EXCLUSIVE

THE THREE SWORDS
interview

THE PAST, PRESENT AND FUTURE OF NATO's CYBER DEFENCE

Photo by NATO

LAURA BRENT

NATO
OTAN

> “NATO has both the **policy** and **experience** to respond to a **cyberattack** with the invocation of **Article 5**, should an attack be of sufficient impact.”

LAURA BRENT 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. NATO operationalized cyberspace as a military domain in 2016, at the Warsaw Summit, saying that "cyber-attacks present a clear challenge to the security of the Alliance and could be as harmful to modern societies as a conventional attack". This same year, NATO endorsed the Cyber Defence Pledge to ensure it "keeps pace with the fast-evolving cyber threat landscape" in the Euro-Atlantic Region.

Interview by Inci Kucukaksoy and Peter Hutson
NATO Joint Warfare Centre

Ms Brent, thank you very much for this interview. Can you describe the role of NATO's Emerging Security Challenges Division and its relation to cyberspace?

— Before moving immediately to the role of the Emerging Security Challenges Division, I would like to describe the evolution of cyber defence at NATO very briefly. Cyber defence has long been a critical security issue for the Alliance. NATO has always protected its communications and information systems, but Allies first addressed cyber defence at a political level 18 years ago at the Prague Summit by recognising the need to improve the technical cyber defences of NATO. In the intervening years, the Alliance has continued to develop and adapt. Consequently, cyberspace is now a domain of operations and cyber defence is a part of NATO's core task of collective defence.

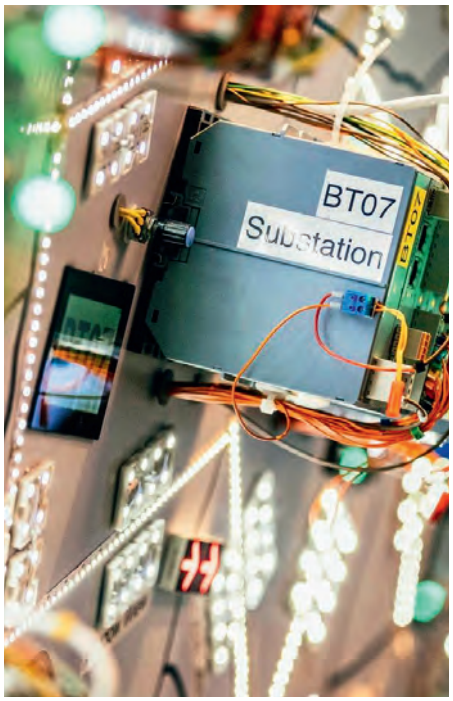
Given the complexity and importance of cyber defence, many NATO entities have cyber defence responsibilities. Allied Command Operations (ACO), Allied Command Transformation (ACT), the NATO Communications and Information Agency (NCI Agency), the International Military Staff, the International Staff, and others, all have a role to play.

The Emerging Security Challenges Division (ESC), which is a part of the International Staff, is a key part of this NATO cyber defence infrastructure. The Cyber Defence Section, which sits within ESC, has two groups: a Cyber Defence Policy team and the Cyber Threat Assessment Cell (CTAC). The policy team, which I am a part of, provides advice and guidance on the development of cyber defence policy at the political level, and we implement the cyber defence policy decisions of the Allies. We also directly support the work of the Cyber Defence Committee, which is the lead committee for political cyber defence governance and policy. My colleagues in CTAC, as the name suggests, provide strategic analysis and assessment of the most serious cyber threats to the Alliance. Additionally, ESC cooperates closely with other NATO entities, as well as with Allies and Partners, to continuously improve and strengthen our cyber defence awareness and capabilities.

NATO's first new domain in 70 years was cyberspace, a virtual space that is manmade, which was added to the more traditional air, land, and maritime domains. Can you explain how this new domain of operations has evolved within and impacted NATO? How would you characterise the key milestones since then?

