ACT Workshop Report
NATO in the Cyber Commons
October 19, 2010
Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia

Executive summary

This workshop constitutes the fifth in a project of seven meetings organized by Allied Command Transformation on "Global Commons Strategic Issues". The goal of Tallinn's workshop was to focus on NATO's challenges in the cyber commons. The workshop sought to identify the vulnerabilities affecting NATO's assured access to the cyber space, as well as make recommendations for NATO's way ahead in developing relevant shaping policies and capabilities.

Secure access to the cyber space is still an immature discipline and so NATO should keep vigilant. The cyber commons is the only man-made of the commons as all the assets have a physical location and belong to someone. The protection of the cyber commons requires a collective effort through the consequent cooperation between public and private entities. Every state should collaborate by protecting its portion of the domain and avoid offenses which originate from its territory.

The main challenge with regard to a cyber attack is the ability to attribute the offense. Attribution will continue to represent a huge complication, sometimes close to insolvable, as the complexity needed for tracking down such actions at times exceeds the basic foundations upon which the cyber commons rely on. Extended collaboration among NATO and its partners, as well as the private sector, is the best possible approach to fight against cyber offenses.

Dominating the battle of the cyber space narrative is essential to NATO. The Alliance should seek to deny the adversaries their ability to propagate their offensive messages. NATO has been quick to provide responses to the new paradigm on cyber security threats and maintaining permanent awareness. The imminent approval of a new Allied Strategic Concept will provide a timely opportunity to review the current NATO Cyber Defence Policy and increase the Alliance's cyber level of ambition.

Cyber space as a global domain

The cyber domain could be considered as one of the global commons as it consists in an international space that is usable by everyone. However, some participants believe that the global community will not consider cyber space as an independent global commons domain because all assets involved have an owner.

There is a bit of misconception when people talk about the borderless feature of the cyber space, particularly in the internet. There are plenty of places where internet traffic could be absolutely controlled and stopped by local authorities (Burma for example). In fact, to defend and respond through cyber space it is essential to monitor the behaviours and activities in the networks.

Some participants exclude the isolated military secure networks from the global commons. To be considered in the global commons one network has to be available, connected to

internet and open. In fact the military networks are interconnected by using the same assets as civilian networks with the risk that when a line or a server is jammed or down all services hosted are stopped, military and civilian. An attack could be launched against the network of the civilian enterprise that control and monitor lines, switches or other essential assets. Therefore, all NATO systems could be affected by the growing criminal cyber activity in this global commons.

Some participants consider that the cyber domain may develop in a similar fashion to that of the air space domain, to include the dominance by certain national powers and the dual use (civil-military) of the domain. One indication that this may be the case is the fact that many of the best expertise are being recruited by the intelligence agencies from the engineering universities with the intention of obtaining the best talent in the cyber arena. Thus, NATO should be vigilant to the emergence of potential cyber powers.

Cyber vulnerabilities

Due to its dynamic, asymmetric and polymorphic structure, many consider the cyber domain to be a kind of “cyber Swiss army knife”. Cyber threats are very flexible and agile and will usually be launched from multiple distinct locations. In this construct all computers are potential weaponry platforms when infected by botnets or performing as zombie PCs. Therefore, responses should be flexible and agile as well, which requires more time and greater expense invested. Most share the view that there are numerous ways to mitigate a threat, but there is not a single way to stop every attack. As the language of the internet is currently changing (from protocol IPV 4 to IPV 6) cyber stakeholders should anticipate and take this opportunity to increase security and reduce vulnerabilities.

Cyber attackers will use a variety of methods such as espionage, propaganda, exploit vulnerabilities (Denial-of-Services), modify existing data, and even infrastructure manipulation. Experts think that one of cyber defence’s basic concepts should be to establish the defence in depth, across as many layers as possible. The focus should be to keep the defences at the server level through a layered security and layered network design. Interim network operators will inevitably be requested to intervene to protect their customers or at least to protect the server itself.

Monitoring abnormal network behaviours is essential to understanding what is happening and to reduce vulnerability as soon as possible. As attackers spend time observing your networks and communications before attacking, there is room to identify irregular performance even prior to the attack. Visibility and controlling the traffic are keys to obtaining conclusions, in particular through watching all the information leaving the network more than monitoring the information entering. However, detection and responses must be automated to be effective requiring previously achieved collaboration and preparedness.

