NATO OTAN

RESEARCH PAPER

Research Division - NATO Defense College, Rome - No. 76 – May 2012

Five years after Estonia's cyber attacks: lessons learned for NATO?

by Vincent Joubert [1]

Contents

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

NATO Defense College
Research Division
Via Giorgio Pelosi, 1
00143 Rome – Italy
web site: www.ndc.nato.int
e-mail: research@ndc.nato.int

Imprimerie Deltamedia Group
Via Portuense 1555, 00148 Rome, Italy
www.deltamediagroup.it

In April 2007 a series of cyber attacks targeted Estonian information systems and telecommunication networks shortly after the relocation of a controversial World War II memorial, known as the "Bronze Soldier", from Tallinn city centre to a nearby military cemetery. Lasting twenty-two days, the attacks were directed at a range of servers (web, e-mail, DNS) and routers. The most visible targets were web sites of political entities such as the President, the government, the parliament, and political parties; among the other high-profile victims were two important Estonian banks, internet service providers and telecommunications companies.[2] Most of the incidents were Distributed Denial of Service (DDoS) attacks, where the attackers commanded nearly a million "zombie" computers to overflow web sites with requests for data, boosting traffic far beyond regular levels of activity and thus bringing the servers to a standstill.

Estonia, though one of the smallest NATO member states, is one of the most highly wired countries in the world. Almost every activity is done over the internet, from personal banking transactions to education, media access and voting in local elections. Estonian society's ubiquitous information technology (IT) dependence has also made the country highly vulnerable to cyber attacks that could potentially paralyze its everyday activities. The 2007 attacks did not damage much of Estonian IT infrastructure because they were not sophisticated,[3] and also because the limited size of the country allowed its cyber experts to take speedy defence measures for national networks. However, the attacks were a true wake-up call for NATO, offering a practical demonstration that cyber attacks could now cripple an entire nation which is heavily dependent on IT networks. Such a prospect is a new threat for NATO member states, as well as for the integrity and efficient working of the information systems which are vital to the Alliance's core tasks of collective defence and crisis management.

As a result, the 2010 NATO Strategic Concept stated that the Alliance would *"develop further [its] 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 Chicago Summit, just weeks

[1] Vincent Joubert is an Associate Research Fellow at the Centre for Geopolitical Studies of the Raoul Dandurand Chair of Strategic and Diplomatic Studies, UQAM, Montreal, Canada. The views expressed in this paper are those of the author and do not necessarily reflect the official opinions of the NATO Defense College or the North Atlantic Treaty Organization. The author wishes to thank Dr. Jean-Loup Samaan and Dr. Karl-Heinz Kamp for their comments on earlier drafts of this paper.
[2] R. Ottis, "Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective", in *Proceedings of the 7th European Conference on Information Warfare and Security*, Reading: Academic Publishing Limited (2008), pp. 163-168.
[3] Most of the attacks were DDoS targeting web sites and e-mail servers; though a few were SQL attacks on key servers and routers, Estonia's cyber network was not in any serious danger of being shut down (Jeff Goldstein, Diplomatic Cable 07TALLINN375, Wikileaks).

away at the time of writing, will offer an excellent opportunity to consider how the new NATO Policy on Cyber Defence and its implementation have addressed these requirements; it will also be a good time to take stock of hurdles still to be negotiated in building a collective cyber defence strategy, consistent with the operational requirements, juridical challenges and constantly evolving nature of the cyber threat.

The evolution of NATO's attitude to defending information and communication networks

The Alliance has long defended its information and communication systems, but has never faced major attacks that represented a critical threat to them. Cyber attacks were until quite recently considered to have limited potential for harm, so that technical responses were thought to be sufficient. During Operation Allied Force in Kosovo NATO faced attacks from pro-Serbian hacktivists hoping to wreak havoc with the Alliance's war-fighting capabilities, but these led only to e-mail accounts being blocked and NATO's web site being disrupted for some days. As a result of these incidents, however, NATO leaders agreed at the 2002 Prague Summit to implement the Cyber Defence Programme. This led to the establishment of the NATO Computer Incident Response Capability (NCIRC), ensuring detection of cyber attacks, protection of NATO networks against them, and provision of information and assistance to users. Protection of Allies' national networks was left to their own domestic agencies.