— At the 2016 Warsaw Summit, Allies recognised cyberspace as a domain of operations. To understand both the implications and implementation of this decision, it is useful to look first at how Allies presented their reasoning in the *Warsaw Summit Communiqué*. Allies recognised cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea. Allies went on to explain that this decision would help NATO better protect and conduct operations across all domains; support NATO's deterrence and defence mission; better integrate cyber defence into operational planning; and better organise and manage cyber resources, skills, and capabilities. In short, Allies took this decision

►►►



ABOVE: Exercise LOCKED SHIELDS, the world's largest international live-fire cyber defence exercise, organised by NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), aims to to assess a crisis situation, maintain services and defend networks that have fallen victim to cyberattacks. Photo by CCDCOE

ther, in January 2020, NATO completed the Allied Joint Doctrine for Cyberspace Operations (Allied Joint Publication, or AJP, 3.20).

The impact of cyberspace as a domain of operations on training and education is also being assessed and addressed. The NATO Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia, has responsibility for defining and coordinating education and training solutions in the field of cyberspace operations for all NATO bodies.

Finally, Allies have ensured that cyber capabilities can be utilised in the context of Alliance operations and missions (AOM). At the 2018 Brussels Summit, Allies announced they had agreed on how to integrate sovereign cyber effects, provided voluntarily by Allies, into AOM. I would stress that this in no way changes the defensive nature of the Alliance; it simply ensures that cyberspace capabilities are approached in the same manner as capabilities in other domains.

Can you summarise NATO's cyber strategy and doctrinal approach? How does the Alliance synchronise its cyber approach across all Member Nations?

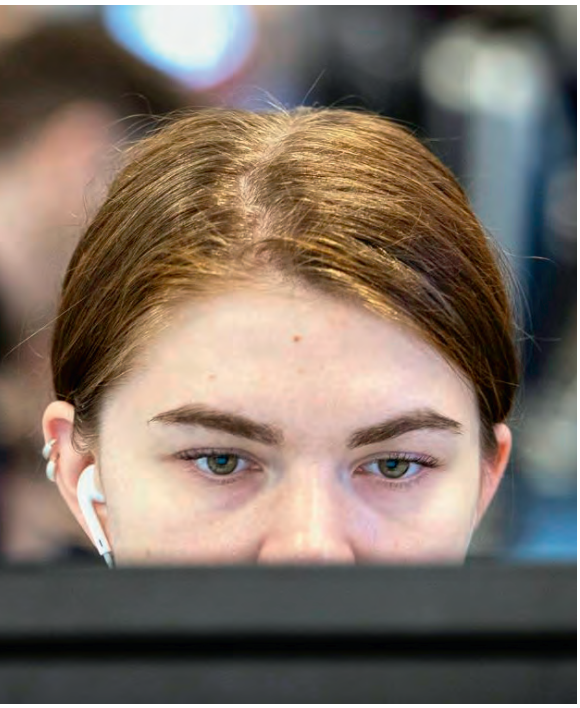
— While the entirety of NATO takes its direction from the North Atlantic Council, it is still a political/military Alliance with different, but complementary, policies across the many parts of the organization. When considering the political aspect, the enhanced cyber defence policy of 2014 serves to lay out key pillars of our cyber approach. This policy provides for strengthening and mainstreaming cyber defence across NATO; streamlined governance; reinforced capability development and capacity building; and enhanced cyber defence cooperation with industry, other international organizations, and partners. It thus emphasises that NATO and Allies both have cyber defence responsibilities, and that cooperation with others is beneficial to improving our cyber defences.

When considering that which is primarily military, I would mention again the "Military Vision and Strategy on Cyberspace as a Domain of Operations" and AJP 3.20. These together help lay out the approach of NATO to cyberspace as a military domain of operations, as well as how cyberspace operations are to be approached in the context of joint operations.

NATO has several tools to ensure that these policies and approaches are aligned across the Alliance. First, key policy and doctrine are approved by Allies, which allows Allies to set to ensure that cyberspace is integrated with, and prioritised equally to, the traditional domains. They anticipated that cyberspace would be contested in any conflict, so NATO must organise, train, and equip itself appropriately to ensure the defence not only of cyberspace, but of all domains.

Over the past four years, NATO has reached numerous critical milestones to implement this decision. One of the key organizational adaptations has been the initial stand up of the Cyberspace Operations Centre (CyOC) within Supreme Headquarters Allied Powers Europe (SHAPE). The CyOC, which serves as the theatre component for cyberspace, is responsible for providing cyberspace situational awareness, cyberspace domain advice, centralised planning for the cyberspace aspects of Alliance operations and missions, as well as coordination for cyberspace operational concerns.

