CYBER DEFENCE, DISRUPTIVE TECHNOLOGIES AND RESILIENCE IN THE 21ST CENTURY

Brigadier General Mihai BURLACU

Chief of Communications and Information Technology Directorate

In an age where technological competition seems to have become fiercer than ever, cyberspace is increasingly one of the main Smart Power vectors for initiating and conducting hostile actions. We are now part of a global society in which Technology has radically changed our daily behaviour and expectations regarding the access to information or digital services. Moreover, Digital Transformation represents the way in which we systemically adapt to the contemporary military operations requirements. The fact that cyber-type attacks have become an everyday phenomenon, whether we refer to the economic, social or military environment, confirms how powerful the asymmetrical, cyber-integrated influence has become in our defence and security environment.

When the issue of cyber capabilities was addressed for the first time in NATO, in 2002, it was taken into account, in terms of the information environment vulnerabilities and risks, a set of technical requirements, in line with the need for the development of the hard military power instruments by adopting and integrating the cyber component into the operational field. Currently, cyberspace has become essential to the strategic engagement in deterrence and defence. The continued political and military success of the Alliance and its ability to fulfil its core tasks increasingly rely on the rapid adoption of digital technologies. It is estimated that the advantages gained and maintained by NATO could be menaced in the 2030s if the member states do not take immediate actions to preserve the technological superiority, which is contested by the efforts and energy of strategic competitors and potential adversaries having an autocratic nature. The mentioned actions require for the Allies to make significant investments in developing and integrating new digital capabilities. In this way, NATO's Digital Transformation will allow for the Alliance to conduct integrated multi-domain operations/MDO, to enhance interoperability across all operational domains, to optimise warning, alert and response capabilities for different types of threats, to facilitate political consultations as well as the decision-making process based on relevant data/information. Thus, to a very large extent, the dependencies on the cyberspace, combined with the physical and electromagnetic one, as an operational environment, become critical in the future military confrontations or actions.

The evolution of the cyber domain has been marked by several important events, such as: the recognition by Allies of cyber defence as part of NATO's core mission of collective defence in 2014, the reconsideration of cyberspace as a domain of operations in 2016 and, most recently, a new NATO cyber defence policy in 2021.

Cyberspace is a unique domain where technologies, including emerging and disruptive ones, play an extremely important role. The mentioned technologies can generate both opportunities, for those in a position to defend themselves in cyberspace, and vulnerabilities, which can be exploited by attackers. In this regard, the analysis conducted by NATO's Allied Command Transformation regarding cyberspace – Cyberspace Strategic Foresight Analysis – highlights the fact that potential competitors and adversaries will increasingly include operations in this domain in their own warfare strategies, especially to respond to hybrid or information operations. Thus, taking into account the anticipated technological advances for the next ten years, it is very likely that the actors in the international arena, state and non-state entities, will optimise their cyber-attack-related capabilities.

Furthermore, the mentioned document identifies the relevant emerging and disruptive technologies, either as a threat or as an opportunity, as follows: artificial intelligence, quantum technologies, 5G communications, the expansion of smart cities, cloud, blockchain, Software Defined Radios and Zero Trust Networks. In this regard, response options are also suggested, being promoted the adoption of a new multi-level approach to different technologies, depending on the stage of their development – embryonic, incipient, mature, which can be exploited by NATO member states as well as by potential adversaries, and technologies already existing in NATO. Among the suggested response options, articulated on the four levels, the following are mentioned: observation and monitoring, research and experimentation, immediate adoption and implementation, maintenance and optimisation of existing programmes respectively.

It is evident that the power provided by the cyber domain generates means of influence for state and non-state actors alike. However, the limits of that power *are under constant evaluation, as are the key concepts of NATO. There are currently active debates whether the notion of "cyber deterrence" can be applied similarly to the traditional domains (land, air, sea and space). Cyberspace is constantly contested at different levels, making it an area where deterring or defending against any hostile activity is nearly impossible to predict and extremely difficult to achieve.*

However, as part of collective defence, under the Alliance's core missions, a serious cyber-attack on one ally could be treated as an attack on all, thus triggering Article 5 of the North Atlantic Treaty. There are no predefined thresholds regarding the response to such an attack. NATO must strengthen its defensive mandate from this perspective so that it could be ready to respond to a cyber-attack even when Article 5 is not invoked. It is the same with all member states..., each one individually has to develop its infrastructure so that it can meet and respond to such a challenge.