In the following years, the development and increasing sophistication of accessible information and communication technologies led to a dramatic growth in the numbers of interconnected networks with poor security, thus creating new vulnerabilities and threats. Member states' economic, diplomatic and military progress benefited from new communication technologies and networks, but also gradually generated a strong dependence on vulnerable communication systems. The Estonian cyber attacks exposed the danger of such dependence: if the coordinated efforts of civilian hackers with unsophisticated techniques resulted in NATO having to send an expert to assist the national Computer Emergency Response Team (CERT), one could easily foresee far greater security risks in the event of more sophisticated state-sponsored cyber attacks.

As a member of NATO, Estonia requested emergency assistance to defend its digital infrastructure against the ongoing attacks. Jaak Aaviksoo, then Estonian Minister of Defence, stated that the attacks *"were aimed at the essential electronic infrastructure"* of Estonia and *"this was the first time that a botnet threatened the security of an entire nation"*.[4] The attacks indeed constituted the first major cyber aggression against a NATO member state, far more important than the ones that targeted the Alliance's website during the Kosovo crisis and, shortly after they ended, Alliance officials held an emergency meeting to address their strategic and political consequences. What quickly became clear was that NATO lacked *"both a coherent cyber doctrine and a comprehensive cyber strategy"*[5]: its Cyber Defence Programme fell patently short of actual needs. While cyber attacks had gradually became a tangible security threat to the communication systems of NATO and individual Allies, the Alliance still lacked the necessary capabilities, clearly defined objectives, and an official position as to how it would respond in the event of a cyber attack.

The Estonian cyber attacks revealed important malfunctions in NATO's cyber defence arrangements, forcing the Alliance to reconsider its strategy in order to cope with this growing threat. As a prerequisite to an overhaul of policy, some important issues had to be addressed: the technical challenge of identifying vulnerabilities on the Alliance's networks, and the political difficulty of defining a defence strategy to be implemented by NATO with the consensus of the Allies. Here it is important to note that cyber attacks are a significant threat to NATO's missions but in practice rarely have a direct military dimension, meaning that the Alliance may actually have only a limited role to play in dealing with them. However, the transnational and multidimensional nature of the cyber threat creates many difficulties. The Alliance needed to assess these thoroughly, as an essential step towards defining its role and responsibilities in setting up defensive measures.

Issues and challenges for NATO cyber defence

The many issues which emerged in 2007 raised crucial questions that needed further examination prior to the implementation of a strategy. Amongst the challenges that have thus arisen for NATO, there has been a focus on three areas in particular: legal, operational, and strategic.

First, from a legal perspective, the circumstances and conditions under which cyber attacks would trigger NATO's collective defence mechanisms (based on Articles 4 and 5 of the North Atlantic Treaty) still need to be defined. These Articles *"indicate that it is the Nations' prerogative to determine whether they consider themselves exposed to a threat or under an armed attack. However, they do not create any automaticism whatsoever concerning the response in such cases"*.[6] A problem in this respect is that there is only limited practical experience on the basis of which to judge the applicability of Articles 4 and 5, and that the response threshold for cyber attacks must therefore be assessed on a case-by-case basis. However, not all states view the matter in the same way: not only is the question of thresholds largely a political concern, but it is further complicated (as in the case of international terrorism) by the overlap between national, transnational and international defence mechanisms. The decision on whether to invoke Article 4 or 5

[4] J. Davis, *"Hackers Take Down the Most Wired Country in Europe"*, wired.com.
[5] R. Hughes, *NATO and Cyberdefence, Mission Accomplished?*, April 2009, No 1/4.
[6] U. Häußler, "Cyber Security and Defence from the Perspective of Articles 4 and 5 of the NATO Treaty", in E. Tikk & A-M. Talihärm (eds), *International Cyber Security Legal & Policy Proceedings*, CCD CoE, 2010.

