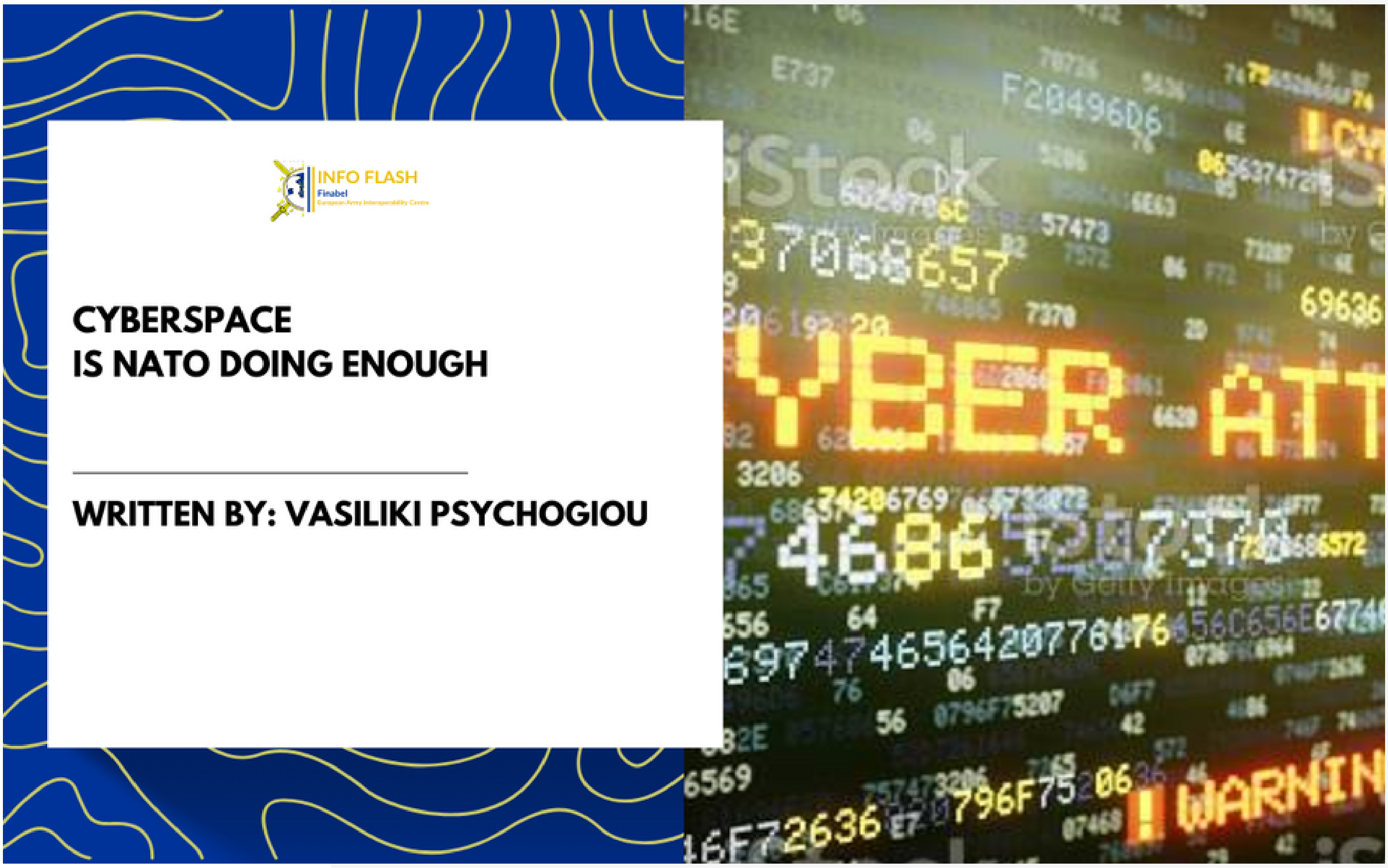
INFO FLASH
Finabel
European Army Interoperability Centre

FINABEL - THE EUROPEAN ARMY INTEROPERABILITY CENTRE

FEBRUARY 2022

CYBERSPACE:
IS NATO DOING ENOUGH


INFO FLASH
Finabel
European Army Interoperability Centre
CYBERSPACE
IS NATO DOING ENOUGH
WRITTEN BY: VASILIKI PSYCHOGIOU
CYBER ATT
WARNIN

