SHAPING THE OPERATIONAL ENVIRONMENT THROUGH CYBERATTACKS

Lieutenant Colonel Marian ȘTEFAN

Defence Intelligence Training Centre, Bucharest

The current geopolitical and geostrategic context, the scale of politics, economics, culture and religious interests, information and cyber problems, the global medical crisis, as well as other non-military measures nowadays occupy a special place in shaping the operational environment. Their importance is felt not only during the escalation of crisis situations and their management and control, but also in military operations, marking the architecture of contemporary conflicts. A variety of present and involved actors, together with the multitude of risks and threats they generate, change the paradigm of the classic operational environment, towards multidimensional operational approaches in relation to the five traditional dimensions we are already familiar with from the military literature: land, air, sea, space and the electromagnetic spectrum, to which now the environment and the information environment are added. Overlapping these environments and creating an integrated battlespace image is a paradigm shift that must be understood and assumed. Social platforms and information warfare, artificial intelligence and self-learning programmes used in the military environment redefine the future security environment and the operation environment both in peacetime and in situations of crisis or at war.

This study proposes a holistic presentation of the problems and challenges at the level of the international operational environment, presenting different typologies of threats identified at the level of the informational component by instrumenting cyberattacks attributed to state and non-state entities. The shaping of theoretical concepts is accompanied by a series of examples presented in order to provide a detailed perspective on events that have affected the information environment.

Keywords: environment operational; cyberattacks; aggressions; crisis; technology;

GENERAL NOTIONS

The broader way of approaching security has lately acquired a new type of components, initially coined *“non-traditional threats”*, and afterwards *“emerging security threats”*, because NATO has considered them to be very important, thus stepping on a new and uncertain territory. This area of threats includes terrorism, proliferation of weapons of mass destruction, cyberattacks, power and power assets supply outages: *“The evolution of international relations, the turmoil and the acceleration of the integration and fragmentation of the World International Order have led to unexpected and unconventional forms and types of threats to national and international security. Some of these threats stem from the process of technological development, others from the impact of technology on our society, others from the growing populism and relevance of identities, and last but not least, the ones generated by our own minds and perceptions, dramatically influenced by our preconceptions and the inclination to seek the easiest ways in rational thinking. All this has an enormous impact on security and national defence threat assessment. Therefore, these factors must be explored, known and addressed in a scientific and comprehensive manner, in order to prevent strategic surprise in these areas, as well as the emergence of new types of conflicts”* (Chifu, 2020, p. 10).

Although the world we live in is constantly experiencing new technological developments, the speed of evolution of our society, international relations and security has created new categories of unconventional threats. In this way, threats from external sources are correlated with internal vulnerabilities that are also transformed into threats. This happens because, in reality, they correspond to the typology of hybrid threats, which are generated by external sources (Chifu, 2018, pp. 23-30). This is the case for all the features of liberal democracy, the values and principles we respect because they represent our way of life, but which are considered vulnerabilities by certain actors (state actors, especially by the Russian Federation and China, and non-state ones, entities and terrorist organisations, organised crime groups), which have built tools to take advantage of them (Chifu, Țuțuianu, 2017, p. 270).

The new types of threats come from speculating on the principles and values of the democratic system of government, taking advantage of the shortcomings and ambiguities identified in these systems, generated by the evolution of technology and its impact on society (Chifu, 2019, pp. 11-23).

Social media and information warfare, artificial intelligence and the use of self-learning programmes in the military environment redefine the future security environment and the operating environment. The most profound changes come from the area of advanced technologies with freedom of action and decision-making.

The geopolitical and geostrategic context, the scope of political, economic, cultural and religious interests, information and cyber problems, as well as other non-military measures occupy nowadays a special place in shaping the operational environment. Their importance is felt not only during the escalation of crisis situations and in the process of crisis management and control, but also in military operations, marking the architecture of contemporary conflicts.

The array of present and involved actors, together with the diversity and scale of risks and threats they generate, change the paradigm of the classical operational environment towards multidimensional operational approaches, in relation to the five traditional dimensions we were familiar in military literature: land, air, sea, space and the electromagnetic spectrum, to which the surrounding environment and the cyber environment are now added. Overlapping these environments and creating an integrated battlespace image is a paradigm shift that must be understood and assumed.

In terms of the traditional approach, US military doctrines extend the list of components of hybrid threats to include *"two or more of the following: military forces, national state paramilitary forces (such as internal security forces, police or border guards), insurgent organisations (movements that primarily rely on subversion and violence to change the status quo), guerrilla units (irregular indigenous forces operating in occupied territory), criminal organisations (such as gangs, drug cartels or hackers)"* placing a strong emphasis on the use of information and cyber operations (TRADOC G-2, 2012, p. 5). This picture of the current operational environment specific to hybrid warfare, including combinations of conventional and irregular forces, provides a perception limited to military warfare tools, along with elements of organised crime and cyberattacks. For a historical study of military campaigns, such an approach may be useful, but to explain the combination of military and non-military power tools used to achieve a state's strategic objectives, this is not enough. The tacit nature of the conflict in cyberspace makes it difficult to distinguish between the origins and triggers and the end state desired by the actors who triggered the aggression.