of the Treaty will therefore *"depend on political policy perceptions, […] and the different roles played by the government agencies involved on the examination and assessment of cyber threats and incidents, and competent to adopt or contribute to actual responses"*.[7]

The legal issue directly related to this consideration is the applicability of existing humanitarian law to cyber attacks. An interesting "consequence-based approach" has been developed by a number of authors, to interpret the notions of "armed conflict" and "attack" in the cyber domain. If adopted, this approach would suffice to make *jus in bello* applicable to cyber attacks[8] and, given the technological progress in modern warfare, some authors consider it more appropriate than the traditional "actor-based approach" to the protection of civilians from contemporary threats. The consequence-based approach rests on the postulate that cyber attacks, because of their potential for causing injury, death, damage or destruction, can from a humanitarian law perspective be identified with physical attacks or incidences of armed conflict and, as such, outlawed. There are, however, important fault lines that need to be discussed before this interpretation of the law can be officially applied to the cyber domain.

Another major concern is the extent to which a state can be considered responsible for cyber attacks launched from its territory. While international law acknowledges the rule of state responsibility for breach of international obligations, and the duty to pay any resulting damages, a state will be responsible for its residents only insofar as it has explicitly allowed them to act on its behalf: *"Proving a formal link between a state resident and a state authority in the case of cyber-attacks might [prove] excessively difficult and [lead to the failure of] any reparatory proceedings"*.[9] Collecting legal evidence will also depend on states' willingness to cooperate with any international investigation and prosecution.[10]

The general underlying questions regarding legal concerns are whether existing international and national laws provide an adequate framework for managing global cyber threats, and how NATO can play a role in global cyber security through the implementation of a suitable strategy.

The second perspective from which NATO needed to examine cyber defence questions after the Estonian attacks was operational: it was obvious that NATO needed to extend its cyber defence capacities. The NCIRC alone could not handle all cyber attacks launched against NATO's internal network and help Allies defend their critical communication infrastructure. The attacks demonstrated that NATO would now have to face a growing number of increasingly sophisticated hostile actions. These could jeopardize a range of networks, including dual-use critical assets (national infrastructure run by private companies, under individual Allies' jurisdiction for purposes of protection but affording vital connections to NATO networks) and communication systems on battlefields. It was plain not only that NATO had to improve the protection of its internal information infrastructure, but also that the need to defend Allies' assets would create important technical challenges and that the sensitive nature of some networks would prove a major obstacle to political agreement. The most significant challenge for the Alliance was therefore to achieve the right balance with a view to implementing a clear, consistent and non-redundant chain of command – in other words, NATO had to focus on ensuring rapid and efficient response to cyber attacks while not overstepping its prerogative.

Finally, from a strategic perspective, the need to defend communication networks from intrusions and attacks created an intellectual challenge because none of the defence strategies and doctrines that worked for any of NATO's other threats could be simply transposed to the uniquely complex digital domain. Cyberspace technologies develop at an extraordinarily rapid pace, both quantitatively and qualitatively. They offer considerable innovative scope, not only in terms of defence capabilities but also for purposes of wrongful use, and therefore pose a major challenge to doctrines and strategies based on older capacities. A case in point is deterrence, of fundamental importance to the Alliance in both nuclear and conventional security. Achievement of deterrence is possible by two different mechanisms. The first of these, deterrence by denial, is based on a level of technological credibility that ensures denial of the adversary's objectives, with a premium on cyber security solutions that afford robust defence of communication networks. The second mechanism is deterrence by punishment. This is set up when a country explicitly states that any action taken against its interests will trigger asymmetric retaliation, meaning that the adversary will inevitably face unbearable costs for any act of aggression. This mechanism implies not only a strong and credible political will, but also the actual capacity to launch asymmetric retaliation.

