The organisation of cyber defence within NATO

BRENNUS 4.0

le capitaine Frédéric Segonne, officier stagiaire à l'EMSST (cycle académique 2018-2019)

Published on 29/03/2020

Sciences & technologies

While cyber defence is nowadays at the heart of concerns both at the state level and within international organisations, awareness of the importance of cyber threats is relatively recent. Like the majority of its nations, NATO has had to develop a cyber defence policy and equip itself with the means to implement it. With the initial objective of defending its information systems, the aim of this policy is to enable the Alliance to respond in a proportionate manner or to carry out preventive attacks in cyberspace.

Cyber defence emerged on NATO's agenda starting with the 2002 Prague Summit, which called for strengthening the Alliance's capabilities against cyber attacks. Initially, it was the protection of the Alliance's own information and communication systems that mobilised the Alliance, including the development of the NATO capability ofNATO Computer Incident Response Capability (NCIRC) at Supreme Headquarters Allied Powers Europe (SHAPE) in Mons, Belgium.

Cyber attack against Estonia :

This attack comes in the wake of a diplomatic conflict with Russia, generated by the Estonian government's plan to move the Bronze Soldier from Tallinn, a monument to the glory of the Soviet army.

In addition to the riots led by a Russian-speaking minority living in the country between 26 April and 18 May 2007, Estonia was the target of a cyber-attack targeting a state structure. Taking the form of a denial of service attack, this attack successively saturated the servers of Estonian public and then private institutions (ministries, banks, media) making them inaccessible for several hours and even days.

Although there was no evidence to directly incriminate the Russian authorities, the Estonian Government quickly designated the Kremlin as responsible for the attack, considering it to be an act of war in the same way as a missile strike on the targeted structures. However, NATO jurisprudence at the time did not take such attacks into account.

The cyber-attack on Estonia in April 2007 led NATO to reassess its level of cybersecurity, but also to take a more proactive stance.s role as a defensive alliance in the event of an attack by one of its members, and thus to develop a cyber defence policy for the Alliance. Indeed, this attack, attributed to Russia, was the first to target a state structure, saturating government and then banking sites for almost three weeks and causing profound disruption to the country's infrastructure. Similar attacks against Georgia (2008) and then Ukraine (2017) confirmed the importance of this threat in the context of a hybrid conflict.

The Bucharest Summit in early 2008 approved NATO's cyber defence concept, leading to the development of its policy in this area. One of the immediate consequences, and the Alliance's most visible response to the attack on Estonia, was the creation of the NATO Cyber Defence Agency (NDA) at the end of 2008.One of the immediate consequences, and the Alliance's most visible response to the attack on Estonia, was the creation, at the initiative of eight member countries, of the Cooperative Cyber Defence Center of Excellence (CCD COE) in Tallinn, Estonia, on 14 May 2008 . The Centre's mission is to improve capabilities, cooperation and information sharing among NATO and Partner countries. It also contributes annually to the organization and conduct of the Cyber Coalition exercise. France became a full member of the WCC CCD in June 2014. Today, the centre brings together 18 members as well as 3 partners of the Alliance (see box below).

The Cyber Defence Policy and the resulting Action Plan were adopted in 2011, but the most far-reaching decision for the Alliance was taken at the Wales Summit in September 2014. Within a strengthened version of this policy, cyber defence is recognised as part of NATO's core task of collective defence, opening the possibility of an invocation of Article 5 of the Washington Treaty. It would then be up to the North Atlantic Council to decide, on a case-by-case basis, whether the circumstances for such an invocation would be met following a cyber attack.

This enhanced cyber defence policy also affirms that, for NATO, not only does international law apply in cyberspace, but also that the main task of thes main task is the defence of its networks and that it is up to each member country to develop and improve its national cyber defence capabilities, a commitment made at the 2016 Summit. Thus, through its training and education capabilities, as well as by improving and enhancing information sharing and mutual assistance, including through the annual Locked Shields exercise, NATO is contributing to strengthening the Alliance's overall resilience . The policy thus implemented also emphasises the need for the Alliance to develop its cooperation in cyber defence, both with international organisations (UN, EU, OSCE, etc.) and with the industrial world. The latter cooperative aspect has been formalised through the NATO Industry Cyber Partnership (NICP), a partnership in which member countries undertake to strengthen their ties with industry by building on existing NATO, state and industrial structures. The partnership promotes, inter alia, information-sharing activities,

exercises, training and education, as well as multinational intelligent defence projects.

