Cyberspace Awareness

NATO Innovation Hub Project

Sep 2017

Intermediary Report

Background

NATO declared Cyberspace as an Operational Domain, comparable to the Air, Maritime and Land domains.

Concretely, this means that NATO needs to prepare for potential Cyber Operations.

While everyone in the west is arguably living within the cyberspace as much as within the physical space, no one knows everything about it.Even renown experts admit that they can grasp only part of it. Therefore, it was agreed to take an open, inclusive approach of the cyberspace operations debate, and to invite at the table not only experts from governments, but also from the private sector and the crowd. This is why the NATO ACT Innovation Hub was tasked to build an outside-of-the-box community to consider the cyber operation challenges. Since February 2017, experts from all backgrounds have been joining the community and sharing their insights with the NATO staff. During three months this happened through direct contacts, interviews, phone an video calls, emails and in the Innovation Hub online forums. In May, the community online interaction reached a climax through a three days workshop (23-25 May 2017). There, some 40 members of the community took the opportunity to interact live and made a step forward in providing recommendation supporting NATO's operations in cyberspace. A particular effort was made to gather a very diverse audience. Therefore one could identify, around the 40 participants (virtual) table experts from industry, academia and the crowd constituting an interesting blend of expertise in risk management, physical security, education, psychology, hacking, cyber security, military operations, strategy, law, communication …

The insights provided during those three days, added up to the inputs gathered though other means since February, produced a first set of findings and recommendations to NATO. Most of it is presented here after.

Approach

In support of the aforementioned requirements, the Innovation Hub launched in Jan 2017 the “Cyberspace Awareness” project aiming at

- building an out-of-the box community that can be leveraged in support of ACT cyber related activities;
- Collect and analyze insights from this community on cyberspace and cyberspace operations;
- Identify actions for the community to take in order to develop innovative solutions to NATO challenges in the cyberspace.

An exploration and community building phase is running until Dec 2017
An solution development phase will follow in 2018.

Objectives

By the end of 2017

- Identify and understand the main challenges NATO will face in the cyberspace and in cyber operations
- Propose innovative solutions to those challenges.
- Select solution proposals to be refined for implementation by the community in 2018

Findings

This report provides intermediary findings (as of 15 Sep 2017) derived from the analysis of all inputs provided by the Innovation Hub community The final report of the exploration phase will be provided by Dec 2017.

NATO Cyberspace Operations
10 Questions and Answers

How would a cyber attack trigger a NATO operation?
NATO nations have recognized that a cyber attack could trigger a NATO response according to the Article 5 of the Treaty[1]. But this does not provide any details on how this could happen. Even for traditional (kinetic Land, Air, or Maritime) operations, there is no rule on what triggers an Article 5 response. Invoking NATO Article 5 happened only once in history, in response to the 9/11 attacks. This allied response to a terrorist attack had not been predicted or planned, there was no pre-existing rule stating what kind of terror attack would trigger the Article 5. It is only in the aftermath of the events that understanding was gained about the response process. However, no rule has been written that would apply to future similar attack. It is safe to say that the same is likely to apply to cyber attacks. No rule will be written. It is only when one nation under cyber attack would call for an Article 5 response and when the other Allies agree to launch a common response, that we will be able to understand how a cyber attack can trigger a NATO Article 5 operation.

Should Cyber Operations been defined as Offense - Defense or else?
This question has been only partially addressed so far. The paradigm of Offensive-Defensive Operations does not necessarily apply to cyber operations. In cyber operations it will be difficult to draw a line between offensive and defensive actions, and though, it might be helpful to define them under a framework more flexible than a dichotomy. Such framework is still to be defined.

The fact that there is no clear boundaries between offense and defense could, arguably, also apply to operations in other domains. As a consequence, whatever the framework chosen to conceptualize the cyber

[1] http://www.nato.int/nato_static_fl2014/assets/pdf/stock_publications/20120822_nato_treaty_en_light_2009.pdf

operations, it might well be decided to define them also in terms of offense-defense for some practical reasons.

What are the interactions between cyberspace and the other domains (Air, Land, Maritime) from a supported/supporting perspective?

All cyber assets need to be protected. While some protection activities and capabilities should be centralized, there cannot be efficient defense without a decentralization of much of it down to the individual assets and their local custodians/users. This calls for Land, Maritime and Air domains that are able to autonomously ensure their own cyber defense; even if they would also benefit from overarching protection support from Cyber Forces.

But cyber operations are not limited to defense of own military assets. Hence, what is the contribution of military and NATO to cyber operations aiming at protected non military assets is still to be defined.