Deterrence by punishment is problematic in cyberspace, because it raises numerous technical obstacles in terms of establishing who is responsible for the attack and which assets should be targeted when retaliating; another problematic issue is how long retaliation can be effective when limited to the cyber realm, since weak links targeted by retaliatory cyber attacks can often be replaced and strengthened. There are also political and legal issues: determining a threshold for retaliation (when should a cyber attack be considered an act of war?), correctly assessing the original intent (was it an attack, or just a mistake?), involvement of third parties in retaliation (under what conditions would a third party join the retaliation process?), and the strategic credibility

[7] *Ibid.*
[8] See Michael N. Schmitt, "Wired Warfare: Computer attack and *jus in bello*", IRRC June 2002, vol. 84, No. 846, pp. 365-398.
[9] Joanna Kulesza, *State Responsibility for Cyber-Attacks on International Peace and Security*, 29 POLISH Y.B. INT'L L. (2009), 131, pp. 149-50.
[10] See Tikk E. & Kaska K., *"Legal Cooperation to Investigate Cyber Incidents: Estonian Case Study and Lessons"*, 9th European Conference on Information Warfare and Security, Reading: Academic Publishing Limited (2010), pp. 288-294..

of the response in relation to the country's declaratory policy on retaliation (what will be done in response to cyber attacks?).[11]

Implementing a NATO cyber deterrence strategy would have been subject not only to enhancement of cyber security, but also to a strong declaratory policy on retaliation. However, considering the issues raised, it was not in the short-term interest of the Alliance to focus solely on cyber deterrence to the exclusion of other defence models.

Positive achievements

If the attacks raised many questions and revealed the unsatisfactory level of protection for NATO networks, they also were un mal pour un bien. They created a dynamic that led the Alliance to ensure rapid improvement of its cyber defence policy and take an active role in cyber threat management.

Many steps have been taken to improve the Alliance's capabilities following the attacks. In the first few months of 2008, a new cyber defence policy was presented to Allies and endorsed by Heads of State and Government at the 2008 Bucharest Summit. This new policy set up the Cyber Defence Management Authority (CDMA), responsible for *"initiating and coordinating immediate and effective cyber defence action where appropriate"*.[12] The CDMA – then superseded by the Cyber Defence Management Board (CMDB) – was established as the central command for the technical, political, and information-sharing activities of the Allies, as well as for directing and managing existing cyber defence entities. The Authority rapidly developed a concept of operations, planned the first cyber defence simulation exercises, and endorsed several policies on cooperation with partners or legal issues.

At the 2009 Strasbourg/Kehl NATO Summit, officials decided to accelerate the acquisition of cyber defence capabilities so as to make cyber defence an integral part of NATO exercises, while maintaining political consultation on the different legal issues. When the Group of Experts chaired by Madeleine K. Albright [13] recommended that cyber defence be an important element of the 2010 NATO Strategic Concept, NATO officials agreed to develop a revised Policy on Cyber Defence with a view to protecting the Alliance more effectively.

The latest Policy was approved in June 2011, along with an Action Plan. NATO's principal focus is now the protection of its own information and communication systems, to be achieved by enhancing Alliance capabilities. The main objective is to implement a *"coordinated approach to cyber defence that encompasses planning and capability development aspects in addition to response mechanisms"*.[14] The NATO Defence Planning Process (NDPP) will guide integration of cyber defence considerations into national defence frameworks and structures; the Alliance is currently identifying its critical dependencies on the Allies' national communication and information networks, in order to develop minimum security requirements and to bring its networks under centralized protection based on the principles of prevention, resilience, and non-duplication. Cyber defence governance is now established within the Alliance, and the different agencies have been given specific responsibilities to improve the protection of NATO's information infrastructure.

