CHAIRE DE CYBERDÉFENSE ET CYBERSÉCURITÉ
SAINT-CYR THALES SOGETI

NATO and cyberdefense[1]

Olivier Kempf

May 2013, article n°III.6

Cyber : the word is uttered in ever conference room, by all the strategists, because it is obvious our world is ever more dependent on information and communication technology, but also their general cross-linking. It therefore stands to reason to consider the consequences and implications that this new environment would have on operations of war, given that war is simultaneously art and science.

The Atlantic Alliance isn't the last to consider this matter, as is proven the concept which it adopted during the Lisbon summit of November 2010. One of the main messages was the importance given to the fight against these new threats, in these new environments. Thus, the cyber-environment was regularly designated as a major element of this novelty. It seems sensible to review the current situation, as well as its relevance and its range.

1 – The alliance has been focusing on the cyber-environment since the year 2000.

The preceding concept of 1999 mentioned nowhere cyberspace or information system security. Its first appearance in an important document is in the declaration given by the Alliance leaders at the end of the Prague summit, in 2002, where they decided to "*reinforce our defenses against cyber-attacks*". This follows the first Serbian activist cyber-attacks, during the Kosovo conflict. "*the website on the Kosovo conflict, designed by the State Department and which intended, through presentations and press releases, to allow the Alliance to present its vision of the conflict, was the target of DDoS*[2] *attacks which rendered it almost unavailable for several days". Simultaneously, the NATO server dedicated to email was overrun with an influx of mail*[3]*"*. Subsequently, a NCIRC program (*NATO Computer Incident Response Capability* – NATO's capacity to react to computer incidents) was established in Brussels and Mons[4].

Even though the cyber-attack had no serious operational consequences (it was a "mere" website), it was deemed unacceptable that such an organization could be hampered in its capacity to communicate. The NCIRC dealt with the protection of NATO's own information and communication systems. It "*plays a key role, which consists in reacting to any cyberattack which could be launched against the Alliance. It beholds a means to deal with and flag incidents and communicates crucial information on them to system and security administrators and to users.*

[1] This text quotes and updates an eponym article, published by Arnaud Garrigues during the spring of 2012 in Sécurité globale n° 19.

[2] Distributed service denial: a computer attack involving a high number of computers, perpetrated with the intent of making a resource unavailable.

[3] SVERRE MYRLI, « L'OTAN et la cyberdéfense », Rapport de l'assemblée parlementaire de l'OTAN n° 173 DSCFC 09 F bis, 2009.

[4] It answers to the NATO Information and Communication Agency (NCIA) which replaced the NATO Communication and Information Systems Agency (NCSA). Its website: http://www.ncirc.nato.int/index.htm .

Moreover, it centralizes and coordinates incident management in a single office, thereby avoiding task repetition[5]".

The Istanbul statement didn't broach the question in 2004, but the Riga statement in 2006 was more verbose on it, because the Allies stated their intention to *« strive to develop NATO's network capacity to share information, data and intelligence in a reliable and safe way, while strengthening the protection of our key computer installations against cyberattacks"*. In fact, it was the attack against Estonia, in 2007, which raised awareness amongst leaders, namely because the Baltic Republic was then a fulling standing ally. Until that time, NATO focused its defense on itself, as an organization, and not on protecting its Allies when they were the target of an attack. Therefore, the shift consisted in moving from a traditional view of information system security, to a more global vision of "cyberdefense". The question is, can these actions be considered as military and violent, and therefore be dubbed "aggressions" in the sense of international law and of the UN convention.

In the Estonian attack aftermath, the ministers of Defense gathered in Noordwijk in October of 2007, and favored the creation of a « *NATO policy for cyberdefense* » (classified), which was approved a few months later in the Bucarest summit in April 2008[6].

In their statement, during the Bucarest summit, in 2008, leaders showed a more marked interest, as the cyber-threat was the object of a specific article, where the « -cyber » prefix isused 5 times. *"Nato remains determined to protect its key information systems against cyber-attacks. We have recently adopted a policy on cyberdefense, and are currently designing the structures and authorities for its implementation. Our cyberdefense policy underlines NATO's and its member-*countries *need to protect key computer installations, in respect to their respective responsibilities, sharing best practices, and become able to help, upon their request, the Alliance's countries to counter cyberattacks. We intend fully to pursue the development of NATO's capacities in terms of cyberdefense and reinforce bonds between NATO and national authorities."*

In the same way, NATO announced the creation of a cyberdefense command (the CDMA – *Cyber Defense Management Authority*)[7]. "*This authority will serve as central command for technical, political, and information-pooling activities, as well as lead and manage the existing NATO cyberdefense entities. THE DCMA will also be in charge of readiness and of being able to provide or coordinate, upon request, the help in response to future cyber-attacks directed at one or several allies*[8]*"*.