Currently, NATO is working to update doctrine and policy. In June 2018, Allies approved the "Military Vision and Strategy on Cyberspace as a Domain of Operations". Fur-



ABOVE: Exercise LOCKED SHIELDS 2019, photos by CCDCOE.

the direction of the Alliance and agree to the key areas on which they must remain synchronised. Second, there are specific planning tools that set a baseline for capability development and alignment. The NATO Defence Planning Process (NDPP) is perhaps the most fundamental part of this process, providing a framework for Allies to develop required forces and capabilities in a coordinated manner. NATO also has a Standardization Office that, unsurprisingly, helps ensure military operational standards across the Alliance. Third, there are less compulsory, but still structured, processes that provide coordination and interaction amongst the Allies, such as the "Cyber Defence Pledge" self-assessment process.

Cyberattacks are used within hybrid warfare with social, economic and strategic impacts on behaviour and morale. How can NATO prepare against the complexities of cyberspace and mitigate cyber threats?

— When considering how NATO should prepare for and respond to the broad array of cyber threats that you lay out, I believe it is important to separate roles and responsibilities, on one hand, and coordination and cooperation, on the other. NATO is fundamentally a defence and security organization that cannot, and should not, attempt to address each and every cyber threat. This interview talks at length about the areas where NATO can, and should be acting, such as ensuring that it can operate in cyberspace, defend its own networks, provide a framework for Allies to continue improving their cyber defence capabilities, and so on and so forth. While cyber-enabled disinformation, or election interference, or other issues absolutely could impact a nation's security, NATO is not necessarily always the appropriate sole or lead body to address these issues. I sometimes consider: would a Ministry of Defence have primary responsibility for a given cyber issue domestically, or might it in fact occupy a role in support of civil authorities? If, nationally, the defence establishment is in a supporting role, it is a good bet that NATO will be so as well.

This would then take me to coordination and cooperation. Even if NATO might not be the primary owner of an issue, it is often well positioned to reinforce and support the work of both Allies and other international organizations. NATO, for example, does not set cyber norms, but it closely follows and supports the work of organizations, such as the United Nations (UN) and Organization for Security and Cooperation in Europe (OSCE). NATO also provides a forum, through Article 4 of the North Atlantic Treaty, in which Allies can consult whenever they believe their territorial integrity, political independence or security is threatened. This gives Allies broad latitude to bring forth some of the issues mentioned above.

Under what circumstances could a cyberattack trigger a NATO Article 5 response?

— In 2014, at the Wales Summit, Allies affirmatively stated that a cyberattack could lead to the invocation of Article 5. When thinking about Article 5, though, I consider it as an effects-based response, rather than an attack-vector-based response; meaning, it is not about how an attack is carried out, but the effect it has on an Ally.

The one time that Article 5 has been invoked — that is, in response to the terrorist attacks against the United States on September 11, 2001 — it demonstrated the importance of this effects-based approach. When the North Atlantic Treaty was signed in 1949, I am not sure how many nations would have thought that it would have been an act of terrorism against the United States in 2001 that led to the invocation of Article 5.

The process of invoking Article 5 after 9/11 is also relevant when considering how

Article 5 could be used in response to a cyber-attack. On 12 September, the North Atlantic Council stated that, should the attack on the United States be determined to have been directed from abroad, the action was covered by Article 5. On 2 October, after the United States presented further information to the Council, it was determined that the attack had emanated from abroad, thus confirming the invocation of Article 5. Basically, it was determined almost immediately that the attack was of sufficient severity to invoke Article 5, and then the exact attribution of the attack soon followed.

It is also important to note the inherent flexibility of Article 5, in that it does not require a specific response, but rather states that the Alliance can take "such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic Area". In short, the Alliance has both the policy and experience to respond to a cyberattack with the invocation of Article 5, should an attack be of sufficient impact.

What is the importance of the Cyber Defence Pledge? Can you explain the significance of resilience in cyber defence?

— At the Warsaw Summit in 2016, Allies pledged to enhance the cyber defences of their national networks and infrastructure as a matter of priority. In order to implement this Pledge, Allies have developed a self-assessment and reporting process. Allies now assess themselves on an annual basis against a wide range of cyber defence areas, covering resourcing, organization, education and more. During this self-assessment process, Allies also meet with the International Staff, which draw up summary reports — a sort of state of the cyber defences of the Alliance, if you will.

