NATO Electronic Warfare and Cyberspace Resilience

XV

By Air Chief Marshal Sir Stuart Peach GBE KCB ADC DL, UK Air Force
Chairman, NATO Military Committee

Any organization needs to adapt to survive. NATO is no different. In the last two years working closely with the NATO Chiefs of Defence, our Alliance has delivered the first NATO Military Strategy since the 1960s. This provides the framework for NATO as a military Alliance. Supreme Allied Commander Europe (SACEUR) is delivering the Deterrence and Defence for the Euro-Atlantic Region Concept and SACT is leading on the delivery of the NATO Warfighting Capstone Concept, which formalizes our approach to the future via a structured warfare development agenda.

NATO's component commands have been equally busy in preparing and adapting for the future, as have some of our Centres of Excellence. Under the leadership of General Harrigian, the JAPCC is developing concepts such as Joint All-Domain Operations, which includes the Electromagnetic Spectrum (EMS) and Electronic Warfare (EW), which help keep NATO strong and fit for the future. Our Alliance continues to adapt, as it has done for more than 70 years, to defend and deter across all domains.

As a strong supporter of the JAPCC, I am especially delighted to be able to contribute some thoughts ahead of the 'NATO EMS Emphasizing Electronic

Warfare' Panel. These are essential topics for NATO and support our thinking on how to understand the requirements, the shortfalls and how to work together to address both.

In recent years, NATO has had to adapt to face new challenges presented by the rapid advancement of technology, some of which are non-conventional, such as cyber or hybrid threats. These threats have become transnational, non-attributable and in some cases, low-cost. Those who want to harm us are using them. They are not 'emerging,' they are in use. So disruptive technologies influence the modern security environment; therefore keeping up with the rapid pace of technological change remains one of the biggest challenges for our Alliance.

Potential opponents are focusing on developing Cyber and EW capabilities, as they represent relatively 'low-cost' and asymmetric ways to impact or dominate operational domains. Russia and China have been particularly active in Cyber and Electronic Warfare, and are exploiting the Electronic Magnetic Spectrum to great effect. By observing Russia's ongoing cyber and electronic warfare actions, as well as China's evolving strategies, the West, including NATO and its allied militaries, need to be able to counter these capabilities.

The combined experience and strategies of our Nations are shaping NATO's view on Cyberspace, the EMS, and EW disciplines. Additionally, the number of nations actively developing new approaches and capabilities in these fields demonstrates the collective understanding that exploiting the Cyberspace domain and electromagnetic environment for military advantage is vital to achieving military objectives across our range of operations. The trick is to evolve coherence, spot opportunities and innovate.

Not only has this helped our Alliance build a response, but it helps strengthen interoperability in Cyberspace and EW among Allies and

Partners. Interoperability remains a key enabler for NATO and facilitates meaningful contributions from all Allies and Partners to its core tasks. Improving our interoperability provides significant cost benefits to NATO Nations as members pool and share resources. Our Alliance is the convening authority for Cyberspace and EW to enable interoperability in response to these emerging threats; we should act like it.

Each of the military operational domains are inextricably linked. In order to deter aggression, NATO must demonstrate its ability to act simultaneously across Land, Sea, Air, Space and Cyberspace. Cross-domain deterrence invariably involves the use of threats in one domain to counter activities in other domains. In the future, the interdependencies between domains will continue to grow, much like what we have seen with the use of hybrid tactics. Countering hybrid actors and activities calls for a comprehensive and coordinated response in multiple domains, which means NATO must start considering deterrence and defence across all domains through a multi-domain warfighting approach. This has re-emphasized the need for NATO to move beyond 'joint operations' and start thinking and acting in a multi-domain environment.

I have made clear our calling for a renewed focus on improving proficiency in our Cyberspace and Electromagnetic Spectrum Operations: by building awareness, developing policies and strategies, acquiring new capabilities, working with industry and academia, and training our people to become experts.

Often our military leaders highlight the critical role that Cyberspace, the EMS, and EW play in warfare within all operational domains to remind Alliance decision-makers of their importance. And we see other actors in this arena making the case for us. The many attacks and displays of cyber and EW activities in the last few years – especially prominent during Russia's illegal annexation of Crimea, but also widely in use throughout the

COVID pandemic – spurred NATO Nations back into action with the largest reinforcement of NATO's collective defence in a generation, including in the fields of cyber and EW.

In Cyberspace, NATO has established a roadmap to Cyberspace as an operational domain approach, with activities along the following lines of effort: training, capability development, organizational constructs, operational planning, exercises and strategic communications. We have reinforced our hybrid and cyber defences by establishing Counter-Hybrid Support Teams and a Cyberspace Operations Centre.

The use of the word 'deterrence' in connection with Cyberspace is significant, because it is another step towards the acceptance of offensive cyber capabilities as part of collective defence. NATO has agreed to integrate national cyber capabilities or offensive cyber into allied operations and missions. We have continued to build our resilience by updating our baseline requirements for national resilience, such as energy, transport, and communications, including the impact of 5G and other new technologies. We also address threats from Cyberspace; the security of supply chains; and foreign ownership and control of infrastructure. All of this will make NATO more effective and resilient in Cyberspace. This work is urgent.

