction teams (RRT). As a matter of fact, the allies are responsible for their own safety and the Alliance is not able to ensure their cyberdefense, in particular the security of their information systems. However, “NATO…will therefore work with the support of national authorities, to define the principles and criteria for ensuring a minimum level of cyberdefense at points of interconnection between the networks of the countries and those of NATO.”[33]

Research and training

In terms of research, the NCIA manages technical projects. Its contributors offer very interesting[34] projects in the field of information system security. In this way, "the Consolidated Information Assurance Picture (CIAP) aims to address these gaps by investigating how all the information required to perform cyberdefence may be consolidated in a comprehensive system, based on a common data model using standards and on a distributed data repository. CIAP also provides various visualization options to monitor consolidated data, including network and geographical views, in order to improve situational awareness."[35]

The DRA (Dynamic Risk Assessment) project, however, is complimentary to CIAP and aims “to continually perform a risk assessment in order to automatically determine the impact of the security posture of the system and the network. [This new methodology] uses an automated attack graph generation tool to determine which vulnerabilities are actually exploitable by an attacker according to the

[32] See: http://www.nato.int/cps/fr/SID-C4621EB1-D3267419/natolive/topics_78170.htm. Original passage in French: “Le premier niveau de la NCIRC est le Centre de coordination de la NCIRC, situé au siège de l'OTAN et composé de personnels du NHQC3S. Le Centre de coordination de la NCIRC est un élément d'état-major responsable de la coordination des activités de cyberdéfense menées au sein de l'OTAN et avec les pays, du soutien administratif du CDMB, de la planification de l'exercice annuel Cyber Coalition, et de la liaison dans le domaine de la cyberdéfense avec les organisations internationales telles que l'UE, l'OSCE et l'ONU/UIT. La Cellule d'évaluation de la cybermenace (CTAC) est également colocalisée avec le Centre de coordination de la NCIRC.”

[33] Original passage in French: “«l’OTAN (…) s’emploiera donc, avec le concours des autorités nationales, à définir les principes et les critères garantissant un niveau minimum de cyberdéfense aux points d'interconnexion entre les réseaux des pays et ceux de l’OTAN.”

[34] See Philippe Lagadec, “Visualisation et Analyse de Risque Dynamique pour la Cyber-Défense,” in http://www.sstic.org/2010/presentation/CyberDefense/ (last accessed 28 May 2011): Presentation of SSI projects of NC3A, in particular, the analysis of risk dynamics in cyberdefense.

[35] The SSTIC translations in English can be found at http://www.decalage.info/sstic10. See original passage in French (https://www.sstic.org/2010/presentation/CyberDefense/): “Le projet CIAP (Consolidated Information Assurance Picture) vise à pallier ce manque en étudiant comment toute l’information nécessaire à la cyber-défense peut être consolidée dans un système complet, reposant sur un modèle de donnée commun s’appuyant sur des standards et sur un système de stockage distribué. CIAP fournit également diverses visualisations complémentaires de toutes les données collectées, notamment des vues d’ensemble de la topologie réseau et des vues géographiques. ”

system architecture. It then determines the resulting risks on assets, services and missions of the organization, in order to prioritize issues and to suggest suitable responses [similar to EBIOS].”[36]

These projects, thus, demonstrate a certain technical dynamism within the organization and a welcome evolution in the development and acquisition of secure communication and information capabilities as well as specific capabilities in field of military information security systems. In terms of training, it is the Cooperative Cyber Defence Centre of Excellence (CCDCOE)[37] in Tallinn (Estonia) that is responsible for the latter.

Though the project dates back to 2004 and was proposed by Estonia to the Alliance (before the events of 2007), the Centre initially reached operational capacity in 2006 and it was officially named the "NATO Centre of Excellence" in 2008. It has a staff of 30 people, notably composed of specialists from contributing countries. In fact, the many NATO Centres of Excellence are not fully integrated into the structure. They are funded by only the participating countries, even if they have Ally approval and they fulfill shared functions. There are currently eleven countries participating in the Tallinn Centre: Estonia, Latvia, Lithuania, Germany, Hungary, Italy, Slovakia, Spain, Netherlands, Poland, and the USA. France and the United Kingdom have announced their participation for the summer 2013.