The successive policy revisions have addressed the short-term cyber security issues NATO needed to deal with as part of its overall cyber defence strategy. The resulting new operational capabilities will help strengthen defence and drastically reduce existing vulnerabilities. Moreover, the clarified procedures within the Alliance's chain of command will allow rapid and efficient response in the event of a cyber crisis by providing coordinated technical response, information-sharing amongst NATO's agencies, and political action if needed. Alongside internal security improvements, the Policy on Cyber Defence provides clear guidance regarding the scope of action of the Alliance's cyber defence agencies: while the Allies bear responsibility for the protection and security of their information and communication systems, NATO will provide assistance to them upon request. In this way national assets can be protected by developing high security standards where national and NATO networks interconnect, and by dispatch of Red Response Teams (RRT) in the event of a cyber crisis. Addressing these issues was the first stage in the implementation of the Alliance's cyber defence strategy.

Recognizing the transnational nature of cyber threats, the Alliance has also started to dialogue with outside partners (international organizations, the private sector, academics) in order to promote complementary solutions and avoid needless overlaps. Collaboration with international partners will help the Alliance address key technical, legal or theoretical issues which are outside NATO's area of competence but crucial to the development of a comprehensive strategy. For example, since the private sector creates, manages and owns most of the technologies that constitute the backbone of a nation's cyber power, industry must be involved in network securitization so that future cyber threats can be analyzed and predicted.

The objective of the Policy on Cyber Defence is to implement a coordinated approach, encompassing response mechanisms to cyber attacks along with the development of long-term aspects of cyber defence such as planning, capability development, and Research & Development (R&D). In 2008 the Alliance established the Tallinn-based NATO Cooperative Cyber Defence Center of Excellence (CCD CoE), to enhance NATO cyber defence capability and cooperation by creating a dedicated

[11] The literature on cyber deterrence is important, but the work of M. Libicki provides an excellent basis of the challenges: M. Libicki, *"Cyberdeterrence and Cyberwar"*, RAND Corp., 2009.
[12] Sverre Myrli, Rapporteur, *"NATO and Cyber Defence"*, report 173 DSCFC 09 E Bis.
[13] See the official report of the NATO Group of Experts chaired by Madeleine K. Albright, *"NATO 2020: Assured Security; Dynamic Engagement"*, available at http://www.nato.int/strategic-concept/expertsreport.pdf.
[14] See *"The NATO Policy on Cyber Defence"*, available at www.nato.int.

research pole. The centre's activities focus on key cyber defence issues (legal framewok, policy, concepts and strategy). Several international conferences and workshops have been organized, publications have been issued, and a comprehensive "Manual on International Law Applicable to Cyber Warfare" is to be published in the second half of 2012. Despite the very high standard of its work, the CCD CoE nevertheless remains a modest structure which has only an advisory function for NATO members and does not actually intervene in the event of cyber attacks against the Alliance.

Overall, NATO's successive cyber defence policies have focused on all levels of a comprehensive cyber strategy. At the operational level, the establishment of the CDMB and the development of the NCIRC combined to bring security improvements. At the strategic level, the 2011 Policy clearly defines NATO and national responsibilities in protecting networks and in responding to cyber attacks; the Action Plan details practical steps to implement both inter-agency coordination within the Alliance and collaboration with Allies. At the doctrinal level, the establishment of the NATO CCD CoE and dialogue with international partners give the necessary impulse to long-term research work that will address key issues outside NATO's areas of competence. However, despite NATO's efforts, collective cyber defence still has many grey areas and faces multiple constraints.

The remaining shortcomings and uncertainties

The issues surrounding the development of cyber capabilities make this one of the most important challenges NATO currently faces: the Alliance must implement collective defence mechanisms against a new type of threat, and in times of severe financial constraint.