Cyber terrorism pursues strategic effects through asymmetric means. The use of high technology assets by terrorists poses a credible threat to critical network management infrastructure. Such an attack could have disastrous effects on the global economy by shutting down cyber systems which run our financial, transportation and communication networks.

Inadequacy of existing cyber defences

Technology evolves rapidly permitting the emergence of new vulnerabilities before cyber defences and laws are consolidated. Therefore, cyber defence is today an immature discipline. Traditional law enforcement expertise is inadequate, and it is difficult to retain personnel with highly marketable cyber defence skills. Challenging international computer investigations are further complicated by the international nature of the internet. For example, in the case of state-sponsored computer network operations, law enforcement cooperation will be very difficult.

There is a necessity to increase the investment in computer network defence capabilities. Training personal first, providing appropriate equipment and frequently organizing cyber defence exercises afterwards, and finally enforcing the performance of the existing set of rules. Nations and organizations do not always have enough people or resources to implement all the best practices, thus additional resources should be assigned and cooperation enforced. Moreover, most infrastructure attacks are often not reported for several reasons (organizations have neither the time nor skills to analyse these attacks) and so most of the attacks are known through anecdotal reports with no validation.

National cyber space responsibility

If you analyze the cyber security by two layers of preparedness, one corresponds to the national security level (countries' responsibility) while the other to cyber warfare (UN's responsibility). Within the first, the countries are internally responsible but there is a lack of global coordination. In the latter, the UN has been unable to formulate a comprehensive cyber policy due to disagreements among three of the Security Council's Permanent Members (Russia, China and US) on concepts such as sovereignty and freedom.

It is the responsibility of each state to ensure the cleaning of the systems and assets located within its territory. Failure to do so could lead to that nation being held responsible for allowing a cyber attack to originate from assets within its territory.

Some participants believe that the consequences of a cyber attack could be resisted by our economies for a period of three days with acceptable risk. Within this period authorities would be able to make decisions and take appropriate action to respond to the attack. After this period, the consequences would become unsurvivable. Thus, the response needed to face a cyber attack would be required less immediately than the responses needed to stop another military attack such a missile aggression.

Due to the international architecture of cyber space, any incident will involve lots of IPs which must be investigated. This means that each nation must to rely on law enforcement in another nation for a successful investigation. Collaborative mechanism should be established in advance.

Acting in cyber security sometimes requires bypassing the state level and utilizing shortcuts to work directly with the users and providers in a two-track approach to share and obtain information.

NATO's concerns on cyber space

Opponents and adversaries will try to deny or disrupt NATO nations and her partner's access to the cyber commons. The methods they may employ are various, but the most dangerous would probably be data modification and the infrastructure manipulation. Data modification could make a legitimate user make an important decision based on maliciously altered information through website mutilation or a database attack to corrupt weapons, targeting or Command and Control systems. The risk for the critical infrastructure is significant as they are highly connected to internet and its control is mainly in private hands.

Mission assurance and force protection are aspects of special interest for NATO in cyber space. While sensitive information should never leave secure networks, less sensitive information is transmitted and processed within unclassified networks. However, classified and unclassified information exchange is often reliant on private sector services, over which NATO has limited direct control and situational awareness. The reliability and security of these networks is of great importance for NATO operations.

Within NATO operations, the risk is more related to the availability and integrity of services than the encryption of the information, as all the information is running along the same physical assets. For NATO, the main goal should be to identify what its critical services are and where these services are hosted (critical infrastructure). The information is separated but not always running through physically separated infrastructures. As a clear lesson identified after the Georgia campaign, countries must require strong security measures from the companies who host their essential services.

Attribution feasibility

The two biggest challenges in a cyber attack are anonymity and asymmetry. It is difficult to conduct deterrence, retaliation or prosecution if you don't know who is attacking. Intelligence services and corporations are probably doing (legally or illegally) better attribution than we all believe, at the edge of legality, to protect their systems and are probably responding with pro-active defensive measures such as contracting external companies to take down offensive networks.

The internet's puzzling architecture and the delays in the prosecution tempo permit cyber attackers a high degree of anonymity. . Smart hackers don't violate the states territorial sovereignty and will use deception and false flags extensively. They can route attacks through countries with which the victim's government has poor diplomatic relations and no law enforcement cooperation. Even successful investigations often lead only to another hacked computer and governments today face the reality of losing a cyber conflict without ever knowing the identity of their adversary.