It organizes its activities around the following four domains: legal and political aspects, concepts and strategy, tactical environment, and protection of critical information infrastructures. In 2010 and 2011 it conducted its activities in the following areas: cyberdefense exercises (the "Cyber Coalition" series and also the "Baltic Cyber Shield" series, which was held in May 2010 and was made in collaboration with the Swedish, later called “Locked Shields” in April 2013); courses on general legal and political topics; technical courses (on cybersurveillance solutions, botnet migration, and attack and defense of IT systems); and conferences (an annual multidisciplinary conference, Cycon, which brings together professionals and researchers with 300 participants−the next conference will be held in June of 2013 and will examine the technical, tactical and legal implications of using automatic methods to manage cyberconflicts).

Eventually, a group of experts produced a manual on international law applicable to cyberconflict,[38] which was published in early 2013. The project was directed for three years by Professor Michael Schmitt from the US Naval War College. It is composed of two parts. The first is regarding cyberspace security in international law and the second deals with the international law of cybernetic conflict. Thus, the main objective of the Manual is to interpret international law relating to cyberonflict. These experts were able to agree on ninety-five laws, accompanied by detailed comments. The experts reached a consensus on the classification of the use of force, armed aggression, and cyberattacks, which is defined as a cybernetic operation, offense or defense that can reasonably be expected to cause loss of life, personal injury, damage or destruction of property. However, they were unable to reach a consensus surrounding the evaluation of armed aggressions thresholds, the concepts of legitimate defense, organized armed groups and direct participation in hostilities.[39] Thus, the contribution of the Tallinn Centre is not on the technical areas of cyberconflict, but rather on the legal and political aspects. What are the criteria (theoretical and practical) for determining if an action falls within the cyber category of conflict?

[36] Ph. Lagadec, op. Cit. The SSTIC translations in English quoted here can be found at http://www.decalage.info/sstic10. Original passage in French: “étude complémentaire de CIAP qui vise à fournir une analyse de risque en temps réel, afin de déterminer automatiquement l’impact réel dû à la situation sécurité globale du système et du réseau. Pour cela une nouvelle méthodologie innovante a été développée en combinant un générateur automatique d’arbres d’attaque (attack trees/graphs) et un moteur d’analyse de risque « traditionnel » similaire à EBIOS.”

[37] See http://www.ccdcoe.org/

[38] MILCW: *Manual on International Law Applicable to Armed Conflicts in Cyberspace*.

[39] See Oriane Barat-Ginies, “Commentaires sur le manuel de Tallinn,” *Egéa*, 12 December 2012 (http://www.egeablog.net/dotclear/index.php?post/2012/12/11/Le-Manuel-de-Tallinn-%3A)

Assistance to partners

This last mission did not initially appear in the objectives of the Alliance. It was added after the adoption of the new NATO policy. This collaboration will be carried out "à la carte." NATO will not hesitate to call on private and academics partners.

Conclusion

The fact remains that the war in Georgia has in some ways shown that tomorrow's conflicts will certainly include "cyber" elements, though their exact form is not yet certain and they could be the source of some surprise. It is probably the legitimacy of NATO in the management of this part of a conflict that has engaged the rest of the Alliance on this issue. However, it would not be legitimate to conduct a conflict reduced to only the cyber environment. First and foremost because it is extremely difficult, in today's world, to isolate the cyber domain from one's environments. In fact, tomorrow's wars will have cyber aspects, but they will not be cyberwars.

The Alliance finds itself in an ambiguous place in this area because war is less simple in the 21st century than it was in 1949, when the Alliance was founded. Essentially, the Alliance is still unsure of its strategic position. Should it adopt the American model of cyber-deterrence? Could that be adapted into the Atlantic context? Or should NATO first focus on increasing its capabilities in protection before considering response options?[40]

[40] For more on this see: V. Joubert, "Five years after Estonia's cyber attacks: lessons learned for NATO ? " *NDC Research Paper*, NDC, May 2012.