WRITTEN BY

VASILIKI PSYCHOGIOU

Introduction

Cyberspace has become the fifth battlespace in an increasingly complex security landscape, and cyber threats have been part of the international security arena. The North Atlantic Treaty Organisation (NATO) has tackled cyber threats for over a decade. NATO's awareness towards cyber threats started rising in the late 1990s, following cyber-attacks by Serbian hackers against NATO Supreme Command's (SHAPE) website during the bombing campaign on Serbian positions as part of the response to the violence in Kosovo* in 1999. The cyber-attacks against Estonia in 2007 and in the context of the conflict in Georgia in 2008 urged the Alliance to take these 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 its 2010 Strategic Concept. The Alliance has already recorded significant performance in cybersecurity policy. Yet, the question is whether NATO is doing enough to address the complexities of cyberspace. The present paper first discusses the evolution of NATO's cybersecurity policy cornerstones. Following, it refers to key challenges that can affect the development of NATO's deterrence, defence, and security posture in cyberspace. Eventually, it provides an overall assessment of NATO's performance in cyberspace policy and further suggestions for improvement.

The Evolution of NATO's Cybersecurity Policy

NATO has taken important steps in cyber defence over the past two decades. Cyber defence was placed on its political agenda with the 2002 Prague Summit when the Allies decided to strengthen capabilities against cyber-attacks. The leaders agreed on additional protection to NATO's communications and information systems at the Riga Summit in 2006. Following the cyber-attacks against Estonia's public and private institutions in 2007, NATO approved its first Policy on Cyber Defence in 2008. The conflict between Russia and Georgia in 2008 demonstrated that cyber-attacks could become a major component of conventional warfare. Thus, NATO adopted a new Strategic Concept at the Lisbon Summit in 2010, during which the North Atlantic Council was tasked to develop an in-depth cyber defence policy and an action plan for its implementation (NATO, 2021; NATO, 2020).

In June 2011, NATO approved the second Policy on Cyber Defence. The policy aimed at coordinated cyber defence efforts among the Allies accompanied by an action plan for implementation. In April 2012, cyber defence was introduced into the NATO Defence Planning Process with the aim to prioritise cyber defence requirements. At the Chicago Summit in May 2012, the Allies agreed on centralised protection for all of NATO's networks and enhanced cyber defence capability. In July 2012, the NATO Communications and Information Agency was established as part of the reform of NATO's agencies. In February 2014, the Allies agreed to develop an enhanced cyber defence policy regarding collective defence, assistance to Allies, streamlined governance, legal considerations, and relations with industry (NATO, 2021; NATO, 2020).

* THIS DESIGNATION IS WITHOUT PREJUDICE TO POSITIONS ON STATUS, AND IS IN LINE WITH UNSCR 1244/1999 AND THE ICJ OPINION ON THE KOSOVO DECLARATION OF INDEPENDENCE – (KOSOVO*: COUNCIL PRESIDENCY AND EUROPEAN PARLIAMENT AGREE ON VISA FREE TRAVEL, THE COUNCIL OF THE EU, 2022, RETRIEVED DECEMBER 20, 2022, FROM HTTPS://WWW.CONSILIUM.EUROPA.EU/EN/PRESS/PRESS-RELEASES/2022/12/14/KOSOVO-COUNCIL-PRESIDENCY-AND-EUROPEAN-PARLIAMENT-AGREE-ON-VISA-FREE-TRAVEL/)

At the Wales Summit in September 2014, the Allies decided that cyber defence should be a core part of NATO's collective defence and subject to international law. Practically, this means that a cyber-attack can trigger the invocation of the collective defence clause under Article 5 of NATO's founding treaty. Moreover, NATO launched cooperation with the private sector on cyber security. The following NATO Industry Cyber Partnership was the practical recognition of the importance of working with industry partners to achieve cyber defence policy objectives (NATO, 2021; NATO, 2020).

In 2016 at the Warsaw Summit, the Allies recognised cyberspace as a domain of military operations. Thus, NATO must defend itself as effectively as it does in the air, on land and at sea. The Allies further pledged to enhance the cyber defences of their national networks and infrastructure through a Cyber Defence Pledge. Moreover, NATO and the EU concluded a Technical Arrangement on Cyber Defence to better equip both organisations against cyber-attacks. The Arrangement between the NCIRC and the Computer Emergency Response Team of the EU (CERT-EU) remains an important framework for exchanging information and best practices between the emergency response teams. NATO and the EU have also strengthened mutual participation in exercises, research, training, and information-sharing (NATO, 2021; NATO, 2020).

