FONDATION pour la RECHERCHE STRATÉGIQUE

NATO Briefs Series N°5

Delphine Deschaux-Dutard

University Grenoble Alpes, CESICE

August 30, 2021

Is NATO ready for cyber war?

In a more and more connected world cyberspace has become the fifth battlespace. The latest Pegasus case, refereeing to a spying hardware which affected many European heads of states and government in the Summer of 2021, shows how much cyber threats are now part of the international security arena. NATO has tackled the cyber topic for over a decade. NATO's awareness towards cyber threats started raising in the late 1990s, following cyber-attacks by Serbian hackers against NATO Supreme Command's (SHAPE) website during the air bombing campaign on Serbian positions in the frame of the Kosovo war. The cyber-attacks against Estonia in 2007 and in the context of the conflict in Georgia in 2008 urged the Alliance to take this new threats seriously. NATO is today the most advanced international organisation regarding cyber defence. With a cyber command structure set up in 2008, its 2010 Strategic Concept has enabled it to lay the foundations of its vision for cyber defence. Indeed NATO frames cyber threats as a direct challenge for transatlantic and national security as stated in the 2010 Strategic Concept.

The Alliance approved its first Policy on Cyber Defence in 2008 (revised in 2011 and 2014) and established a Cyber Defence Management Authority (CDMA) in 2008 and even a Cybersecurity Operations Centre within NATO Command Structure in 2018. The Strategic Concept adopted in November 2010 in Lisbon fully acknowledges cyber defence capabilities as a necessity for the Alliance. NATO also created tools to prevent cyber-attacks and cyber offensive capabilities with a central objective: to defend the Alliance's own communications and information systems and to arouse its member states' awareness on the need to protect critical infrastructures implied in contemporary military operations.

At the NATO Summit in Wales in September 2014, the organisation crossed a new important threshold by recognizing cyber defence as part of the Alliance's core task of collective defence and therefore included cyber threats as relevant article V material. This concretely means that NATO could trigger the article V of the Washington Treaty in case of a massive cyber attack with lethal implications against one of its members. Yet such a case would raise the difficult question of the attribution of the cyberattack. Such an attribution to a specific state or state-sponsored hacker would necessitate a consensus among the member states within the North Atlantic Council, which would probably make it difficult as it tackles diplomatic strings and strategic priorities which keep diverging among the EU member

states. Indeed attribution continues to be a competence of member states until now, and not of NATO as such.

Since 2014 NATO regularly reaffirms the importance of cyber defence as one of the core tasks of the Alliance, as it has been done during the Alliance's summit in Brussels in June 2021: NATO endorsed a new Comprehensive Cyber Defence Policy supporting the three main priorities of the Alliance (collective defence, crisis management and cooperative security). The member states also agreed to commit to making use of the full range of capabilities to actively deter, defend against and counter the full spectrum of cyber threats at all times.

Aside from these policy aspects, NATO also develops a wide range of tools and capabilities in the area of cyber defence, with the aim of being able to provide assistance to its member states in case of cyber-attack. It should also be acknowledged that NATO owns its information and computer networks used in NATO military missions, whereas in the case the EU for instance, the EU depends on the members states ICT infrastructures for CSDP missions.

NATO set up a specific agency dedicated to cyber defence in 2012 at its SHAPE headquarters: the NATO Communications and Information Agency (NCI Agency), which hosts since 2016 a Cyber Security Operations Center (CyOC) dealing with around 500 cyber incidents each month and responsible for the cyber defence of NATO's information and computer infrastructures in the world and on military theatres (like in Afghanistan until August 2021 for instance). This Cyber Operation Center should be fully operational in 2023. In addition to these tools the Alliance created a Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn, which is a research and training facility dealing with cyber defence education, research and development. The main task of the Centre is to provide expertise on cyber defence, and organise cyber exercises involving both NATO Allies and partners. These tools are completed with NATO's smart defence initiatives entailing cyber defence aspects and aiming at bringing member states to cooperate to develop and maintain capabilities they could not afford to develop or alone. The Alliance develops yearly exercises under the label Cyber Coalition.

The development of NATO cyber capabilities over the last 15 years clearly shows that NATO started developing its own cyber defence culture. The organization therefore issued a Cyber Defense Pledge at the Warsaw summit in 2019 to facilitate cyber cooperation among its member states. As a follow up, France decided to host the first international conference in Paris in 2018 gathering the 29 NATO member states and the Secretary General of the Alliance to urge its allies to keep developing strategic thinking on cyber issues.

Last but not least, NATO also develops an important cooperation with the EU on cyber defence. Both organizations have enhanced their cooperation in cyber defence since their joint declaration at the Alliance summit in Warsaw in 2016. They regularly organize common training and exercises and develop information sharing in order to raise mutual. Cooperation is even more needed in a context of limited financial resources: some experts suggest using the Berlin Plus agreements in cyber defence. The EU and NATO have also concluded a technical agreement between their response teams for cyber incidents (NCIRC and CERT-EU) in February 2016 to intensify their cooperation on cyber defence. This agreement has been enforced to discuss cyber threats in the context of 2019 European elections for instance.

NATO also started a partnership with industry through the NATO Industry Cyber Partnership (NICP). More precisely the Alliance develops links with computer firms such as Microsoft, Atos, Thales, Cisco or Apple.

The panorama of NATO's cyberdefence assets shows therefore that the Alliance takes cyber threats seriously and dedicates resources and reflection to the topic. Even though NATO could not decide itself to trigger article V against a cyber aggressor, its member states have the common framework enabling them to act, should they manifest the political will to do so.

WWW.FRSTRATEGIE.ORG

4 BIS RUE DES PÂTURES 75016 PARIS TÉL : 01 43 13 77 77 FAX 01 43 13 77 78

ISSN : 2273-4643