Often forgotten, the C3 Bureau (C3B) of the ex-NC3A[9] (NATO Consultation, Command and Control Agency) also supplies technical expertise in the field of communication and information technology, and has seen its security-related workload rise.

[5] Agency website , http://www.nato.int/cps/fr/natolive/topics_49193.htm, accessed on April 9, 2013.

[6] « *La France a largement participé au processus de définition de la politique de cyberdéfense de l'OTAN* », in « Cyberdéfense : un nouvel enjeu de sécurité nationale », Rapport d'information n° 449 (2007-2008) de M. Roger ROMANI, for the foreign affairs commissions, filed on July 8, 2008.

[7] Nato sets up cyber defense management authority in Brussels, Computer weekly, 4 avril 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*"

[8] Sverre Myrli, op. Cit.http://www.ncia.nato.int/Pages/default.aspx

[9] The NCA3A has been integrated to the NCIA. http://www.ncia.nato.int/Pages/default.aspx

The summit in Strasbourg-Kehl is even more detailed, the cyber- prefix being used 8 times in its final statement[10]. It was obvious to everyone, during the Georgian conflict, in the summer of 2008, that attacks against Tbilissi were launched, and even if Georgia was a mere partner, and also weakly computerized, unlike Estonia, and confirmed the importance of these attacks, in support of more conventional attacks[11].

The confrontation of hacktivist communities has been, for several years, an almost classic way to express demands, namely in tension or conflict areas. On the precise point, computer attacks in Georgia are not radical game-changers, if only because the Internet "target" or the Georgian networks are not a primary target. However, the Georgian case shows a real preparation and military coordination with military operations. Despite lack of evidence, common in the case of cyber-attacks, there is a feeling of general organization, and entices to analyze, in-depth, the events and develop action and reaction scenarios.

The Alliance thus announced the setting up of rapid reaction teams, ready to be sent to member-countries in the case of an attack. A request for assistance by non-member countries should be validated first by the North Atlantic Council.

2 – The Lisbon summit and cyberspace.

The year 2010 confirmed this new bearing. First and foremost, allied transformation command mentioned this subject within its "multiple futures" study (April of 2009), designed to prepare the drafting of the new strategic concept. It recommended writing a strategic concept for cyberdefense, bettering the technical capacities to detect, identify, pinpoint and engage the cyber-attack point of origin, and develop cyber-offensive capacities. Still in the perspective of preparing the concept, a high-level meeting was held in Tallinn in June of 2009. Finally, the group of experts, led by Mrs. Albright, handed in a draft to the concept which recommended protection against unconventional threats[12].

The strategic concept marked the concern it had for the topic, ranked among the first priorities, by dedicating two articles[13] to it. The newness lies on the resorting to "the

[10] Art. 49 : *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.*

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

[12] « *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.* »

[13] Art 12 : *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.*

NATO planning to reinforce and coordinate the national capacities for cyberdefense» which implies that cyberdefense is part of defense planning and, possibly, of the plans of defense[14].

This vision is, after all, perfectly logical, as “cyberdefense” encompasses an information system security and protection chapter, a long-term and complex process but which isn’t normally part of military preoccupations. It also implies a very operational aspect of response to computer crises which NATO, as an organization, could be confronted to. Finally, it includes a more military dimension, corresponding to the NATO missions and which could be described as a response to computer attacks, which a member-country could undergo, within an aggression phase.

Practically speaking, the leaders’ statement[15], published at the end of the summit, enounces the short-term objectives: accelerate the evolution of the NCIRC, set up a centralized capacity for cyberprotection, and renovate the cyberdefense policy.

The Chicago summit confirmed this focus on cyber. Thus, article 49 of the declaration of heads of state and of governments, published on May 20, 2012, states:

The Chicago summit confirmed this focus on cyber. Therefore, article 49 of the declaration of chiefs of states and governments, published on May 30, 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*

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*; (…)

[14] See the NATO website http://www.nato.int/cps/en/natolive/topics_49193.htm : *L’OTAN utilisera aussi ses processus de planification de défense pour promouvoir le développement des capacités de cyberdéfense des Alliés, aider les Alliés qui en feraient la demande, et optimiser le partage de l’information, la collaboration et l’interopérabilité. Les Alliés s’emploieront aussi à soutenir l’élaboration de normes internationales de conduite dans le cyberespace.*

[15] Art 40 : *yber 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.*

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.» .

