CSS | ISSUE BRIEF

NATO: CYBERSECURITY AND CYBER COALITION

Urjasvi Ahlawat *

ABSTRACT

NATO, one of the strongest international organisation, faces innumerable dangers, where the threat to security in terms of cybersecurity is the highest. The attacks on the security bases of the NATO allies are not only increasing but are becoming more coercive and destructive. In July 2016, analysing the recent cyber-attacks which took place, the Allies realised that an equal amount of importance shall be given to the domain of cyberspace's security, and hence, they pledged to prioritize cybersecurity. NATO and its Allies rely on strong and resilient cyber defences to fulfil the Alliance's core tasks of collective defence, crisis management and cooperative security.[1] This issue brief is divided into three segments: the first segment will demonstrate the three phases of NATO concerning cybersecurity. The second segment will discuss NATO's step towards secure cybersecurity, which includes cyber coalition. The third segment will illustrate the arguments concerning the actions that can be taken by NATO as a whole and the US, the dominant ally, towards better security of the NATO cyberspace.

PHASES OF NATO AND CYBERSECURITY

Even though the cyber threats were recognised in the Prague Summit of 2002, important developments regarding cybersecurity in NATO were made in the Warsaw Summit of 2016, when cyberspace was acknowledged as the fifth domain of warfare. This recognition illustrated the ability of NATO to conduct cyber exercises and allocate resources towards the betterment of NATO's cyber defence. It further illustrated the increased importance of cybersecurity for NATO. In the Wales Summit 2014, it was agreed how cyber defence was recognized under NATO's core task of collective defence. In furtherance to the aforementioned decision, the Warsaw 2016 summit reassured NATO's defensive mandate. It will also give NATO a better framework to manage resources, skills, capabilities and coordinate decisions. This will not change NATO's mission or mandate, which is defensive. [2]

A revised Cyber Security Strategy and a blueprint for incorporating cyberspace as an operating domain were approved by the defence ministers. The aforementioned action will strengthen the willingness of the NATO Allies to work together, build capacity and exchange information. Allied leaders decided, at the Brussels Summit 2018 to set up a new Cyberspace Operations Centre as part of NATO's reinforced Command Structure. Situational understanding and coordination of NATO operational operations in cyberspace will be provided by the Centre.

[1]* ***The Author is a student at the Jindal School of International Affairs and Research Intern at the Centre for Security Studies, JSIA.***

[1] "Cyber Defence." NATO. Accessed December 28, 2020. https://www.nato.int/cyberdefence/.

[2] "NATO Cooperative Cyber Defence Centre of Excellence." *2016 8th International Conference on Cyber Conflict (CyCon)*, 2016. https://doi.org/10.1109/cycon.2016.7529417.

Assessing the performance of NATO in cybersecurity over the years, it is divided into three phases. The first phase did not emphasize on cybersecurity as it was considered as a simple 'technical challenge' which was to be tackled with by the member states individually. It was the issue of the Atlantic Alliance and its ICT partner organisations. The second phase when was when the topic [cybersecurity] became an important political issue; the process was primarily initiated during the Riga Summit and subsequently stepped-up following the cyber-attacks against Estonia. [3]The third phase focused on the time of 2016 when NATO announced cybersecurity as the domain of military operations and a domain which is of utmost priority due to not only the increase in several threats to the allies but the increased political involvement threatening the peace within the allies. Unlike the first phase, the last phase demanded collective action by the allies to defeat. The phases reflect the increased recognition of cyber threats to NATO. However, the larger argument demonstrates whether the actions taken by NATO are sufficient to counter the complex evolving cyber threats?

CYBER COALITION: NATO'S ACTION TOWARDS CYBERSECURITY

When cybersecurity was discussed in the Bucharest Summit of 2008, NATO launched the Cooperative Cyber Defence Centre of Excellence, which conducts and organises exercises and activities related to cybersecurity. All the actors, including member states, military, technical experts and decision-makers participate in these activities for the betterment of their cyber defence. Cyber-attacks are becoming more common, intense and advanced. Cyber-specific exercises are being continually updated in light of changed policy and doctrine. [4] This segment will elaborate on the actions taken by NATO to ensure the efficiency of their cyber defence, where the annual cyber coalition is of high importance as it is NATO's largest cyber defence exercise.

