commentary

ISTITUTO PER GLI STUDI DI POLITICA INTERNAZIONALE

Commentary, May 2, 2018

CYBERSPACE AND THE ARMED FORCES

FABIO RUGGE

In a 1983 movie, "War Games" a US teenager, while trying to hack into a computer-game company in order to play video games for free, unknowingly logs into the Pentagon's networks and starts a game of "Global Thermonuclear War" playing the role of the Soviet Union. The Pentagon believes that the Russians are in fact initiating preparations for a nuclear strike, and, just minutes before the US supercomputer is about to autonomously retaliate to the (non-existent) threat, its machine learning algorithm is taught the concept of Mutual Assured Destruction, and concludes that in a nuclear confrontation "the only way to win is not to play". The catastrophe is hence avoided. A few weeks after the release of the movie, reality matched fiction: Colonel Stanislav Yevgrafovich Petrov, on duty at a Soviet nuclear early-warning facility, decided to infringe the protocol and not to react to an alarm (which immediately he considered dubious) indicating the United States had launched nuclear missiles on Russia – the alarm this time was caused not by an hack, but by the malfunctioning of the computer detection system. Petrov saved humanity.

These two examples prove that since the very beginning of the cyber age (before the term "cyberspace" even existed!) it was evident that reliable technology was going to be crucial in military operations, that Information and Communications Technologies (ICT) networks were inherently insecure as they may be hacked or malfunction, and that the distinction between what is "cyber" and what is "real" was going to be increasingly difficult to grasp. A few decades later, technological progress added complexity to this scenario. The "first web war" was waged against Estonia in 2007: a massive distributed denial of service attack (DDoS) was launched from the Russian territory (although the involvement of the Russian government was never proved) and paralyzed the country for days. Even if the attack was described as "more like a cyber riot than a military attack", its political, military and strategic implications were clear: cyberspace had been used to achieve actual results "on the ground".

Fabio Rugge, Head of ISPI's Centre on Cybersecurity, and Senior Advisor at Fincantieri to the President for International and Institutional Affairs

Cyberspace has become much more than an infrastructure that enables weapons and early-warning systems: it is now a domain where power is projected, strategic goals may be achieved without the use of force, and wars will be fought. In this "domain of ambiguity", high-end threats share the same operational environment and many of the technical features of low-level skirmishes and criminal activities, and it is impossible to interpret the motivation and the scope of a cyber campaign without considering the strategic, political and operational context in which it occurs. Straightforward operations of intelligence, surveillance and reconnaissance (ISR) when conducted in cyberspace become a key element in a country's deterrence posture, and may constitute, in fact, preparation for war. How to read, for instance, the malwares that have been found in critical infrastructures around the world, other than weapons ready to be used in case of a conflict? Cyber campaigns do not need to exceed the threshold of the use of force to represent a vital threat to national security, and, as such, call into action the Armed Forces in their role of ultimate protector of National security. At the 2016 Warsaw NATO Summit, Allies recognized 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" and that cyberspace is a "domain of operations"[1]. Only two years later, according to the Command Vision for US Cyber Command (eloquently titled "Achieve and Maintain Cyber Superiority") published last March [2] cyberspace is "already militarized" [3], and disruptive technologies (artificial intelligence, autonomous lethal weapons, neurological implants…) will eventually accelerate the adversaries' ability to impose costs.

The US Cyber Command Vision takes a further step, as it draws attention to ongoing cyber campaigns under the threshold of the use of force that pose a strategic, persistent threat to the vital interest of United States. In this perspective, the current reactive posture introduces unacceptable risks to US interests and must be updated by scaling the response to the magnitude of the threat, seeking greater freedom of action and pro-actively engaging US adversaries wherever and whenever they are found, in order to obtain tactical, operational and strategic advantage. The new US posture in the cyber domain must acknowledge that cyberspace is a continuously contested domain, and that an effective deterrence in cyberspace is impossible without persistent engagement with the adversaries.

