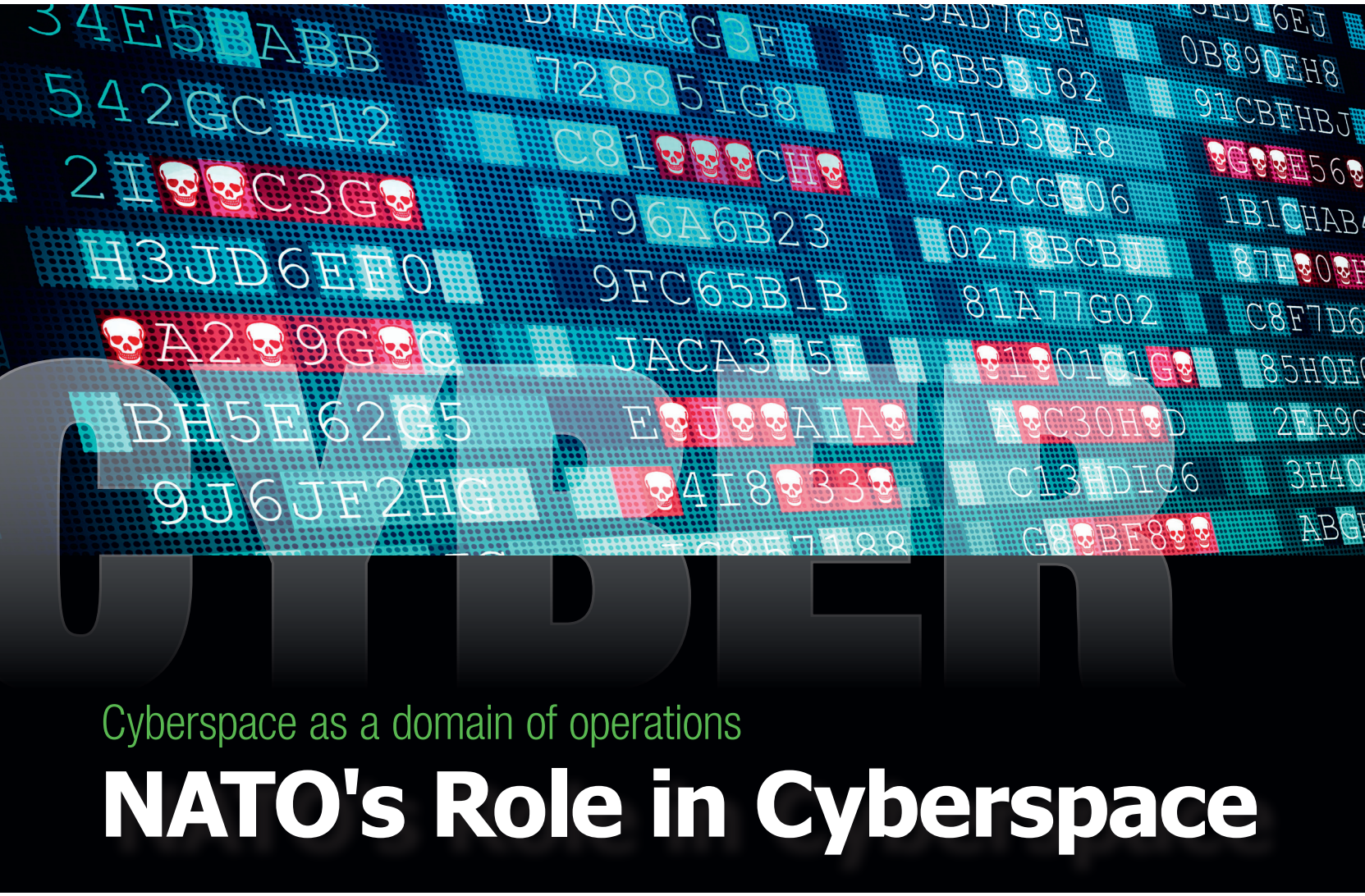

Cyberspace as a domain of operations

NATO's Role in Cyberspace

by **Laura Brent**
Emerging Security Challenges Division
NATO Headquarters

CYBER THREATS TO ALLIANCE security are becoming more frequent, complex, destructive, and coercive. The Allies have taken important steps in cyber defence over the past decade. Most recently, in 2018, they agreed how to integrate sovereign cyber effects, provided voluntarily by Allies, into Alliance operations and missions, as well as to stand up the initial Cyberspace Operations Centre. But is NATO doing enough to address the complex and evolving challenges of cyberspace?