To that end, NATO can serve as a platform for connecting and disseminating the lessons learned among Allies, facilitating the consultation policy and the initiation of collective actions in response to cyber-attacks. Cyberspace is often exploited by adversaries for the purpose of disinformation and propaganda – forms of soft power hybrid threats that further complicate the security environment, as they are intended to undermine societies from the inside by influencing decisions at the institutional level. Therefore, maintaining competitive advantage, in a world where the international norms and laws governing cyberspace are constantly challenged, is more crucial than ever.

The war in Ukraine confirmed that the Russian Federation is capable and very active in cyberspace, resorting to full spectrum attacks and destructive actions in pursuit of its strategic objectives, with lower or higher intensity, not only in the period preceding the conflict but also in the demonstrative support or in the actions complementary to the kinetic ones. Russia has carefully prepared the cyber battlefield by securing early access to critical networks and infrastructure. Throughout the crisis and the conflict, Russia has exploited those previously identified vulnerabilities as part of a coordinated cyber campaign that includes exfiltration tactics as well as an unprecedented number of destructive malware variants. They have had multiplicative effects, being propagated outside Ukraine, including in NATO member states (e.g., damage to Viasat services), highlighting Russia's determination to accept risks with unpredictable cascading consequences.

Although resilience remains a national responsibility, NATO Allies have analysed a set of basic requirements, which can be used by each state to assess its levels of resilience. The requirements relate to vital public services, including energy supply, transport and telecommunications networks, healthcare, critical infrastructure, food and water resources – all components being necessary for both integrated crisis management and defence operations support. Moreover, ensuring the security of cutting-edge telecommunications networks will be even more important with the integration of 5G networks, as they become *the foundation of existing and new technology ecosystems that can radically transform the concept of security. As most of our devices and interactions are digitalised, the connection between cyberspace and emerging and disruptive technologies (EDTs) will expand. In other words, there will be new ways to disrupt societies and the rules-based international order. Therefore, the rules and norms must be adapted so that societies can face the change of the strategic environment in relation to the technological advances.*

In Romania, the deterrence and defence posture with regard to concerted cyber-attacks targeting national critical infrastructure requires a higher level of inter-agency cooperation, especially at the level of Cyber Operations Centres and of the entities involved in incident management, a sustained and structured cooperation with the private sector, which calls for engagement based on long-term established public-private partnerships and superior integration of efforts to develop a common operational picture and cyber situational awareness at the political, military and technical levels. An active deterrence posture in cyberspace also requires the preparation of capabilities that produce effects in the networks and critical infrastructure of potential adversaries, based on a digital force ready to intervene in cyberspace, highly skilled, motivated and encouraged by assertive cultural change and appropriate leadership that can recognise performance and innovative qualities, support experimentation in the data exploitation and integrated management, as well as the development of the ability to take calculated and well-informed risk.

In conclusion, technological progress can have major military implications, in terms of changing the nature of war and the character of conflicts. As a result, it is expected that the future Alliance operations will be conducted in a completely different framework than the traditional one. The implementation and continuous development of the fifth domain of operations, represented by the cyberspace, favours the emergence of new centres of power whose objectives can be interspersed with different areas of interest and can lead to new conflict situations both in the real environment and in the virtual one. Last but not least, the cyber environment represents the modern vector of designing the conditions necessary to be met in order to obtain a higher level of Smart Power, related to the specificity of the current reality challenges.

Thus, in order to be able to adequately respond to technological threats, it is necessary for security and defence decision-makers to focus on the activities of developing capabilities and planning operations at the three levels – strategic, operational and tactical, in the medium and long term. Romania, alongside the other NATO member states, is implementing the related measures, so that it can contribute to the collective defence effort as well as to NATO defence and deterrence posture, especially in the eastern flank, where it is located the Wider Black Sea Region, having its particularities, generated, first of all, by its geostrategic position, while being aware of the effects of the technological progress on the confrontations in cyberspace.