In addition, the potential for NATO to play a bigger role in defending the information infrastructure by implementing a credible cyber deterrence strategy is limited by political disagreements on the conditions and circumstances which would prompt any collective response to cyber attacks. NATO is currently focusing on implementation of an active cyber defence strategy, with improved security standards and requirements. While improved defence will to a certain extent dissuade potential aggressors, this is of course not enough for it to be considered as a real deterrent in its own right. For actual cyber deterrence (by punishment), there is the prerequisite that Article 5 of the North Atlantic Treaty be considered applicable to cyber attacks. In this respect the NATO Policy on Cyber Defence reiterates that any collective defence response is subject to political decisions of the North Atlantic Council, and that NATO will remain flexible on how it will respond to cyber attacks. This flexibility can be interpreted in two ways: as a deliberate position calculated to keep potential aggressors in a state of uncertainty regarding the consequences they might face, or as a sign that the Alliance has difficulty in achieving consensus on a firm response option. In the first case the aggressor might indeed be dissuaded from attacking NATO's information networks by fear of an unforeseeable retaliation. Unfortunately, however, leaving response options unspecified creates a degree of ambiguity which might be perceived as reflecting political disagreements among the Allies on when and how NATO should intervene. If this were indeed the case, it might actually give an adversary good reason to favour cyber attacks over other forms of action against the Alliance's – or the individual Allies'– critical infrastructure. In other words, the rationale for a cyber attack would be that political and conceptual divergences within NATO might delay the consensus required to trigger a collective response. Here, an interesting historical parallel is often drawn with the ambiguity regarding NATO's nuclear deterrence in Europe during the Cold War: the point made by some analysts is that the experience of nuclear deterrence as practised by NATO and other actors can be usefully applied to the cyber domain, insofar as nuclear deterrence doctrine prevented nuclear conflicts. Unfortunately, nuclear and cyber deterrence differ significantly in both technical and strategic terms. Attackers might thus interpret the perpetuation of ambiguity in NATO's nuclear and cyber retaliation posture as additional proof not only of political disagreements, but even of strategic misunderstanding.

Such an interpretation must unfortunately be taken seriously. Cyber attacks can take various forms, depending on their objectives and techniques – ranging from espionage, organized crime and disruption to outright destruction. Determining which category a specific type of attack falls into will largely depend on legal and political considerations at the national level. Interpretations might thus vary from one country to another, to the extent that a given action might be considered an act of war by one member state but not by another. This severely jeopardizes the political consensus required to initiate collective defence measures. The resulting difficulty in defining a threshold for collective response and an appropriate form of retaliation might in turn lead to a considerable weakening of NATO's strategic credibility in cyber defence.

Added to the issue of political disagreement is the changing nature of the threat. The information infrastructure is very complex, and the integration of new technologies into existing networks creates vulnerabilities for which there is no precedent. Today, NATO faces direct cyber attacks whose aims vary considerably – to discover entry points into networks, to damage systems, steal data, or implant malware. Some of the attacks are politically motivated and target the "reputational integrity" of the Alliance by publicly exposing the weaknesses of the networks.[15] More recently, a new form of threat is posed by large, complex, highly sophisticated malware programmes with an impressive array of components and functions exploiting multiple vulnerabilities of the host system. The Stuxnet malware is an example: discovered in 2010, it targeted industrial control systems to sabotage

[15] J. Shea, in a Defence Management Journal interview, November 2011, accessible at http://www.defencemanagement.com/feature_story.asp?id=18166.

centrifuges at Natanz and thus delay Iran's uranium enrichment programme. The sophistication of this malware led many computer security specialists to believe that it had been state-sponsored and engineered by a team of experts. Even though NATO has not yet faced such threats, future aggressors are likely to develop attacks of this kind. The constantly evolving nature of cyberspace and of the related threats will eventually challenge the Alliance's capabilities and put its response mechanisms to the test, even if the NCIRC permanently monitors a wide range of existing threats in preparation for future attacks.