Other actions embody the interest held in cyber: the Alliance's international secretariat in Brussels reorganized itself by creating, in August 2010, a new division, "Emerging security challenges[16]", which included one service dedicated to cyberconflicts. Finally, on March 10, 2011, defense ministers of NATO countries approved a new conceptual document on cyberdefense[17]. They approved a new NATO cyberdefense policy[18] and an action plan in their June 2011 meeting (the plan had been approved by ministers in October of 2011). As is explained on the Alliance's website[19], «*The revised policy offers a coordinated approach to cyber defence across the Alliance. It focuses on the capability to better detect, prevent and respond to cyber threats against NATO's networks. All NATO structures will be brought under centralised cyber protection to deal with the vast array of cyber threats it currently faces, integrating these defensive requirements into the NATO Defence Planning Process. This way, Allies will ensure that appropriate cyber defence capabilities are included as part of their planning to protect information infrastructures that are connected to the NATO network and critical for core Alliance tasks. The revised cyber defence policy also stipulates NATO's cooperation with partner countries, international organisations, the private sector and academia.*»

Likewise, «*In February 2012, a €58 million contract was awarded to establish an upgrade of the NCIRC, to be fully operational by autumn 2013. A Cyber Threat Awareness Cell is also being set up to enhance intelligence sharing and situational awareness.*»

Simultaneously, in a new conceptual project, "Global Commons[20]", ACT counts four flat spaces which deserve future actions from the Alliance: sea, air, space and cyberspace. The SACT therefore explains:"*First of all, we do not claim that the "Global Commons" are where conflicts will necessarily take place in the future. But it is a place where any attack on free access will have considerable impact, not only on the ability to deploy military means but also on our societies, their safety and world economic prosperity. No nation is able to respond alone to these threats. This study has contributed to better perception of future challenges. It should give way, eventually, to a more elaborated conception in terms of use, doctrines and capacities[21] ".*

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

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

[18] See NATO, « the cyberdefense policy in one grasp », *NATO website*, September 2011, http://www.nato.int/nato_static/assets/pdf/pdf_2011_09/20111004_110914-policy-cyberdefence-fr.pdf

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

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

[21] For more insight on the notion of Global commons, see O. Kempf, « *Introduction à la cyberstratégie* », Economica, 2012.

3 The Alliance's action

The Alliance's action is currently articulated around 4 domains: Project coordination (CDMA), Aid to allies (quick response teams), research and training and cooperation with partners.

Project coordination

The North Atlantic Counsel supervises the cyberdefense actions at the political level, and it remains the main political decision level in the event of a crisis linked to cyberdefense. It is assisted by the The Defence Policy and Planning Committee. On the operational level, the Cyberdefense Defense Management Bureau (CDMB) is in charge of coordinating cyberdefense activities between all of the civilian and military organizations within NATO. It is embedded in the Emerging Security Challenges Division, at the International Secretariat. For technical questions, it consults the C3 Bureau (C3B). Needs expression is dealt with by military authorities (international staff, SHAPE and SACT) and the NCIA.

The NCIA, thanks to the NCIRC, provides technical and operational services enabling organizational cybersecurity. "The first NCIRC level is the NCIRC Coordination center, located in NATO headquarters and staffed by NHQC3S personnel. The coordination center of NCIRC is a staff element, responsible for coordinating activities of cyberdefense led within NATO and with countries, for administrative support to CDMB, for planning the annual Cyber Coalition exercise, and for liaison with international organizations such as the EU, the OCSE and the UN/WTO. The cyberthreat evaluation cell (CTAC) is also located with the coordination center of the NCIRC[22]".

Aid to allies

Mechanisms have been designed: upon request from an allied country, NATO will send rapid response teams (RRT). Indeed, allies remain in charge of their own security, and the Alliance could not be held responsible for their cyberdefense, and namely the safety of their computer systems. However, "*NATO (...) will work with national authorities to develop principles and criteria to ensure a minimum level of cyber defence where national and NATO networks interconnect.* ».