In the cyber domain, attribution is a political decision since technical and physical attribution is not feasible in short time and is only likely if there is a full cooperation among the different actors. Across the air space you can monitor your territory and know who is using it. In the cyber space you don't have this capacity. Analysing the digital code of a cyber weapon shows you who created or modified the tools, but does not necessarily attribute the action.

A command and control centre is needed to conduct a wide and highly-coordinated cyber attack launched from disparate locations. Therefore, it would be possible to identify a link towards a specific state that performs enough ability to operate it and coordinate the attacks.

Considering the importance in achieving a proper level of deterrence, some participants support the right to retaliate accordingly to the first identifiable source of the offense. Nevertheless, it is clear that the first identifiable source of one cyber attack is probably not directly related to the aggressor itself, but is rather used as a single launching point.

Winning the battle of the narrative

It is clear that an important aspect of modern conflicts is the publicity campaign. CNN, for example, could declare a war, assign roles (aggressor, freedom fighter, terrorist, etc) and determine the winner. This cyber aspect is therefore closely tied to public relations and information operations. Dominating the battle of the narrative in cyber space is therefore very important to NATO. Cyber warfare can enable NATO to deny adversaries the ability to propagate their offensive messages.

Historically, Prime Ministers, Presidents and sovereigns liked to write the narrative of the battles because they used to have great control on the information. Today, the nature of the cyber environment makes it extremely difficult the exercise such centralized control.

A cyber attack seeks to produce the greatest damage possible, but moreover to generate a lack of trust in our systems. NATO adversaries will try to exploit any lack of trust to damage the Alliance's interests and attack its collective values.

Defining the NATO's cyber policy

To define a policy in the cyber space, some restrictions must first be considered. Technology defines what is possible; within the possible the law categorizes the permissible; and finally within the permissible the policy chooses the preferable. Thus policy problems are always workable, but prior you first must understand the technical and legal issues. Despite the lack of clear adversaries in the cyber domain, a realistic policy and strategy should be developed. NATO was very quick in providing responses to the new paradigm on cyber security threats and maintaining awareness afterwards. Some participants expressed the view that NATO initial steps in the cyber domain were remarkable, but not much action and come since then. From their perspective, there is a need to review the NATO Cyber Defence Policy and increase the Alliance's level of cyber ambition after the approval of a new NATO Strategic Concept at the Lisbon Summit.

Some believe NATO is too broad to provide clear official political guidance and can only issue flat policy statements on cyber as an important security challenge. Occasionally national interests and priorities hinder NATO's timely engagement, delaying decisions on what needs to be solved, researched, secured or procured.

Some support the Group of Experts' report on the new NATO Strategic Concept which declared that a cyber attack against one Ally could possible lead to a collective defence response. The questions of when an Article 5 is applicable to a cyber attack and when NATO should organize a cyber offensive capability remains debatable.

There is a growing percentage and importance of state sponsored activities and a wider use of cyber offensive capabilities by NATO's adversaries. So far NATO has a defensive attitude and policy. Some participants believe NATO needs to start thinking about cyber offensive policy and capabilities to build a credible deterrence and help win the battle of narrative in cyber space. NATO cyber offensive policy could include the right to use less destructive

offensive responses in very clear specific situations,, using national assets for NATO missions, and clarifying and coordinating cyber roles and tasks.

Comprehensive Approach and new partnerships to confront cyber threats

International level is the key level to respond in the cyber space. But this level is much influenced by national priorities and so there are different policy concerns inside every International Organization.

The UN has great difficulties producing constructive policy in legal terms because the lack of consensus among UN members. Moreover, several international organizations are working on cyber policy without coordination which risks wasteful overlap of resources and effort. As a result, many participants agree that UN should be complemented by EU and NATO to reach a Comprehensive Approach to the cyber security challenges.

The EU has a whole package of cyber regulations which presents an integrated approach to cyber issues by using different mechanisms from information sharing to traditional cooperation. It has a framework to support interaction among its three pillars in the cyber arena. At this moment, the official EU position is not to develop offensive capabilities.