At the time of writing the Allies are preparing to discuss an extensive agenda of key issues during the forthcoming Chicago Summit. At the same time, the United States Department of Defense (DoD) has recently presented its Defense Strategic Guidance outlining defence priorities up to the year 2020. These include enhanced US presence in the Asia-Pacific and Middle-East regions, and an increased focus on technologies to protect the national interest and conduct the most important missions. [16] The United States wishes to rebalance its position in Europe in accordance with the evolution of the regional security situation, encouraging Allies to implement the "Smart Defence" concept developed by Secretary General Anders F. Rasmussen in order to meet new security challenges while reducing defence expenditure. In this scenario, the evolution of cyber defence within NATO remains uncertain: if "leading from behind" becomes the established pattern for the United States, it might reconsider its financial contribution and the development of new cyber defence capabilities would obviously be affected. On the other hand, despite the $487 billion cut in the American defence budget, the White House and the DoD will continue to increase investments in technology, which includes cyber security and defence. According to the recent Defense Strategic Guidance, *"cyber is one of the few areas in which we actually increased our investments, including in both offensive and defensive capabilities"*.[17] The United States has clearly identified cyberspace operations as among the most important challenges of the future international security environment, and wants to further develop its cyber capacities in order to maintain its technological advantage over potential adversaries outside the NATO arena. To what extent will US investments in cyber capabilities ensure protection of NATO's information infrastructure? The United States can decide either to be the leading actor in cyber defence and improve the security of the Alliance's networks by sharing its knowledge and skills, or to develop its national capabilities and help NATO as and when needed by sharing specific capabilities that the Alliance has for financial or strategic reasons not developed.

All in all, cyber defence in NATO still faces many important challenges. The key issue, then, is to define the implications for the Alliance so that recommendations can be made as to how the remaining questi ons can be addressed in key areas.

Implications for NATO

To develop its cyber capabilities and implement a policy that will not only address existing issues and operational needs but also ensure long-term planning, NATO should focus on the priorities outlined below.

Concentrate on core activities.

- The Alliance should pursue the implementation of the 2011 Policy to strengthen its basic capabilities: incident response, coordination and cooperation (not only among Allies but also between NATO and Allies), and resilience of networks. The Memoranda of Understanding signed within the overall setting of current cyber defence arrangements define a framework to facilitate and enhance consultation mechanisms, early warning and situational awareness among Allies. NATO needs to ensure this framework is correctly implemented so as to create a dynamic information-sharing environment. Considering the vast array of cyber threats and the number of networks to protect, coordination between the cyber defence agencies of NATO and the individual Allies is a prerequisite to prevention of redundancies and improvement of response to attacks. Sharing information on specific situations will speed up response processes, and ultimately contribute to the success of defence coordination.

- The Alliance should also expand Research & Development on cyber defence. NATO provides a formal structure that allows member states to collectively discuss and tackle cyber defence-related issues at the operational, strategic and political levels. In addition, having a NATO Centre of Excellence dedicated to the cyber domain provides an essential basis for comprehensive review and analysis of specific issues in key areas. This helps the Alliance understand the evolution of the cyber environment and identify the strategic issues involved, underlining the importance of continuing investment in research and capability development.

- NATO should multiply simulation exercises to cover the different crisis situations involving a cyber element. It is necessary to "stress-test" the networks as in the 2011 Cyber Coalition Exercise, to appraise vulnerabilities, crisis-management failures and the implementation of decision-making procedures. Simulation exercises should cover attacks at the operational (a single cyber attack), tactical (a cyber attack combined with other forms of aggression), or strategic (simultaneous cyber attacks) level. They should also envisage every possible target (IT on battlefields, NATO's internal networks, Allies' national networks), technique (from the simplest to the most complex), and scenario.

[16] US Department of Defense, "Sustaining U.S. Global Leadership: Priorities for the 21st Century Defense", January 2012.
[17] US Department of Defense, "Defense Budget, Priorities and Choices", January 2012.

Focus on deterrence by denial while discussing deterrence by punishment.