Cyber in focus

The need to strengthen capabilities to defend against cyber attacks was first acknowledged by Allied leaders at their 2002 Summit Meeting in Prague. Since then, cyber has become an increasingly important focus of NATO's Summit agendas. In 2008, the first NATO cyber defence policy was adopted. In 2014, Allies made cyber defence a core part of collective defence, declaring that a cyber attack could lead to the invocation of the collective defence clause (Article 5) of NATO's founding treaty. Moreover, in 2016, Allies recognised cyberspace as a domain of military operations, and further pledged to enhance the cyber defences of their national networks and infrastructure as a matter of priority.

Significant strategic, operational and technical strides have been taken by NATO and its Allies to address malicious cyber activity. Nevertheless, Allied leaders warned at their most recent Summit in Brussels in 2018 that cyber threats to the security of the Alliance are becoming more frequent, complex, destructive, and coercive.

The enduring challenge yet evolving nature of cyber threats requires that the Alliance continuously evaluate whether it is adapting and responding appropriately. Three questions are key to evaluating NATO's role in cyberspace:

- What is NATO's primary purpose in cyberspace?
- What challenges does NATO face in achieving this purpose?
- Is NATO doing enough to address the complexities of cyberspace?

Purpose and challenges

The clearest statement of NATO's purpose as an Alliance in cyberspace was made first at Warsaw and reiterated in Brussels: "We must be able to operate as effectively in cyberspace as we do in the air, on land, and at sea to strengthen and support the Alliance's overall deterrence and defence posture."

Perhaps the biggest challenge to this vision is that, while it is a military outcome, it cannot be achieved solely through military means. All Alliance operations and missions 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.

These enabling capabilities, as well as traditional military targets, have already been subject to cyber attack—and would certainly be so during crisis or conflict. Furthermore, malicious cyber activity has not been the sole purview of militaries, but has been publicly attributed to actors ranging from hacktivists to state intelligence services. So, what may be a military challenge is in fact inextricably linked with both civilian government, private industry and even individuals.

Addressing cyberspace threats is also complicated by the significant amount of activity that takes place below the threshold of armed conflict. Though it is complex to determine proportionate and effective response to such malicious cyber activity, individual Allies have been pursuing various strategies.

Some Allies—including Denmark, Estonia, Lithuania, the Netherlands, the United Kingdom and the United States—have sought to use public attribution of malicious cyber activity to change behavior. The United States has also signaled a new policy to attempt to reduce malicious cyber activity. The United States Cyber Command now recognises that "adversaries operate continuously below the threshold of armed conflict to weaken institutions and gain strategic advantages," and the United States will now pursue persistent engagement, by which it seeks to similarly continuously interact with those who would seek to exploit vulnerabilities of the United States in cyberspace.

While NATO is often identified with its Article 5 collective defence commitment, it has a significant history of engagement below the threshold of armed conflict. NATO's Strategic Concept lays out three essential core tasks for the Alliance: collective defence, crisis management, and cooperative security. Today, for example, NATO has a training mission in Iraq and is engaged in maritime security operations in the Mediterranean. NATO must continue to explore how best to similarly engage in cyberspace, as even a below-the-threshold cyber attack can be highly damaging, disruptive and destabilising. Finally, these challenges—many stakeholders, myriad threat actors and actions in grey space—are compounded by the increasingly rapid pace of change: technology continues to evolve and vulnerability to attack increases as a greater range and number of devices connect to each other and to the internet. To simply keep abreast of the threat requires significant information, investment, human talent and technical capability.