If Cyber Forces are developed, it is likely that they conduct operations in support of the other domains and independently of other domains too. The latter more likely to be the case for operations conducted within the cyberspace only (without kinetic footprint). Coordination between domain components should be conducted within the framework of existing operational command and control processes. The way Information operations are coordinated across the three physical domains could serve as an example.

What Capabilities does NATO need to develop?

The need for capabilities specialized in cyber aspects is unanimously recognized. The various disciplines of cyber, that encompass much more than just security, call for a cohort of specialized staff in support of cyber operations. The personality of those experts, who might not feel comfortable within a hierarchical structure, together with the way cyber operations would be managed (high speed, abstraction, …) call for an organization and processes that are different from those of traditional armed forces. This would justify the creation of specialized cyber forces. The way in which Special Operation Forces are based on different structure, processes, mindset and people could serve as an example of a successful way to develop Cyber Forces based on a non-traditional model.

The main advantage of a Cyber Force would be not to be bound to rules, processes and attitudes fitting other type of forces.

However, an inconvenient of developing dedicated Cyber Forces is the risk of excluding other forces from the cyber operations. As often stressed during the project, since all capabilities and personnel are deeply cyber dependent, cyber security and operations are everyone's and every force's concern. It would be counter-productive if, because of the existence of Cyber Forces, other forces would not achieve effectiveness in cyber operations. This might happen, for example, if other forces would not feel responsible for the cyber aspects, or would not be able to allocate enough resources to their own cyber capabilities.

The known case of Special Operation Forces and General Purpose Forces seems to show that, on one hand, it is totally manageable to develop Cyber Forces while keeping General Purpose Forces able to operate in cyberspace; but also that it would require vigilance to avoid that cyber operations would not drift towards becoming a "Cyber Forces-only" ability.

Other innovative capability solutions should not be discarded but further explored, such as crowdsourced and outsourced cyber operational capabilities.

NATO needs the capability to understand the cyberspace and monitor it; educate and train its personnel; design and acquire relevant assets; and finally command and control defense activities conducted in cyberspace. Because the leaders in cyberspace knowledge and operations reside within the private sector, developing relevant NATO cyber capabilities implies partnering with them. In addition, because there are no clear boundaries within the cyberspace, and side effects of cyber actions are difficult to predict, NATO defensive cyber operations are unlikely to happen in isolation, but would need to be, at least, coordinated with other relevant entities of the cyberspace. So, the first thing to develop is probably the capability to partner with external actors in a very comprehensive way, in a sort of Comprehensive Approach to the cyberspace. Then, leveraging those partnerships, NATO would develop the capability to monitor the cyberspace. The goal being to understand it and follow its permanent evolutions, identify potential threats and also opportunities. The monitoring capability should also include the capability to assess and help improve NATO Nations cyber assets' security.

When developing cyber defense capabilities, it will be necessary to ensure that processes, people and technologies are optimally combined in order to achieve the expected effects.

The most important element of cyber capabilities are the people. Therefore, a cyber approach to personnel management should focus on recruiting and retaining expert cyber staff; educating and training decision makers in priority and all other personnel for cyber operations and cyber security.

What roles for NATO command structure and what roles for NATO nations?

As it applies to other domains, in cyberspace nations should possess their own capabilities and be responsible of their own defense, the role of NATO being to cover capabilities over and beyond what nations can do. This idea is concretized within the NATO Cyber Defence Pledge. It needs now to translate into capabilities.

Besides protecting the NATO Command Structure[2] (NCS) assets in the cyberspace, NATO's role should focus on providing cyber command and control capabilities allowing efficient information sharing and cyber operation coordination between allies. The functions of standards setting and assessment of the Alliance cyber capabilities should also reside with the NCS.

The backbone of the Situation Awareness network should as well belong with the NCS.

How could NATO maintain situational awareness of the fast evolving cyber environment?

Cyberspace nature is nothing like other domains. Understanding it and keeping up with its continuous and fast evolution requires the ability to

[2] NATO has a permanent, integrated military command structure where military and civilian personnel from all member states work together. It is called the NATO Command Structure (NCS) Unlike those of the NATO Force Structure, the NCS assets don't belong to a specific nation but to all the NATO nations.

adapt or change one’s mental model frequently. Developing this ability is likely to require specific education, training and cultural change among the military.

In addition, military and other governmental entities are not the most important players in the cyberspace. As already stated, knowledge of the cyberspace resides among private actors. It is through partnerships that the needed situational awareness should be achieved. Given its size and decentralized nature, understanding and monitoring of the cyberspace should be better achieved through a network including as many nodes as possible. Emphasizing the comprehensive approach needed for efficient cyber capabilities, NATO cyber situation awareness would benefit from a large open network welcoming anyone willing to help building the common cyberspace picture. This network should include state and non-state actors, entities and individuals. All NATO entities would also be part of the network. Interactions would be regulated through processes and technologies ensuring information validation and trust.