Some participants believe that NATO has better potential and more flexibility than EU to make effective use of the comprehensive approach to cyber security due to the lack of such detailed regulations. It is also relevant to say that the Alliance tends to establish a specific cyber component for the crisis response operations, which allow it to identify many useful lessons. In the near future, the development of the projected CIMIC COE will also contribute to the Allied efforts towards a Comprehensive Approach. NATO and EU should collaborate on a comprehensive approach to cyber security since both organizations complement each other as one can influence political policies and the other national security policies.

Only a Comprehensive Approach, combining all the stakeholders, can strengthen NATO's position in the cyber commons. A Comprehensive Approach will be understood as an optimized and consolidated way of dividing responsibility and resources to counter a common security concern. NATO's article 5 is one of the relevant specialities that NATO can provide to this global effort.

The solutions to cyber defence will most likely not come from new hardware since technicians are talking about open protocols, not new ways of encryption. In a Deny-of-Service attack, increasing the bandwidth is one of the solutions, but cooperation is probably the best response. As during recent attacks, NATO perspective should be the collaboration among NATO members and partners through information sharing, traffic control, collaboration towards attribution and assistance in stopping the attacks from involved countries.

Much of the cyber experience lies within specialized companies who use to pay great attention to threats and risk calculation. Very often states lag a long way behind the commercial companies regarding the latest technology. Consequently, to preserve its services, NATO must work together with the server providers, keeping in mind that if one attack succeeds against one server all the services hosted by the attacked server will be stopped.

The challenge is who and how to lead this full-spectrum Comprehensive Approach. The leader can promote more effectiveness in collective efforts once the majority of national and international actors become conscious of the necessity.

Non-state actors' role in the cyber space

Today, transnational elements with no chain of command spontaneously band together online with the aim to influence political agendas. The challenge for national security leadership is whether such activity could upset the delicate diplomatic equilibrium. Capable cyber criminals can act as mercenaries, providing states with an easy and affordable ways to target NATO's digital infrastructure.

There are good strategic reasons to invest in cyber capabilities and obtain high returns. A skilled hacker can illegally obtain thousands of research and development data in just seconds, or eavesdrop on sensitive information and network communications. The hacking elegance lies in the fact that information may be obtained for a fraction of the cost (and risk) of any other method of information collection or manipulation strategy.

Social networks in NATO

NATO personnel want to communicate with their friends, family, and even their colleagues. NATO's own social networks could be problematic considering security incidents caused by unintentional misuse or the mixing of private issues with official business. Guidelines should be put in place to regulate the activity and avoid those interferences. The requirement is to define the policy and then to educate NATO personnel on the policy enforcement and awareness. NATO will probably never be able to compete with social networks like Facebook or Youtube.

Recommendations to NATO

Participants underlined a number of aspects that NATO can do better in its efforts to secure Alliance's military operations and to ensure future free access to the cyber space:

- Work with nations on the need to delineate national responsibilities and burden sharing among allies.
- Establish a revised cyber policy to help national policy makers produce their own strategies, facilitating a better understanding on the cyber issue. The revision could consider the inclusion of guidelines to actively respond to cyber offensives and the necessity of using offensive cyber capabilities and dedicated specialities in military units similar to electronic warfare units of yesterday and today.
- Build a credible deterrence taking into consideration that full attribution is not feasible.. Making effective and timely political decisions is part of deterrence against adversaries.
- Reinforcing personalized attention to each partner nation and organization, as well as extensive collaboration with the industry and private sector. The benefits of such cooperation should be underlined and stimulated.
- Illuminate the current NATO's Treaty article 5 wording to focus on the political interpretation more than the legal one.
- Lead the cyber coordination effort at the national level, while working with the national security authorities to develop the appropriate legal framework.

- Promote the establishment and adoption of common guidelines (such as the Cooperative Cyber Defence Centre of Excellency initiative called “10 rules”) among nations and assist countries in implementing them. Over time this set of rules could be adopted by more nations.
- Establish a mechanism to explore national best practices in cyber security, adapting them to NATO and facilitating their knowledge and implementation to the Allies.
- Promoting the collaboration to cyber crimes investigation under an appropriate international convention.
- Reinforce the level of legal automation at all levels by getting the legal advisors involved on the daily cyber discussions and operational planning processes.
- Mitigate the risk from Deny-of-Services attacks and test the systems resiliency through frequent real-life red-team exercises.
- Diversify Internet Service Providers and improve communication with providers as the best way to avoid, or at least mitigate, the so-called volumetric attacks.