The Alliance should concentrate on enhancing its defence capabilities and response procedures, properly implementing the Policy on Cyber Defence so as to dissuade attackers and deny them an objective. It has started to develop a robust defence system with improved security standards, focusing on prevention, resilience, and non-redundancy. This active defence will allow the NCIRC to reduce vulnerabilities in NATO's networks, patching current weak links while anticipating future attacks. As a whole, these elements afford a valid deterrence by denial strategy. Hence the importance of implementing the Policy on Cyber Defence: with better information-sharing and coordination between NATO and Allies, responses to cyber attacks will be improved, and overall defence strategy will be more efficient.

On the other hand, several elements may contribute to deterrence by punishment as a complement to deterrence by denial. Even if NATO remains ambiguous on how it will retaliate to a crisis involving a cyber element, the Allies have made it clear that they will not hesitate to invoke Article 4 or Article 5 if necessary. Last year, the United States issued the strong statement that *"[w]hen warranted, we [the United States] will respond to hostile acts in cyberspace as we would to any other threat to our country. All states possess an inherent right to self-defense, and we reserve the right to use all necessary means – diplomatic, informational, military, and economic – to defend our Nation, our Allies, our partners, and our interests",*[18] implying that a major cyber attack threatening US or NATO interests could trigger offensive cyber operations or kinetic retaliation. Though NATO does not have an offensive cyber capability, some Allies have developed national capabilities that could support NATO operations in a retaliation scenario. Despite the issues that continue to limit adoption of a formal political position on cyber deterrence by punishment, these elements can serve as a basis to discuss a move in this direction.

Strengthen collaboration with the private sector and international partners to better address cyber threats.

Establishing strong and durable partnerships with the private sector will help NATO facilitate the development and acquisition of appropriate cyber capabilities, as well as benefit from the expertise, knowledge, and procedures of specialist companies.

NATO has initiated such dialogue with its industrial partners in the framework of Trans-Atlantic Defence Technological and Industrial Cooperation (TADIC), as part of the Smart Defence concept. Collaboration with the cyber industry is required for a number of purposes: to better identify the cyber security needs of NATO at every technological level (from physical elements such as wires to data encryption); to define appropriate security and resilience standards; and to develop cost-effective solutions and adaptive capabilities consistent with the sharing and pooling objective defined in the Smart Defence concept. There are also private actors outside the cyber industry with strong cyber capabilities that might help meet NATO's defence needs. These actors have developed defensive best practices, response procedures and situational awareness which NATO could learn from. The Alliance should create a setting like ACT's Framework for Collaborative Interaction (FFCI), for sharing of information, expertise and knowledge. This would help build a relationship of trust which would make for closer collaboration and better cyber security.

International partners are essential actors of NATO's cyber defence. NATO stated that it would "*tailor its international engagement based on shared values and common approaches"*, to establish complementarity and avoid any needless overlaps in procedures. NATO should develop bilateral arrangements with its partners and with other international organizations, focusing on information-sharing, exchange of best practices, and judicial agreements. In doing so, the Alliance would improve situational awareness and benefit from the specific competence of other actors: the European Union would have the legal capacity to ensure application of security and resilience standards to vital national infrastructure, while Interpol procedures could serve as a blueprint framework for international investigation and prosecution. In this perspective, NATO could explore existing procedures and use the mechanisms implemented by its international partners so as to strengthen its cyber defence capabilities.

[18] Department of Defense Cyberspace Policy Report, A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934, November 2011.

Conclusion

NATO's cyber defence policy has changed beyond recognition since the time of the Estonian cyber attacks. The Alliance has learned the lesson, improving both its response capacities and its policy procedures. Despite some persistent issues yet to be addressed, the existing law and defence mechanisms are generally sufficient to protect NATO's networks and provide assistance to Allies when needed. NATO has established a framework between Allies' national cyber defence authorities and its own cyber defence agencies, for the improvement of information-sharing and the coordination of responses. In current circumstances, the Policy on Cyber Defence provides the Alliance with the necessary guidance to respond to cyber attacks, but the success of this policy lies in its implementation. NATO must therefore ensure that Allies and partners follow its cyber agenda. Cyber threats are a permanent challenge for the Alliance's security, requiring strong commitment and a flexible response.