At the Warsaw Summit in 2016, another historic step was taken with the recognition of cyberspace as an area of operations in which NATO must be able to defend itself as effectively as it does in the air, land and maritime environments. Historic because, for the first time in its history, NATO was adding an operational area to the three traditional areas. Cyber defence is thus fully integrated into operational planning and the conduct of Alliance operations and missions. The most notable consequence of this recognition was the announcement, in October 2018, of the creation of the Cyber Operations Centre, or CyOC. Located at SHAPE in Mons, its main objective is to provide the information necessary for situational awareness in cyberspace. It is also responsible for coordinating the efforts of the many existing and well-established elements, both within the NATO command structure and in individual member countries, to carry out Alliance operations and missions in cyberspace. As NATO does not have sufficient cyber defence capabilities of its own, the Allies agreed that sovereign capabilities would be made available to the Alliance, on a voluntary basis, for the conduct of cyber operations, as is the case with traditional means in the other three areas.

For the defence of its own networks, NATO relies on the NCIRC. Attached to the NATO Communications and Information Agency (NCIA), it protects NATO's networks.NATO's networks by providing centralized and permanent cyber defence support for all Alliance sites through its Technical Centre. However, the NCIRC's role is not limited to responding to cyber incidents. Its coordination centre is effectively responsible for coordinating cyber defence activities within NATO and with member countries.

Since its first steps in cyber defence in 2002, NATO has developed an ambitious cyber defence policy. The physical means to implement it exist and are expanding for the most recent ones. The Alliance now needs to develop the legal and diplomatic arsenal that will enable it to legitimise its action in cyberspace, but also, from a military point of view, a doctrine for operations in cyberspace that will be a valuable guidance document for NATO commanders. Subject to Allied approval, this doctrine is expected to be developed during the course of 2019.

The legal aspect is proving more complex to deal with. The Alliance's goal is to arrive at a definition of a cyber-war state that would allow it to conduct preventive operations in cyberspace if necessary.

However, it is crucial to define the threshold beyond which a malicious act is considered to be a state of armed conflict and, at the same time, NATO's response to acts that would then be considered cybercrime. In this sense, the Alliance is considering how it could respond systematically to malicious acts without triggering disproportionate conflict. The Allies' objective is therefore to develop as broad a range of responses as possible, so that they can develop measures to counter, always in accordance with international law and the principles of restraint and proportionality, any attack against them and thus deter any further cyber-malicious acts.

NATO now has the capabilities to ensure its resilience to cyber attacks against it. The Alliance continues to improve them and to develop new ones. This building must continue while addressing new threats from cyberspace. Indeed, the Alliance's resolve is

as strong in cyberspace as it is in every environment where it has interests. NATO must now show that its determination to deter aggression against its members remains and ultimately only extends to a fourth operational area.

NATO Cyber Exercises :

Every year, NATO conducts a number of different exercises that now systematically incorporate a cyber aspect. However, there are some exercises dedicated to cyber defence, the most notable of which is the Cyber Coalition, which will celebrate its 12th anniversary in 2019 . This exercise aims to improve coordination and collaboration between NATO and the Allies and enhance their capabilities to protect Allied cyberspace.

Also on an annual basis since 2010, Locked Shields, a real-time cyber defence exercise has been held at the CCD COE, during which France ranked first for its 2019 edition.

Sources

Official Communiqués of the NATO Summits in Bucharest, Lisbon, Norfolk, Warsaw, Brussels ;

Senate Information Report No. 449 of 8 July 2008;

NATO Fact Sheet of February 2018 and 2019;

"What is NATO really doing in Cyberspace?"Don Lewis, 4 February 2019;

https://www.nato.int/cps/en/natohq/topics_78170.htm?selectedLocale=fr;

https://www.nato.int/docu/review/2019/Also-in-2019/natos-role-in-cyberspace-alliance-defence/FR/index.htm;

https://ccdcoe.org/news/2019/france-wins-cyber-defence-exercise-locked-shields-2019/.

Title : le capitaine Frédéric Segonne, officier stagiaire à l'EMSST (cycle académique 2018-2019)

Author (s) : le capitaine Frédéric Segonne, officier stagiaire à l'EMSST (cycle académique 2018-2019)

Release date 18/03/2020

FIND OUT MORE