In 2018, the Cyber Coalition, NATO's cybersecurity exercise with more than 700 Allies, partners, and NATO members, jointly adopted the incorporation of sovereign cyber effects provided by an Ally. Apart from the aforementioned activities, NATO does conduct activities which tend to involve more robust cyber situations, such as the Crisis Management Drill (aimed at NATO Headquarters) and Trident Juncture 2018 (aimed at the entire military chain of command). In addition to this development at NATO, the Cyber Defence Commitment encourages simultaneous all-government adaptation for each ally. The Cyber Defence Pledge was made under Article 3 of the Washington Treaty, which states that "Allies will maintain and develop their individual and collective capacity to resist armed attack." NATO has a keen interest in developing the cybersecurity capability of entities outside the defence system, as it is difficult to distinguish political, political, and industrial issues completely in this space.

Concerning the Cyber Coalition 2020 (CC20) that took place from 16th November 2020 to 20th November 2020. For the first time, due to the pandemic, the event took place virtually. Since NATO's cybersecurity considers its poor decision making as a lack of effective cyber defence (which will be elaborated on in the next segment), the CC20 specifically focused on aspects including but not limited to decision making processes, collaboration capabilities and the technical and operational procedures. National Cyber Defence capabilities were also tested.

[3] Hasanov, Arif Hasan. *The Evolution of NATO'S Cybersecurity policy and Future Prospects*, 2019, 1–10.

[4] Brent, Laura. "NATO's Role in Cyberspace." NATO Review. Nato Review, February 12, 2019. https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html.

Furthermore, the exercise aims to strengthen cooperation within the cyberspace domain of NATO, boost the member states' capability to execute and implement operations.

Furthermore, guidance is also provided to NATO on its cyberspace transition. Cyber defence is a mutual defence component. Even during a pandemic such as COVID 19, CC20 demonstrates NATO's capacity to not only evolve but tackle any cyber threat, said Commander Robert Buckles (US Navy), Exercise Chief.

The CC20 also observed a similarity in NATO and the European Union's ability to protect its network against the increased cyber threats. Lessons learned from previous exercises have recognised this with greater involvement from the European Union Cyber Defence Staff. [5] Greater emphasis is being put on cyber defence being a part of collective defence, which is NATO's indication towards its severity concerning Article 5; a serious cyber threat could trigger Article 5. The way to tackle the increased cyber threats, the Cyberspace Operations Centre was introduced by NATO (within the framework of the Cyber Coalition), which is NATO's first and only cyberspace theatre component, responsible for persistent, centralised and comprehensive cyberspace situational awareness and co-ordination of the full spectrum of NATO military activity within cyberspace. [6]The goal of Cyberspace Operations Centre is to put together a cyber coalition of NATO, which also includes member states and Allied nations. Furthermore, it allows the allies to enhance their capability of the Alliance in support of NATO's key tasks to prevent, protect and fight attacks in and across cyberspace.

Thus, CC20 illustrates NATO's willingness to defend its own IT networks from cyber attacks twenty-four hours a day and exchange real-time intelligence on cyber threats with allies and partners, including the EU. The discussion and actions towards NATO's poor decision-making skills and operational flaws reflect the coherence of the CC20 as this exercise focused on the root problems of NATO's cyber defence.

FUTURE: ACTIONS TO STRENGTHEN CYBERSECURITY

As the Cyber Coalition demonstrates the actions taken by NATO, this segment will further elaborate on more aspects that can be covered in the aforementioned exercises. The core of NATO cybersecurity efforts lies at the member-state level.[7] The size and severity of today's cyber-attacks involve a new approach to political, military, and civilian responses. NATO should take a few effective steps in the organisation to establish a quick decision-making mechanism while confronting a cyber-attack. The solution towards more secure cyberspace lies in the functioning and accountability of member states; currently, no mechanism exists to ensure that the member states are adhering to the Cyber Defence Pledge taken in the Warsaw Summit of 2016. NATO can discuss and provide expertise, however, there is no apparatus to enforce that expertise on the member, and the efficiency of the cyber defence efforts depend on the implementation by the members.

[5] "Exercise Cyber Coalition 2020 Underway." shape.nato.int, 2020. https://shape.nato.int/news-archive/2020/exercise-cyber-coalition-2020-underway.

[6] "Exercise Cyber Coalition 2020 Underway." shape.nato.int, 2020. https://shape.nato.int/news-archive/2020/exercise-cyber-coalition-2020-underway.

[7] Lété, Dege , Bruno, Daiga. *NATO Cybersecurity: A Roadmap to Resilience*, 2017.