In order to continue adapting to the changing security environment, NATO is developing better policies and doctrines. Amongst others, the 2019 NATO Military Strategy, provides us with overarching military guidance that sets out NATO's military priorities and approach to current and future threats, and guides commanders on tasks to maintain our security. Our thinking has fundamentally shifted from capability-based assessments to threat-based assessments. We are intelligence-led and threat informed. Building on the military strategy, two concepts have been developed. First, the concept of the Deterrence and Defence of the Euro Atlantic area (DDA), which brings together current military thinking as we

face a more unpredictable world and deal with the consequences of a changed security environment. The DDA is supported by the NATO Warfighting Capstone Concept, which looks forward 20 years and sets a vision to support Allies' efforts to develop the Alliance's Military forces. The concept will identify potential capability gaps and provide the necessary recommendations to ensure NATO exploits opportunities and innovative approaches, including the use of emerging and disruptive technologies, to maintain its military advantage. This work is essential for maintaining NATO's military edge and ensuring that our capabilities remain fit for the future. We must also consider new technologies to enable our defence in the digital age, and in the age of artificial intelligence. Crucially, these concepts steer the resource plans that are required to make this a reality.

NATO continues to research, develop, test, and train new capabilities as well as develop and refine our tactics. Thanks to the work done thus far, our Alliance has already been acquiring some of these capabilities. NATO's fleet of AWACS aircraft will undergo a modernization effort, valued at 1 billion US dollars, providing the fleet with sophisticated new communications and networking capabilities. It will ensure that NATO AWACS continue to be our 'eyes in the sky', supporting our operations until 2035. NATO will also acquire over 1 billion euros worth of satellite capacity in 2020–2034. This is NATO's largest investment in satellite capacity. It will help our forces communicate with each other more securely and more quickly. We have a Space Centre, which will grow. Allies will also be able to share information gathered by remotely piloted platforms. In addition, NATO will move ahead with 1.4 billion euros of investment in new technologies in areas ranging from cybersecurity to surveillance and reconnaissance. Earlier this year, SACEUR declared NATO's fleet of new Alliance Ground Surveillance aircraft initially operationally ready to conduct missions. This is a major milestone for the programme. We have a Joint Enterprise for Intelligence, Surveillance and Reconnaissance. With a reset on EMS/EW, NATO is on the right track, but in an unpredictable world, we

cannot let our guard down. NATO is determined to stay ahead of the technological curve.

However, for NATO to be successful in its deterrence and defence posture, it must harness both traditional and non-traditional technologies, including innovation from the civilian sectors. Today, most advancements in technology are driven by the commercial sector rather than the public defence sector; industry now far exceeds military investments in research and development. Readily available cutting-edge components produced by the civilian sector allow our military research and development to leverage commercial-scale production and thus prioritize the development of military-essential components without the duplication of work. NATO understands the benefits of working with subject matter experts and start-ups, their expertise is crucial for NATO to remain agile and capable; we need to make it easy for them to work with us.

More advanced technologies and better interoperability can improve NATO's overall efficiency throughout Cyberspace and the EMS. While, heavily investing in new capabilities, NATO is also looking at our existing courses to identify any types of gaps and overhaul the individual training opportunities. We are also increasingly incorporating cyber and EW in our exercises. Locked Shields, Cyber Coalition, Trident Juncture, Unified Vision, and NEMO exercises all have cyber and EW components, so allied and partner troops can observe their effects in real life, and practice countering them.

NATO is aware of the opportunities, challenges, and threats posed by cyber and EW. We are working together to achieve an edge, be it by increasing our defence spending, investing in better capabilities, improving the institutional awareness of our leadership, educating and training our troops in realistic scenarios, developing supporting policies and strategies or building our interoperability.

However, we must also consider that to provide a credible military advantage, the people, processes, and systems of the future must be able to operate in a complex, multi-domain, cross-organizational and multinational environment, to deliver needed effects through the superior employment of EMS, EW, and Cyberspace capabilities. Therefore, we must aim for NATO to achieve its vision of Cyberspace and EMS exploitation, access, and control when and where needed to achieve Alliance objectives.

For over 70 years, NATO has protected our populations, by learning from the changing security environment and continuously adapting to existing and emerging challenges. By engaging together as an Alliance of 30 Nations, on complex topics related to Cyberspace and EW, we all benefit.

As we have demonstrated time and time again, NATO's success rests in its ability to continuously adapt to a changing world and a shifting security landscape. We will continue to do so to guarantee the security of all of our Allies.

Air Chief Marshal Sir Stuart Peach (UK Air Force) is the 32nd Chairman of the Military Committee of NATO. He is NATO's most senior military officer and is the Military Adviser to the Secretary General and the North Atlantic Council. He attended the University of Sheffield (BA), University of Cambridge (MPhil in International Law and International Relations), RAF Staff College and the Joint Services Command and Staff College (HCSC). He holds four honorary Doctorates from UK Universities: Hull, Kingston, Sheffield and Loughborough, in Technology and Letters (DTech, DLitt).