In 2017, NATO approved the updated Cyber Defence Action Plan and a roadmap to implement cyberspace as a domain of operations. The Plan allowed the Allies to work together, develop capabilities and share information. Hence, NATO and Finland signed a Political Framework Arrangement on cyber defence cooperation to improve the resilience of their networks (NATO, 2021; NATO, 2020).

At the Brussels Summit in 2018, the Allies set up a new Cyberspace Operations Centre as part of NATO's strengthened Command Structure. The Allies agreed that NATO could draw on national cyber capabilities for its missions and operations. Furthermore, they aimed at enhancing national resilience through the Cyber Defence Pledge. In 2019 a NATO guide of response tools was set out to further strengthen NATO defence against significant malicious cyber activities. The tools consist of military, political, and diplomatic means to tackle cyber threats by enhancing NATO's situational awareness in cyberspace and resilience and allowing for partnerships among the Allies (NATO, 2021; NATO, 2020).

In 2020, NATO took a further step towards coordination among the Allies. The North Atlantic Council issued a statement condemning the malicious cyber activities taking place in the context of the coronavirus pandemic. The statement expressed mutual support for the Allies dealing with malicious cyber activities in critical infrastructure such as healthcare services, hospitals, and research institutes. It called for respect for international law and norms of responsible state behaviour in cyberspace (NATO, 2021; NATO, 2020).

At the Brussels Summit in June 2021, the Allies endorsed a new Comprehensive Cyber Defence Policy. The new Policy aimed to support NATO's three core tasks of collective defence, crisis management and cooperative security, as well as its overall deterrence and defence posture. This implies that NATO must actively deter, defend against and counter the full spectrum of cyber threats at all times - peacetime, crisis and conflict- and at all levels -the political, military and technical level (NATO, 2021; NATO, 2020).

Key challenges to NATO's Deterrence, Defence, and Security Posture

NATO's primary purpose remains to operate as effectively in cyberspace as in the air, on land, and at sea and strengthen its overall deterrence and defence posture. Yet, NATO cannot achieve this goal solely through military means. All Alliance operations have some degree of reliance on civilian government or private industry, whether in the context of communications infrastructure, logistics, equipment, or host nation critical national infrastructure. Moreover, malicious cyber activity has also been attributed to actors ranging from hacktivists to state intelligence services. Although cyber-attacks remain a military challenge, they are further linked with the civilians, government, private industry and even individuals (NATO, 2021; NATO, 2020; Deschaux-Dutard, 2021; Brent, 2019).

The significant activity that takes place below the threshold of armed conflict can complicate the efforts to address malicious cyber activity. Although determining an effective response to malicious cyber activity can be quite complex, individual Allies have pursued various response strategies. For instance, some Allies have sought to use public attribution of malicious cyber activity to change behaviour. The United States has also recognised that "adversaries operate continuously below the threshold of armed conflict to weaken institutions and gain strategic advantages", and it has interacted with those who seek to exploit its vulnerabilities in cyberspace. Similarly, although NATO's Strategic Concept lays out collective defence, crisis management, and cooperative security as its three essential core tasks, it must constantly explore best ways to engage in cyberspace, as even a below-the-threshold cyber-attack can be highly disruptive and destabilising (NATO, 2021; NATO, 2020; Deschaux-Dutard, 2021; Brent, 2019).

Is NATO Doing Enough?

Undoubtedly, cyberspace has become a key playing field of NATO's overall defence and deterrence posture. Yet, the question remains whether the Alliance is doing enough. NATO's internal challenges can significantly underestimate its efforts to build a solid cybersecurity posture. NATO has traditionally focused more on its military character rather than on its political role to promote constructive internal dialogue among its members, to consult on defence and security-related issues to solve problems, build trust and, in the long run, prevent conflict. Thus, it is essential that NATO updates its political foundation and enhances its political cohesion under its common purpose, that is, the protection of the Euro-Atlantic area (NATO, 2021; NATO, 2020; Deschaux-Dutard, 2021; Brent, 2019).