The first action can be taken concerning the decision making of NATO, which is divided into NATO as an organisation and its members. In the former aspect, the resource allocation to NATO should be increased as it will help in not only detecting and indicating hostile cyber activities but will allow better use of the civil and military intelligence units. Furthermore, the powers of the Supreme Allied Commander Europe should be increased by the North Atlantic Council, along with which the CCDCoE should increase cyber defence activities and exercises as it will increase efficiency. The focus of these exercises should be on dynamic and challenging cyber crisis-conflict situations, fast decision-making processes. Concerning the members' role, identifying and sharing information about any potential threats to any of the members should be shared; the national intelligence services should supply and exchange such information. *Allies and willing partners should continue to work on improving and updating threat assessments, and facilitating closer intelligence cooperation.*[8] Cyber challenges arrive in the form of networks and to defeat these threats involves an equally well-organized network of multinational and cross-sector collaboration. CC20 did deal with the aspect of decision making, however, as explained above, this aspect has a greater potential to secure the member states of NATO from the cyber threats.

The second factor includes the rules of engagement of the member states. NATO has not defined the actions (i.e. circumstances, conditions, degree) to be taken by other members in case of the identification of cyber threat by one of the members. If a member state faces a large-scale, crippling cyber-attack where the root of the attack can be easily attributed, it could be more apparent to cause an authorisation to use force with respect to the Article 5. However, the need to identify details such as when and how NATO must respond to day-to-day cyber intrusions that fall below the level of being viewed as a direct act of aggression is of extreme importance and more urgent. NATO strategy also leaves it possible for so many grey areas to be abused by opponents who are wise enough not to cross a line that would cause a common Alliance reaction. Lack of action in the case of Russia's unethical intervention in the Democratic National Committee's emails reflects the lack of clarity of the actions to be taken against such incidents. Without the assistance of assessment instruments that can help NATO devise a proportionate political or military response, the North Atlantic Council will also need to analyse any particular cyber-attack case by case. When more cyber policy and regulations take shape, by specifically specifying the rules of engagement in cyberspace, NATO may show political, military, and analytical leadership.

The third factor is about the consideration of offensive cybersecurity. NATO acknowledges Article 5 a potential cyber-attack trigger. The doctrine and crisis management requirements are established in the cyber policy of NATO, however, the emphasis is only on a defensive stance. As such, cyber is not regarded by the Alliance as a power generator that may be of value to member states of NATO's defence; as mentioned above, the integration of NATO and cybersecurity was only in 2008. In 2016 it was considered as an important domain; as of now, it was not considered to be important. On the contrary, Russia views aggressive cyber capability as an important part of its military strength and, in particular, as a way of compensating for its relative lack of conventional forces compared to NATO. The growth of networking, the proliferation of smartphones, cloud computing, the development of software, and other technical developments open new opportunities for attackers and compel defenders to protect a rising range of fields. The defensive strategy of NATO is not viable in the long

[8] Lété, Dege , Bruno, Daiga. *NATO Cybersecurity: A Roadmap to Resilience*, 2017.

term. There are valuable cyber capabilities worth attaining, including the ability to conduct reconnaissance and surveillance, intercept communications, or deny resources and access.[9]

THE UNITED STATES ASPECT

Being the influential and dominant member, the United States did not consider NATO or cybersecurity to be of great importance, however, the dynamics are likely to change post-2020 Presidential elections. Joe Biden, the President-elect, declared cyber threats as "one of the defining challenges of our time." He believes that in today's time, Russia and China impose a threat to NATO's security by continuously attacking the Alliance and its members. To equip with protection from the aforementioned threats, Biden under the US believes that NATO has to adopt a policy of constructive, ongoing responses to China and Russia in cyberspace to achieve its mission of deterrence and security, where great power rivalry is taking place in real-time. NATO's central focus should be on cybersecurity, for which the following three key actions are to be followed.

First, NATO should mandate that resilient cybersecurity architectures, the powers of its members and its main essential infrastructures be built and enforced by itself. Primary elements of a robust infrastructure could include the use of cloud technologies in the private sector; zero confidence architecture for successful access management; creation of stable hardware capabilities; and cyber defences increased by deep learning and artificial intelligence. To achieve this, the architecture framework suggested needs to be flexible to adapt to the rapidly developing and emerging technologies. However, the barrier arises as it is a challenge for NATO to itself build the suggested architecture. Using the NATO Defence Planning Process (NDPP), procurement processes, requirements and goals, and Allied Command Transition strategy to promote a robust research and development initiative, it should stress their necessity and require its members to do so.