When thinking about the importance of the Pledge, I would highlight a few key aspects. Firstly, it has been extremely useful that this Pledge was made at the level of Heads of State and Government. This has helped ensure that cyber defence is treated as a strategic and political issue, rather than solely a technical one.

Secondly, the Pledge has encouraged enhanced intragovernmental communication and collaboration. As the Pledge covers a broad range of issues, a broad range of actors must coordinate on the response. Finally, the Pledge has been useful for sharing a diverse set of best practices amongst the Allies. The Pledge has no specific end date or target maturity level. Instead, it is about the need for continuous

> "**Resilience** recognises that there will be **cyber incidents** and that it is impossible to prevent them all. Organizations must thus be prepared to **effectively manage** and **recover** from such incidents."

Joint Warfare Centre: NCI Agency's Stavanger Unit life-tests IT prior to a training event. Photo by Tudor Jelescu

improvement. I see this as closely linked to the concept of resilience. Resilience recognises that there will be cyber incidents and that it is impossible to prevent them all. Organizations must thus be prepared to effectively manage and recover from such incidents.

Many governments and private sector organizations now often say that incidents are a matter of *when*, not *if*, which makes resilience a more flexible and realistic approach. The mindset of ongoing improvement and adaptation captured through the Cyber Defence Pledge is thus well-aligned with the idea of cyber resilience.

The Joint Warfare Centre first introduced cyber defence to its operational level exercises in 2011, giving NATO the opportunity to explore the wide and far reaching impacts of cyber threats to operations and allowing the Joint Force Commands to evaluate the effectiveness of their preparations against an aggressive and competent cyber adversary. You have also participated in the command post exercise portion of TRIDENT JUNCTURE 2018, which was directed by the Centre. What were your key observations and general impressions regarding cyber play in this exercise?

— Cyber, as a component of operational level exercises, is absolutely critical, and it is excellent that the Joint Warfare Centre has nearly a decade of experience incorporating cyber aspects into its exercises. As you note, I was fortunate enough to observe a portion of TRIDENT JUNCTURE 2018 from the Centre in Stavanger. It was extremely useful to see the real-time interaction between the many cyber elements of NATO, such as NATO Headquarters, SHAPE, the Joint Force Commands, as well as the NATO Communications and Information Agency. Such an exercise makes clear that an integrated understanding of relevant cyber threats from all perspectives — technical, operational and political/strategic — is necessary during operations. From this experience, I would also emphasise the continued importance of ensuring that the cyber portions of an exercise are made relevant to all participants, not just those who are cyber defenders.

Do you have any recommendations for future cyber scenarios? Additionally, how can our exercises support the progress?

— When cyberspace was declared a domain of operations, it was to ensure that NATO approached cyberspace as it would any other domain. In other words, it must be viewed as integral to, and integrated with, mission success. Thus, cyber can — and should be — incorporated into any scenario. While cyberspace may often be the supporting rather than supported domain, it is still critical to the conduct of missions. As such, scenarios that adequately test operations in a degraded cyber environment, for example, are useful. I would simply encourage the Joint Warfare Centre to support the maturation of this domain of operations by ensuring that cyberspace is a central component of its exercises.

As NATO moves forward with the cyber domain, what issues would you highlight as the most challenging for the Alliance?

— All Allies are making progress to improve their cyber capabilities. Threats, however, will continue to evolve, which means that we must continue to adapt and mature as well. While this can seem overwhelming, it is the great advantage of NATO that it has 30 Allies who are working to address these challenges, both individually and in concert. Though it requires attention to ensure that Allies remain aligned in the face of different cyber priorities or governmental structures, the diversity of approach is fundamentally useful to Alliance. All Allies are able to learn from each other. The challenges of cyberspace are both myriad and complex. NATO, though, presents a key structure to continue addressing these issues in a coordinated and reinforced manner. ✦

BELOW: Joint Warfare Centre's Exercise Situation Centre (SITCEN). With a long-lasting experience in joint operational training, doctrine development, and transformational activities, the Centre is the ideal establishment to support NATO in the evolution and adaptation to the rapidly changing cyber warfare. Photo by NRDC-Italy PAO

LOCKED SHIELDS:
https://ccdcoe.org/exercises/locked-shields/