Moreover, the Alliance has often been accused of being a monolithic structure rather than a hub of political dialogue (Shea, 2020). Disputes between its Allies have often impacted NATO unity on external matters. Driven mainly by national interests, these disputes have constrained NATO's cohesion. Worries have also been expressed about the commitment of the United States to the defence of the European continent, the impact of the European Union's development as a security actor on the future of NATO, the commitment of some European Allies to burden-sharing of defence, and the development of political inroads by NATO's rivals into the Alliance territory (Reflection Group, 2020; Belkin, 2020; NATO, 2021; NATO, 2020; Deschaux-Dutard, 2021; Brent, 2019; Shea, 2020). All these issues have significantly challenged NATO's decision-making, which needs political cohesion to shape decisions, including on cyberspace-related matters.

Another major challenge emanates from undermining NATO's fundamental principles from inside. Some allied governments have moved away from NATO's fundamental freedoms (Ricketts, 2020). For instance, Poland, Hungary, and Turkey have undermined free speech, free press, and the independence of courts. These actions have threatened democracy, individual liberty and the rule of law, the foundation of the North Atlantic Treaty (Lute & Burns, 2019). Erdogan has aligned Turkey closer to Moscow rather than the United States or the European Union (Petrov, Schütte et al., 2020). As a result, NATO's cohesion and credibility are at stake with important implications for its deterrence, defence and security posture in all domains, including cyberspace (NATO, 2021; NATO, 2020; Deschaux-Dutard, 2021; Brent, 2019; Shea, 2020).

Yet, NATO remains an adaptable Alliance with a powerful toolbox. NATO's Strategic Concept needs to be updated in line with the current security developments (Moller & Rynning, 2021; Reflection Group, 2020). The 2021 Brussels Summit has paved the way for enhanced political dialogue, cohesion, and consultation amongst the 30 Allies on critical issues against unilateral decisions that hurt NATO's credibility (Petrov & Schütte et al., 2020). Furthermore, although NATO's forward-looking reflection process suggests a useful consultation mechanism, it risks that NATO goes shallow by undertaking more tasks and sitting alongside collective defence, crisis management, and cooperative security (Moller & Rynning, 2021). Therefore, it is an element that should be considered within the renewal process of NATO's Strategic Concept (NATO, 2021; NATO, 2020; Deschaux-Dutard, 2021; Brent, 2019; Shea, 2020).

NATO remains associated with more classical military operations outside its territory. However, today's non-conventional threats can originate just as easily from within and outside NATO's borders (Shea, 2020). Thus, NATO needs to constantly enhance its resilience capacity to better achieve early warning of attacks, best limit the damage and recover as quickly as possible (Shea, 2020). NATO can also share its leadership and decision-making with civilian actors outside the conventional military chain of command (Shea, 2020). Coherent policies with a common denominator that the Allies are all willing to support can empower NATO's posture (Shea, 2020; NATO, 2021; NATO, 2020; Deschaux-Dutard, 2021; Brent, 2019; Shea, 2020).

Political consultation with partnerships is equally valuable. In recent years, NATO's partnerships have been affected by blockages due to bilateral disputes between partners and Allies, inadequate funding, and over-reliance on voluntary trust funds (Reflection Group, 2020). Furthermore, instead of a pick-and-choose model, NATO members can distinguish between different categories of partners to engage and influence NATO (Emerging Leaders Working Group, 2014). Thus, NATO, as the only institutional framework for the transatlantic partnership, needs to consider this issue (Heinrich, 2018; NATO, 2021; NATO, 2020; Deschaux-Dutard, 2021; Brent, 2019; Shea, 2020).

Conclusion

In conclusion, NATO finds itself in a complex security environment characterised by the constant rise of non-conventional threats such as cyber threats. As an Alliance with proven record of adaptability over the years, it needs to overcome external and internal challenges. NATO needs a political adaptation to match the progress made in the military sphere since 2014. Although the Allies have tested NATO's unity by taking divergent positions based on their long-term strategic interests, they must reaffirm their political commitment to one another and to NATO's democratic values. Although NATO has already recorded significant steps in cyberspace policy, there is still room for improvement.

