Jacob Galbreath

DOI:10.33179/BSV.99.SVI.11.CMC.24.2.00

EDITORIAL

CYBER SECURITY AND DEFENCE CHALLENGES

Ferdinand Foch, the Supreme Allied Commander during the First World War, famously said in 1910: »The aircraft is all very well for sport - for the army it is useless«. Despite achieving forty years of distinguished service across multiple campaigns and territories, being an acknowledged intellectual leader of the highest regard, and a proponent of advances in land warfare, this expert in his profession was yet completely blind to the fundamental technological shifts that would reshape the world forever. General Foch believed, as did many others in his time, that the domains of the battlefield were as old as human history and absolute. When we look back through the lens of history over the last eighty years, his statement seems naive and archaic, a glimpse of a simpler time. Just as Foch and his contemporaries lived through a time of fundamental change, after 24 February 2022, we shall now look back to our thoughts, statements, and conversations of the last twenty years as naive and archaic. Cyberspace was recognized as a domain of operations at the 2016 NATO Summit in Warsaw. Cyberspace is as critical a domain to be mastered as the skies, the seas, and the land. The debate is over. We must organize, manage, and defend ourselves and our allies wherever our adversaries decide to fight or manipulate our sovereignty.

Will there be a conflict in the future that doesn't involve global cyber actors? How do the Hague and Geneva Conventions apply to these global cyber actors? What is considered a violation of national sovereignty »in the cloud«? What is the difference between a cyber combatant and a cyber spy? Cyberspace does not yet have the agreed upon historic norms, codes of conduct, or even common understanding across the world or even within our own nations and organizations. Now is the time that we must come to an agreement between free nations on those definitions, rules, and codes of conduct so that we may operate in this global domain not just at peace, but also cooperate and collaborate with others to maintain and enforce order in times of conflict.

While we continue to understand this new domain, what is made clear by the Russo-Ukrainian War is that modern nations and organizations will use this domain to conduct operations in order to achieve their objectives and influence results in the physical world. While cyberspace is unique, it cannot be removed from the physical domains. Cyberspace must be seen as more than a simple tool, but instead as an integrated modern hybrid apparatus fundamental to the resilience of our infrastructure and society.

The tools and terrain of all of the domains are understandably different, however they all have something in common: the people. The ideas of Sun Tzu, Jomini, Clausewitz, Mahan, and many other intellectuals are just as relevant in cyberspace. Their insights are still valid in this »new« realm. We can no longer have our people, organizations, and nations view cyberspace as a separate system to their equipment and abilities, but must instead train them to view cyberspace as the integrated part of the whole that it is.

NATO and free nations around the world must lead the way in securing cyberspace as a global resource that freely allows information exchange, trade, and the sharing of ideas. Cyberspace knows no borders or boundaries and we must act together to maintain its security.

We can do this. We must do this.

In order to achieve this goal, we decided on the cooperation of the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia, and the publication Slovenian Contemporary Military Challenges, issued by the General Staff of the Slovenian Armed Forces. This cooperation resulted in a thematic issue dedicated to topical issues in the field of cyber defence.

In **Henrik. P. Beckvard's** article entitled *Protecting critical infrastructure and critical information infrastructure*, we first get acquainted with the terminology. Critical infrastructure and critical information infrastructure are the concepts that need to be defined before we open a debate on their protection, both nationally and internationally. The next step is to start serious discussions and the development of systemic solutions and their unification within international security structures. Despite the differences in definitions, there are many perceived risks and ways to protect critical (information) infrastructure.

Those who pose a risk to critical (IT) infrastructure as well as to other areas of cyberspace and its security also include the employees. This topic has received a lot of attention in NATO, which is also discussed by **Christopher Young** in his article *Planning for success: a call to optimise NATO cyber training*. Training in such a large and diversified international security organization needs appropriate approaches to evaluate such a process and to continuously revise and update it. How the evaluation process in this field is carried out and how many phases it covers is more specifically presented in the paper.

Cyber espionage poses many challenges for both spies and those who wish to prevent or even sanction it. What is the basis for sanctions when generally applicable norms and ethics are violated? What legal norms apply when unwanted activities occur to the detriment of a specific state or society in a way that cannot be geographically or nationally classified in relation to the national and international legal order? **Davide Giovannelli** addressed these and other dilemmas in his article *Extraterritorial jurisdiction over cyber espionage: a new trend in international law or just an example of lawfare*.

Cyber operations fall within the scope of the armed forces. As **Taťána Jančárková** notes in her article *Leashing the dogs of cyber war*, this is a relatively new subject that must be properly regulated, especially from the perspective of oversight. Cyber operations can lead to several types of abuses. To avoid this, they must be properly supervised. Civilian oversight of the armed forces should also include this aspect of supervision. In her paper, the author outlines some approaches to regulate this area.

Cyber war seems to be a logical consequence of cyber operations. However, the latter are not only conducted in a military but also in a civilian setting in various fields. Where are the boundaries, oversight, coordination, and overview? **Ignacio Pizarro's** paper *Learning from experience: old lessons for a new battlefield* benchmarks these new trends in cyberspace against those first lessons learned, which Sun Tzu wrote about. Is it really all new or is it perhaps a long-known »phenomenon«?

In the last article *Russian aggression on Ukraine: cyber operations and the influence of cyberspace on modern warfare*, **Damjan Štrucl** argues that Ukraine has been a testing ground for various Russian forms of cyber operations and cyber war in the last few years, i.e. before the Russian military attack in February 2022. In other words, the so-called 'Gerasimov Doctrine' is being implemented to the full. The author notes that the West perceives cyber operations differently than Russia, or rather, it uses them to achieve military objectives, while Russia uses them to achieve all objectives.