"Cyberspace capabilities" adds the US Cyber Command, are key to identifying and disrupting adversaries' information operations[4] which are also a key components of hybrid warfare, and an enabler of kinetic military operations. The Russian cyber-enabled information warfare campaign during the last US presidential election is proof that operations on the networks may exploit in many new ways the most critical vulnerabilities of our national securi-

[1] Warsaw Summit Communiqué, paragraph no. 70, available at: http://www.nato.int/cps/en/natohq/official_texts_133169.htm

[2] *The Command Vision for US Cyber Command*, "Achieve and Maintain Cyber Superiority", released in March 2018 and available at: https://assets.documentcloud.org/documents/4419681/Command-Vision-for-US...

[3] Ibid., p. 10.

[4] Ibid., p. 4.

ty[5]. 2018 marks the tenth anniversary of the first use of cyber attacks in support of kinetic military operations, during the Georgian War: a new era in military affairs began. Since then, examples of cyber attacks during international crisis and military operations have multiplied: the Stuxnet worm (2010), the cyber attack against the Ukrainian power grids (2015), the hacking of the Qatari news agency during the recent Gulf crisis (2017).

These are all good examples of how cyber attacks may in the future be, at the same time, the sparkle that ignites a war and the weapon that determines its final outcome. Ensuring the highest level of protection of the Command, Control, Coordination & Communication (C4) networks established for international crisis management and national/collective defence has always been one of the highest priorities for the Armed Forces, and it is therefore not a surprise that with the advent of the cyber age they pursued a solid cyber defence capability. Moreover, virtually all weapons systems depend today upon secure, reliable and resilient networks; technological progress will only contribute to make cybersecurity a core enabler of military capabilities. However, cyber defence goes well beyond the protection of military networks: a cyber attack that disables civilian national critical infrastructures would almost certainly impair the correct conduct of military operations. But there is more: as the potential surface of cyber attacks expands to encompass all sectors of modern societies, defending the nation requires attaining "cyberspace superiority"[6], a goal that only the Armed Forces can achieve. Cyber superiority is key in mapping the theatre of future conflicts, in signaling about cyber capabilities for deterrence purposes, and in shaping international norms of states' behaviors in cyberspace. And it is also critical to national security since, as stated in the 2018 US National Defence Strategy, "it is undeniable that homeland is no longer a sanctuary"[7].

The contributors to this Dossier of the ISPI Center on Cybersecurity will provide different perspectives on how the Armed Forces' scope of action, capabilities, doctrines and force structures evolve following the increasing relevance of cyberspace in all aspects of our daily life. The Dossier will focus, in particular, on how both NATO (that has recently agreed to the creation of a new Cyber Operations Center at SHAPE) and national defence are transforming, and on some of the most relevant and thorny issues about cyber warfare with which the

[5] "Russia uses information operations as part of its offensive cyber efforts to influence public opinion across the globe", *National Security Strategy of the United States*, released December 2017 and available at: https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-20...

[6] "Cyberspace superiority is the degree of dominance in cyberspace by one force that permits the secure, reliable conduct of operations by that force, and its related land, air, maritime, and space forces at a given time and place without prohibitive interference by an adversary", *The Command Vision for US Cyber Command*, p. 6.

[7] "It is now undeniable that the homeland is no longer a sanctuary. America is a target, whether from terrorists seeking to attack our citizens; malicious cyber activity against personal, commercial, or government infrastructure; or political and information subversion. New threats to commercial and military uses of space are emerging, while increasing digital connectivity of all aspects of life, business, government, and military creates significant vulnerabilities. During conflict, attacks against our critical defense, government, and economic infrastructure must be anticipated". *2018 US National Defence Strategy*, p. 3, released in January and available at: https://www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-S...

International Community is struggling: the difficulty in identifying widely recognized red lines and humanitarian norms applicable to the use of force in cyberspace and in establishing a cyber armament control regime.

As we never abandoned a nuclear security paradigm that postulated that "the only way to win is not to play", we are, in the cyber domain, drifting toward one where – so we are told – "the only way to win is to persistently engage the adversaries". The ultimate goal of this persistent engagement is "to improve the security and stability of cyberspace" and to avoid escalations in the conventional domain "by clarifying the distinction between acceptable and unacceptable behavior in cyberspace"[8]. We all subscribe to those goals. The purpose of this Dossier is to contribute to the debate on the military transformations required in order to seize them, and to draw the attention to the security implications that these transformations will have on international relations.

[8] *The Command Vision for US Cyber Command*, p. 6.