With this understanding of NATO's fundamental cyberspace objective and the characteristics of cyberspace that make achieving this difficult, let us explore the programme of cyberspace work that has already been undertaken, before moving on to consider whether NATO is suitably ambitious in both its objective and actions.

A Belgium Navy Remote Environmental Monitoring Units team analyses the data saved by their autonomus underwater vehicle during TRIDENT JUNCTURE 2018. Photo by Fran C. Valverde

Current state of work

NATO has devoted serious attention to achieving the military end of operating in cyberspace, while not being able to rely on solely military means or stakeholders. Two main strands of NATO activity are addressing this: first, the implementation of cyberspace as a domain of operations and, second, the enactment of the Cyber Defence Pledge.

Cyberspace as a domain of operations: Since the Allies recognised cyberspace as a domain of operations in 2016, NATO has achieved several important milestones. Perhaps most notably, in October 2018, NATO announced the initial stand up of the Cyberspace Operations Centre, or CyOC, in its trial structure. The CyOC serves as NATO's theatre component for cyberspace and is responsible for providing cyberspace situational awareness, centralised planning for the cyberspace aspects of Alliance operations and missions, and coordination for cyberspace operational concerns.

Along with this critical organisational adaptation, Allies agreed at the Brussels Summit how to integrate sovereign cyber effects, provided voluntarily by Allies, into Alliance operations and missions. This is fully coherent with NATO's defensive mandate, as it aligns how NATO defends itself in cyberspace as it does in other domains, with Allies contributing tanks, planes, and ships to Alliance operations and missions.

ABOVE: LOCKED SHIELDS 2018, the largest and most complex international live-fire cyber defence exercise in the world, organized by NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE). In 2018, the exercise included new critical infrastructure components and integrated the technical and strategic game, enabling participating nations to practice the entire chain of command in solving a large-scale cyber incident. Photo by NATO CCD COE

Strategy and guidance is also maturing. In June 2018, Allies approved the Vision and Strategy on Cyberspace as a Domain of Operations. It is anticipated that, in 2019, NATO's first cyberspace operations doctrine will be completed, subject to Allied approval, which will provide guidance to NATO Commanders.

These structures and concepts are only of value if implemented and put to use. To this end, NATO is adapting its education, training, and exercising programmes. The NATO Cooperative Cyber Defence Center of Excellence has been given responsibility for identifying and coordinating education and training solutions in the field of cyber defence operations for all NATO bodies across the Alliance.

Cyber-specific exercises are being continually updated in light of changed policy and doctrine. In 2018, Cyber Coalition—NATO's flagship cyber defence exercise with more than 700 participants from Allies, partners and NATO—exercised the integration of sovereign cyber effects voluntarily provided by an Ally. Other NATO exercises, such as the Crisis Management Exercise (aimed at NATO Headquarters) and TRIDENT JUNCTURE 2018 (aimed at the entire military chain of command), have and will continue to include more robust cyber scenarios.

The Cyber Defence Pledge: Along with this progress at NATO, concurrent whole-of-government adaptation for each Ally is being encouraged through the Cyber Defence Pledge. The Pledge was taken in the context of Article 3 of the Washington Treaty, which states that "Allies will maintain and develop their individual and collective capacity to resist armed attack." As it is impossible to entirely separate military, civil, and industrial concerns in this space, NATO has a strong interest in the improvement of the cyber defence capabilities of organisations outside of the defence establishment. The Pledge highlights development in areas such as appropriately resourcing cyber defence across government; exchanging information and best practices; and leveraging innovative practices from academia and the private sector. Allies assess themselves on an annual basis against a common set of benchmarks. In their most recent report at the Brussels Summit, Allies highlighted the continued utility of the Pledge—it has brought senior political attention to cyber defence issues and has encouraged intra-government collaboration within Allied nations.