Reference List

Belkin, P. (2020). NATO: Key Issues Following the 2019 Leaders' Meeting. Congressional Research Service. [online]. Available at:https://www.everycrsreport.com/files/20200401_R46066_a0abb404b866107cd315ba156d0d673c81ae4898.pdf

Brent, L. (2019). NATO's role in cyberspace. NATO REVIEW. [online]. Available at: https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html

Burns, N., & Lute, D. (2019). NATO at Seventy: An Alliance in Crisis. Belfer Center for Science and International Affairs. [online]. Available at: https://www.belfercenter.org/publication/nato-seventy-alliance-crisis

Deschaux-Dutard, D. (2021). Is NATO ready for cyberwar?. [online]. Available at: https://www.frstrategie.org/sites/default/files/documents/publications/nato-briefs-series/2021/052021.pdf

Ellehuus, R., Allers, R., Eggen, K. A., Gullestad Rø, J., O'Neill, P., Major, C., & Mölling, C. (2021). Security in Northern Europe in the Biden Era. Center for Strategic & International Studies. [online]. Available at: https://www.csis.org/analysis/security-northern-europe-biden-era

Ellehuus, R. (2021, February 4). Repairing and Rebalancing NATO. Center for Strategic & International Studies. [online]. Available at: https://www.csis.org/analysis/repairing-and-rebalancing-nato

Ellehuus, R., & Morcos, P. (2021, March 12). 'Lifting Up Our Values at Home': How to Revitalize NATO's Political Cohesion. Center for Strategic & International Studies. [online]. Available at: https://www.csis.org/analysis/lifting-our-values-home-how-revitalize-natos-political-cohesion

EURACTIV (2022). Top US cyber official meets NATO allies on Russian threats. [online]. Available at: https://www.euractiv.com/section/global-europe/news/top-us-cyber-official-meets-nato-allies-on-russian-threats/

Heinrich, B. (2018). NATO Beyond 70: Renewing a Culture of Readiness. International Centre for Defence and Security. [online]. Available at: https://icds.ee/wp-content/uploads/2018/11/ICDS-Analysis_NATO-Beyond-70_Heinrich-Brauss_November-2018-1.pdf

Masters, J. (2021, May 6). The North Atlantic Treaty Organization (NATO). Council on Foreign Relations. [online]. Available at:https://www.cfr.org/backgrounder/north-atlantic-treaty-organization-nato

Moller, S. B., & Rynning, S. (2021). Revitalizing Transatlantic Relations: NATO 2030 and Beyond. The Washington Quarterly, 44(1), 177-197. DOI: 10.1080/0163660X.2021.1896133

NATO (2021). Brussels Summit Communiqué. [online]. Available at: https://www.nato.int/cps/en/natohq/news_185000.html

NATO (2021). NATO Cyber Defence. [online]. Available at: https://www.nato.int/nato_static_fl2014/assets/pdf/2021/4/pdf/2104-factsheet-cyber-defence-en.pdf

Petrov, P., Schütte, L., & Vanhoonacker - Kormoss, S. (2020). The Future of EU-NATO Relations: Doing Less Better. Atlantisch Perspectief, 44(2), 38-44. [online]. Available at: https://www.atlcom.nl/artikel-atlantisch-perspectief/the-future-of-eu-nato-relations/

Ricketts, P. (2020). Rediscovering a Strategic Purpose for NATO. PRISM, 9(1), 22-31. Retrieved May 20, 2021, from [online]. Available at: https://www.jstor.org/stable/26940157

Shea, J. (2013). How is NATO Dealing with Emerging Security Challenges? Georgetown Journal of International Affairs, 14(2), 193-201. Retrieved May 20, 2021, from [online]. Available at: http://www.jstor.org/stable/43134426

Morcos, P. (2020, December 3). NATO in 2030: Charting a New Path for the Transatlantic Alliance. Center for Strategic & International Studies. [online]. Available at: https://www.csis.org/analysis/nato-2030-charting-new-path-transatlantic-alliance

NATO (2021). Cyber defence. [online]. Available at: https://www.nato.int/cps/en/natohq/topics_78170.htm

NATO (2021). NATO 2022 Strategic Concept. [online]. Available at: https://www.nato.int/strategic-concept/

NATO (2022). Deputy Secretary General stresses NATO will continue to increase Ukraine's cyber defences. [online]. Available at: https://www.nato.int/cps/en/natolive/news_191143.htm?selectedLocale=en

NATO (2021). Leaders agree NATO 2030 agenda to strengthen the Alliance. [online]. Available at: https://www.nato.int/cps/en/natohq/news_184998.htm?selectedLocale=en