Cyberspace in the current security environment

Diego James Cano Prentice // MSc in Security Studies. Defence.

Cyber is a newcomer to humankind's long history of warfare, yet most countries have been quick to recognise it militarily. Cyber appears in several military strategic concepts, it is considered as a domain of operations by NATO and the U.S., and several countries have created a dedicated cyber combatant command. This essay sets out to offer a brief account of cyberspace's evolution, significance and direction in political-military thought.

In 2008, an infected flash drive inserted into a U.S. military laptop in the Middle East led to what a top Pentagon official described as "the most significant breach of U.S. military computers ever" (NY Times, *Military Computer Attack Confirmed,* Aug 25th 2010). The cyberattack compromised the U.S. Department of Defense's unclassified and classified networks, prompting the Pentagon to lead a counterattack, Operation Buckshot Yankee, which would ultimately lead to the creation of Cyber Command in 2010. The Command now consists of over 6,000 people located at the headquarters at Fort Meade in Maryland and across bases in Georgia, Hawaii and Texas.

> Nowadays, cyber is a crucial element of most operations, across any geographical domain, and not simply as an enabler, but as a battleground of its own

At NATO, cyber was first discussed at the political level in the 2002 Prague Summit. Allied leaders furthered their commitment to protecting their cyberspace at the Rita Summit in 2006, and recognised cyberspace as a domain at the 2016 NATO Summit in Warsaw. The significance of this decision can hardly be overstated: cyberspace was consolidated as a domain of operations of equal importance to the traditional air, land, and sea domains, formally becoming part of the Alliance's core task of collective defence, and Allies confirmed that international law applies in cyberspace. Concurrently, Allies made a Cyber Defence Pledge, which placed a priority on enhancing their cyber defences of national infrastructures and networks. Since then, NATO allies have not only strengthened their defences, but also reinforced their capabilities for cyber education, training and exercises.

The cyberspace domain has thus been recognised by several nations to be as significant as the traditional domains of operation. These domains, after all, share the same essential objective, to enable freedom of action to create desired military effects and deny adversaries such freedom of action. Nevertheless, as retired U.S. Air Force four-star General Larry D. Welch highlights in his essay "Cyberspace: the fifth operational domain", cyber is fundamentally distinct from the traditional domains (as well as the newly recognised space domain) in two regards. Firstly, cyberspace is manmade, and can be constantly changed. Secondly, "cyberspace is embedded in all domains, and operation in all domains is dependent on operation in cyberspace" (Welch, 2011, p.3). Admittedly, one could push back on this characteristic being unique to cyber. After all, traditional domains of operation do relate to and rely on each other in several ways. Multi-domain operations such as anti-submarine warfare (involving ships and aircraft) are commonplace. Arguably, much of traditional warfare, such as army air defence and naval aviation, cannot be effectively carried out in a single domain. Nevertheless, as Welch argues, whereas land, sea, air and space relate to each other in a geophysical hierarchy (land is surrounded by sea, land and sea are surrounded by air, and land, sea and air are surrounded by space) cyber cuts through all domains. Nowadays, cyber is a crucial element of most operations, across any geographical domain, and not simply as an enabler, but as a battleground of its own. Consequently, cyberspace is uniquely interconnected with other domains, meaning that successful cyberspace operations are a precondition for success in most operations.

So what is the current and near-future state of cyber in political-military thought? NATO's Supreme

Foto: iStock.com/metamorworks

Headquarters Allied Powers Europe (SHAPE) has recently established the Cyberspace Operations Centre (CyOC) from which Alliance operational planning and situational awareness is conducted. Allies have also made doctrinal progress, approving the *Military Vision and Strategy on Cyberspace as a Domain of Operations and the Allied Joint Doctrine for Cyberspace Operations (AJP 3.20)*. At the 2018 Brussels Summit, Allies announced that they had integrated sovereign allied effects, so that they could be jointly utilised in Alliance operations and missions (although NATO remains a defensive alliance). Likewise, the U.S. Cyber Command has undergone significant progress from its conception 11 years ago, but it has also recently seen a development in posture. Its Commander, four- star General Paul M. Nakasone, recently published an article in Foreign Affairs where he delineates this evolution, from "a reactive, defensive posture to a more effective, proactive posture called persistent engagement" (Foreign Affairs, August 25th 2020). This posture change sees the command take a more proactive approach to securing the military's networks, prompted by adversary's attacks becoming more "frequent, sophisticated, and severe". Nakasone stresses the importance of operating outside of U.S. networks, together with allies and partners. For example, U.S. Cyber Command worked with Montenegro in 2019 to investigate signs of hacker penetration in Montenegrin government networks.

This essay will not attempt to make any conjectures about the potentially dramatic evolution of cyber in the future security environment due to emerging and disruptive technologies and our increased connectedness. Nevertheless, it is clear that cyber has been playing an increasingly central role in military preparedness across the globe, and will continue to do so in the years to come. ●

FURTHER READING

- NATO, *Warsaw Summit Communiqué*, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016, available at nato.int.
- NATO, *Allied Joint Doctrine for Cyberspace Operations (AJP 3.20)*.
- Nakasone, P. and Sulmeyer, M. "How to Compete in Cyberspace", *Foreign Affairs*, August 25 2020.
- Welch, L. 2011, *Cyberspace, the Fifth Operational Domain*, Institute for Defense Analyses.