Research and training

For the research part, the NCIA is in charge of project management in technical projects. Its staff therefore proposes very interesting projects[23], pertaining to computer systems security. Thus, the " *the CIAP project (Consolitated Information Assurance Picture) aims at filling this gap by studying how all the information necessary to cyberdefense can be consolidated in a comprehensive system, hinging on a common data model and on a distributed storage system. CIAP also provides various extra views on all collected data, namely geographical views and comprehensive views of the network topology".*

The DRA project (Dynamic risk assessment), on the other hand, is a "*complementary study from the CIAP which aims at analyzing real-time risks, so as to automatically determine the real impact due to the network and system global security situation. To that end, a new innovating methodology has been developed by joining an automatic attack-tree generator (attack tree/graphs) and a "traditional" risk-analysis motor, similar to EBIOS[24]".*

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

[23] See Philippe Lagadec, « Visualisation et Analyse de Risque Dynamique pour la Cyber-Défense », in http://www.sstic.org/2010/presentation/CyberDefense/ (accessed on May 28, 2011): Présentation des projets SSI du NC3A en matière notamment d'analyse de risque dynamique pour la cyber-défense.

[24] Ph. Lagadec, op. Cit.

These projects therefore indicate a certain technical momentum within the organization, and an appreciated evolution in the development and acquisition of communication capacities and secured data, as well as specific skills in terms of military information systems security.

As for training, the Cooperative Cyber Defence Centre of Excellence (CCDCOE[25]), from Tallinn, Estonia, is in charge of that area.

If the project goes back to 2004 and was then suggested by Estonia to the Alliance (and therefore prior to the 2007 events), the initial operational capacity of the center is achieved in 2006, and it is officially labeled “NATO excellence center” in 2008. It counts 30 positions, and employs specialists from contributing countries. Indeed, excellence centers are not part of the integrated structure *per se*, and are financed solely by participating countries, even if they have an allied registration and perform a shared function. Therefore, 11 countries partake to the Tallinn center, today: Estonia, Lithuania, Latvia, Germany, Hungary, Italy, Slovakia, Spain, Holland, Poland and the United States. France and the United Kingdom have announced their partaking as of summer of 2013.

It organizes its activity around the four following axes : cyberdefense exercises (“*cybercoalition*” series, but also “*Baltic cyber shield*”, in May of 2010, in collaboration with the Swedes, *Locked shields* in April of 2013), classes on political and legal basics, technical classes (cybersurveilance solutions, botnet migration, attack and defense of IT systems), and conferences (one annual conference, multi-discipline CyCon, gathering researchers and professionals, with 300 participants : the first conference will be held in June of 2013 and will examine the technical, tactical and legal consequences of resorting to automated methods to deal with cyberconflicts).

Finally, a group of experts has proposed a manual on international law, applicable to cyberconflicts[26], which was published in the beginning of 2013. It was directed for 3 years, by Professor Michael Schmitt of the US Naval war college. It is composed of two parts, the first pertaining to cyberspace security within international law, and the second deals with international law applied to cybernetic conflicts. Thus, the main objective of the manual is to interpret the norms of international law to cyberconflicts. Experts have managed to agree on 95 rules of law, along with detailed commentaries. Experts have found a consensus on defining resorting to force, qualifying armed aggression, and cyber-attacks which are defined as a cybernetic operation, offensive or defensive, which can be expected to cause loss in human lives, injuries to people, or damage to and destruction of goods. However, they were unable to agree on the evaluation of the armed aggression threshold, the notion of legitimate defense, and the notions of organized armed groups, and direct partaking to hostilities[27].

The Tallinn centre does therefore not contribute to the technical aspect of cyberconflicts, but more to the legal and political part : which criteria (both theoretical and practical) will enable to determine whether a cyber-action can be categorized within the conflict?

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

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

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

Aid to partners

This last mission initially didn't appear within the objectives of the Alliance. It was added after the adoption of NATO's new policy. This cooperation will be optional for its members. NATO will not hesitate to call upon private companies and university researchers, in this perspective.

Conclusion

The lasting feeling is that the Georgia war, in a way, highlighted that tomorrow's conflicts will necessarily have a "cyber" aspect to them, of which the form is not yet known, and which could therefore come as a surprise. Here lies probably NATO's legitimacy, in the management of the part of a conflict which would engage the rest of the Alliance. But it would not be legitimate to lead a conflict which would be encompassed within the cyber-environment: first of all because it is very difficult, today, to circumscribe cyber within its environment. In fact, tomorrow's war will have cyber aspects to it, but it will not be a cyberwar.

This distinction explains the ambiguous position the Alliance is in, on this field: war in the 21st century will not be as simple as in 1949, when the Alliance was founded. In the end, does the Alliance still hesitate on its strategic position: must it embrace the American model of cyber-deterrence? Is it fit for the Atlantic board? Or shouldn't it concentrate on raising the protection level, before working on retaliation means[28]?

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