NATO must agree that one size would not fit all when determining specifications for these resilient architectures. Not only will requirements differ among military, government, and critical infrastructures operators, but, as has been shown in the development of autonomous vehicles and space capabilities, there are a variety of different approaches that may prove effective.[10]

Second, NATO should conduct active cybersecurity in cooperation with its nations. Due to technological loopholes or human error, even the best exclusionary technologies in a cybersecurity resilient design may fail. As a result, even after an attacker has abused cybersecurity, the alliance requires "active cyber defences" that will create durability. These features impact only certain networks where they have been built by providers and owners and are not for offensive purposes. In its Active Cyber Defence[11], the US National Security Agency illustrates how the key elements of active defence capacities include "real-time communication,

[9] Lété, Dege , Bruno, Daiga. *NATO Cybersecurity: A Roadmap to Resilience*, 2017.

[10] "NATO Needs Continuous Responses in Cyberspace." Atlantic Council, December 9, 2020. https://www.atlanticcouncil.org/blogs/new-atlanticist/nato-needs-continuous-responses-in-cyberspace/.

[11] Active Cyber Defense (ACD). NSA/IAD, 2015. https://apps.nsa.gov/iaarchive/programs/iad-initiatives/active-cyber-defense.cfm.

sense-making analytics to understand the current state and automated decision-making to decide how to react to current state information.**''**[10]

NATO must be capable of searching for potential enemies within electronic networks vital to security as a core aspect of successful cyber defence. By removing malware and closing redundant ports, the Alliance could build highly competent specialist hunting teams to review device operations, identify irregularities, and combat intruders. NATO Standing Cybersecurity Hunt Teams should also be working with the cooperation and active collaboration of national governments and operators of infrastructure networks. These hunting teams will perform in-depth technological assessments of live networks to detect unnoticed risks, according to the US Department of Homeland Security. Standing Cybersecurity Hunt Teams will broaden the capacities of NATO's existing Cyber Rapid Response teams, which are small in size and work reactively, with an emphasis on aggressive protection.

Third, NATO should strategize a sustained intervention policy aimed at reducing Russian and Chinese interventions to undercut the cyberspace alliance. US Cyber Command developed the idea of sustained commitment, but the reasoning still extends to NATO, arising from the need to tackle the current cyber attack campaigns emanating from Russia and China. Persistent engagement includes monitoring enemies, recognising their objectives, evaluating the instruments used for attacks, and taking steps to degrade their ability to blunt current attacks or stop potential attacks. As a core aspect of its deterrence and security, the Alliance wants a sustained commitment cyber policy.

NATO should exploit its intelligence and defence preparation resources to build a framework for allies to actively control cyberattacks from Russia and China to ensure sustained participation successfully in the Alliance. NATO can collect information through its Intelligence and Security Branch, attacking allied vital assets, strategic capabilities, or democratic structures. Using this material, the Cyberspace Operations Center (CYOC) of NATO could outline ways to decrease the capacity of Russia and China to carry out such attacks. The CYOC should share its analyses with pre-designated Allies who would work with targeted countries and employ their cyber effects against the identified threats[12]. In support of NATO operations, nine NATO nations have already pledged to make those results possible. The aforementioned cyber-capable allies will be responsible, based on NATO guidelines, for persistently undermining the cyber operations of adversaries. This model will make the CYOC of NATO a strategy platform with an approach to persistent interaction around the Alliance. It will allow NATO to encourage its members to take individual or multilateral measures against hybrid cyberspace operations by adversaries.

CONCLUSION

Thus, in conclusion, several member states fail to adopt and review their national cyber-security policies, considering the promise at the Warsaw NATO Summit. As a result, NATO's attempts to develop alliance-wide cybersecurity are hampered by considerable national contradictions, and NATO's collective cyberspace defence and deterrence also reveal significant vulnerabilities against the background of a rising amount of attacks. For NATO to operationalize cyberspace as a sphere of NATO security policy and planning, the Alliance

[12] "NATO Needs Continuous Responses in Cyberspace." Atlantic Council, December 9, 2020. https://www.atlanticcouncil.org/blogs/new-atlanticist/nato-needs-continuous-responses-in-cyberspace/.

should have permission from member states to do more than just provide guidance, experience, training, or instruction. NATO should establish benchmarks and better metrics that allow a consistent assessment of the annual success of a country and should be charged annually with testing and assessing the skills of members. Cooperation with the European Union is necessary to meet this goal. NATO and the EU might work together to create minimum standards and benchmarks for cybersecurity that the European Defence Agency will then implement.