Such network has been already somewhat conceptualized and blockchain is a promising technology that could support it. A prototype of this might be developed as part of the project.

Another element of this capability are the experts in charge of analyzing, translating and presenting the cyber common operational picture to the decision makers. This element might include the Cyber Advisor to the Commander function. Its model could be very similar to what is already used for non-cyber situational awareness and Common Operational Picture.

In support of Cyber operations, the Cyber Situational Awareness process should provide the commander not only with potential threat awareness, but also with cyber opportunities awareness.

What is the role of artificial intelligence and autonomous systems in cyber operations?

Bots (cyber autonomous systems) are omnipresent. For good or bad reasons, millions of them are crawling the cyberspace in search for the opportunity to carry on the task they have been designed for. With the rise of the Artificial Intelligence, those bots will be more and more capable of adapting their ways to the environment, become more efficient and more dangerous as well.

History shows that all technology comes with some risks. It can be inadvertently misused, and it can also be abused. Because of the specificities of the cyberspace (speed and outreach) any AI mishap could have tremendous effects. It seems wise not to grant damaging capabilities to bots, and limit the realm of AI application to peaceful, passive activities. But if we can enforce this rule to ourselves, there is no doubt that some adversaries or less ethical actors would not hesitate to launch autonomous aggressive systems in the cyberspace.

This might result in a scenario in which NATO would be facing hostile autonomous cyber systems while not possessing any..

What is the need for education in support of cyber operations?

Humans are a very important element in the cyberspace awareness discussion. It is often said that the personnel is the most important aspect to take care of, or even the weakest part of the system. From one side, everyone one must be aware of the cyber risks and adopt safe behaviors while in the cyberspace. But when it comes to Cyberspace Operations, it is paramount for decision maker to have a thorough awareness of the cyber situation, risks and opportunities alike. Bringing the personnel to the needed level of knowledge and skills is a demanding endeavor that requires significant adjustments to military, government, and even public education.

Last but not least, NATO has to be able to leverage cyber experts. While some of them could or should be military, many of them should also be recruited outside of the military for their expertise build in the private sector.

Should NATO develop specific partnerships in support of cyberspace operations?

Real expertise in cyber matters resides within the private sector. It is unlikely that the military would become autonomous in the cyberspace soon if ever. As a consequence, it is paramount for NATO and nations' military to seal partnerships with relevant actors of the cyberspace. Such partnerships should involve the main cyber industry and the cyber networks physical component custodian industry. Smaller companies and unaffiliated individual experts could also provide NATO with significant help in monitoring cyberspace, and in developing adaptive and innovative solutions to the always evolving cyberspace challenges.

How should rules of engagements be updated to account for the recognition of cyberspace as an operational domain?

The general principles for the Rules Of Engagements (ROE) in other domain also apply to the cyberspace. In some cases, developing cyber ROEs could be as easy as developing traditional ROE, i.e. cyber protection of critical physical military assets. But in many cases it is expected to be difficult. The difficulty to attribute hostile activities and to foresee side effects of friendly actions are two reasons for this.

Non-cyber ROE are directly linked to legal concepts such as self-defense. When national lawyers have clarified and agreed on concepts such as cyber self-defense or cyber private property it might be easier to leverage those for the development of military cyber ROEs. As a consequence, the question of cyber ROE should be first tackled through a close collaboration between cyber experts and lawyers. It is also accepted that, like for other domains, there should be a set of general/permanent cyber ROEs that would be complemented with situation or mission specific cyber ROEs when possible.

Way Ahead

To properly address the whole spectrum of cyber implications on NATO and defense activities, it is paramount to bring an eclectic community around the table. A cyber experts-only community would not be able to fully understand the impact of their field of expertise on other domains. Therefore, the project stakeholders will continue to broaden the community and expand it towards as many fields of expertise as possible.
it has been identified that one of the priority objectives for this project is to develop a cyber platform through which an open community could safely exchange cyber related information and build trust among its members.
A workshop to address this topic will be organized on 10-11 Oct at Norfolk State University, and online.
information and registration at https://innovationhub-act.org/content/cyberspace-workshop-10-11-oct-17

The exploration phase of the project will continue until Dec 2017 through interactions on the IH forums, the social media, expert interviews and live online workshops.

By December, recommendations, including solution proposals to be further developed, will be provided to NATO and the other \participants.
The solution development phase will start in 2018, aiming at designing and implementing innovative solutions to identified challenges.

Trust & Information Sharing in Cyberspace

Human Behavior & Blockchain

Online and Onsite Workshop

10-11 Oct 2017 - Norfolk State University

Information and Registration at
InnovationHub-act.org
mahoppa@nsu.edu