"It is anticipated that, in 2019, NATO's first cyberspace operations doctrine will be completed, subject to Allied approval, which will provide guidance to NATO Commanders."

1. Responding to below-the-threshold cyber attacks: Allies are also taking steps to consider how to more systematically respond to malicious cyber activity that falls below the threshold of armed conflict. At the Brussels Summit, Allies expressed their determination "to employ the full range of capabilities, including cyber, to deter, defend against, and to counter the full spectrum of cyber threats, including those conducted as part of a hybrid campaign."

Further, they resolved "to continue to work together to develop measures which would enable us to impose costs on those who harm us." This full spectrum of response, always exercised in accordance with international law and following the principles of restraint and proportionality, is critical to effectively address the prevalence of problematic cyber activity below the threshold of armed conflict.

2. Working with partners: Lastly, to successfully adapt in this quickly changing environment, NATO is working more closely with an ever-increasing range of partners. In 2016, the Secretary General of NATO came together with the Presidents of the European Council and European Commission to issue a Joint Declaration on NATO-EU Cooperation. Under the auspices of this declaration, as well as a technical arrangement concluded between the incident response teams of NATO and the European Union, the two organisations have increased their collaboration, notably in such areas as information exchange, training, research, and exercises.

NATO is also deepening its ties to industry through the NATO Industry Cyber Partnership. This overarching programme provides numerous platforms for the exchange of information, threat trends, and best practices. These interactions help NATO build trusted relationships with industry and better enable all parties to prevent and respond to cyber attacks.

Level of ambition

In all these ways, the Alliance and its Allies are actively improving their cyber defences, positioning NATO to defend itself as effectively as it does on land, at sea, and in the air—allowing cyberspace to contribute to the overall defence and deterrence posture of the Alliance.

But are the Alliance and Allies doing enough? Given the centrality of cyberspace to the modern way of warfare, it is imperative that the Alliance be equally capable in this domain as the others. The approach of the Alliance is sensible: it seeks to address the most significant challenges associated with operating in cyberspace. Ultimately, though, the Alliance must continue to consider how it can do more, since cyber threats are trending only towards more serious impact.

What more, then, should the Alliance be doing? Allies may wish to consider what aspects of their current work should have the greatest priority and resourcing. The CyOC, for example, is the most significant aspect of adapting the NATO Command Structure for cyberspace. As the CyOC moves towards first initial then final operating capacity, it will be critical that it is resourced with sufficient—and sufficiently expert—personnel.

The level of malicious cyber activity below the threshold of armed conflict will remain a continuous challenge; as Allies consider how best to respond, both individually and as an Alliance, they may wish to consider existing tools. In addition to Article 5, generally the most well-known part of the Washington Treaty, Allies also have Article 4 at their disposal, which allows for consultation whenever any Ally believes an Ally's "territorial integrity, political independence, or security" is threatened.

Finally, when seeking to keep pace with change in this domain, Allies might see benefit in continuing to evaluate how collaboration with industry might evolve—both how it shares information and how it procures technologies. The Alliance, in short, should continue on its current path, ensuring that through continued attention and resources, cyberspace can become an ordinary part of business. ✦

ABOVE: With the requirement for resilient and secure cyber systems, NATO developed its Cyber Defence Concept and the Joint Warfare Centre recently launched a multi-year Cyber Capability Integration Campaign within its collective exercise programme. The aim is to challenge NATO at the operational level with simulated real-world threats and facilitate the development of the DOTMLPFI (doctrine, organization, training, material, leadership, personnel, facilities, interoperability) for cyber. Read more about the initiative at www.jwc.nato int "Warfare Development in Focus" (**Transformational Activities at the JWC** by Peter Hutson)

EDITOR'S NOTE: *This article was first published in NATO Review Magazine, 12 February 2019.*

LAURA BRENT currently serves in NATO's Emerging Security Challenges Division and has previously held cyber policy roles in both the public and private sectors, addressing complex strategy, policy and operational challenges in varied and fast-changing environments.