THE INTERNATIONAL CONTEXT OF THE OPERATIONAL ENVIRONMENT

The global operational environment is characterised by the existence of two main phenomena. First of all, there is an increasingly acute phenomenon of power vacuum generated by states with fragile or failed systems of governance, which, through the vulnerabilities created, enables the rise of non-state actors through their asymmetric or hybrid nature, generates security crises at the state or even regional level. Increasing the number of well-organised, armed and funded non-state actors poses threats to security and sovereignty at the level of weakly governed states. These interferences in the governing act of non-state actors manifest themselves in two ways: on the one hand, they can position themselves as a possible alternative to the traditional form of government based on the rule of law and recognised, but failed state structures, given the taken measures and exercised policies, and on the other hand they can challenge, by the nature of their existence and presence, the monopoly of the force structures of the host state.

The second important phenomenon that manifests itself in the current medium-sized operation is represented by strategic competition (struggle for different resources, markets, areas of influence, geopolitical and geoeconomic interests) between strong states with conflicting interests.

The two phenomena may seem contradictory at first sight, but analysing the details and especially the common elements we find that in fact there is a connection: in situations where instability leads to the breakdown of existing elements of government, a state creates gaps in command structures and so-called *"open doors"* that regional or global powers, regional or transnational non-state entities can exploit to improve their positions or strengthen their influence.

The fragmentation of states was the main concern for international security in the decades after the end of the Cold War. Unlike the tense international security environment that existed during the Cold War, but stable in terms of the foreign policies of the two power blocs, the conflicts of the 1990s and 2000s were perceived as *"asymmetric"*, at least in terms of the use of unconventional elements. Thus, states with inferior and outdated military technical equipment, but innovative and adapted to the context of the operational environment have become formidable opponents for the armed forces of states that spend significant budgets for the defence industry, just because they knew the vulnerabilities of their opponents and managed to exploit them successfully. Although this phenomenon persists, we are now witnessing an increase in hybrid conflicts characterised by situations in which both classical and asymmetric threats are used in a combined manner. Innovative combinations of the use of conventional technologies and the products of new technological advances create a kind of dynamic and unpredictable conflict. The current operational environment blurs the distinction between war zones and peace zones, as well as between legitimate combatants, unassigned opponents and civilians.

One of the most critical dimensions of the hybrid conflict is the countering of military and political efforts at the same time with the overlapping use of information aggression.

Information warfare is usually used in hybrid conflicts to create dissent in the public opinion of the population of the target state, to generate legitimacy of intrusive actions by fabricating a credible pretext, to prevent or slow down the response of the target state to kinetic and non-kinetic attacks and to reduce the chances of external interference by creating situations of legislative confusion. The most successful hybrid campaign is the one that paralyses the institutions of the target state and makes unavailable the ability to resist or react before the forced introduction of force – the nature of which can later be characterised as an instrument of stability (generators of peace and stability) instead of the instrument that created the instability. The control of all classical and modern media channels will lead to the possibility of using them in order to influence the internal public, and given that this control will be achieved from the initial state of conflict or in an incipient form, before any other actions, the effects will be to undermine the will of the target population to withstand further aggression. In situations where topics and messages constructed by the aggressor for the purpose of misinformation and intoxication have to compete with the international press and the unregulated Internet, the specific content of these launched topics is less important than saturating these areas with misinformation to help mask the aggressor's actions.

VULNERABILITIES OF THE INFORMATION ENVIRONMENT – THE TARGET OF CYBER AGGRESSIONS

Conceptually, a complex operational environment is composed of a multitude of actors who interact quickly, in different ways, being highlighted by structural complexity and interactivity. The levers that govern interactions are sometimes ambiguous and can be opaque to external actors without a deep understanding of the context. The characteristics of the conditions in an operational environment are constantly evolving, the information component being the most dynamic.

Part of the operational environment, the information dimension presents complexity, volatility, uncertainty, instability and ambiguity in events that change in speed, pace and tempo. A number of hybrid threats, including cyber-aggression, propaganda and influence, and misinformation spread in virtual environments, can extend the impact of planned military operations. Cyber-attacks pose an increasingly critical threat to information technology infrastructure and the ability to effectively execute a mission command. Any adversary will try to shape an operational environment to his advantage, changing the nature of the conflict and using capabilities for which any military force used is not fully prepared.

An information system, in general, can be defined as the set of elements involved in the process of collecting, transmitting and processing information, which has a central role in this system. The information system includes the following components: spread information, documents carrying information, personnel who have access to information, means of communication, information processing systems (usually, automatic) etc. Some of the activities carried out within this system involve: the acquisition of information from the basic system, the completion of documents and their transfer between different compartments, the centralisation of data etc. In the broadest sense, any information system refers to the various interactions between people, data, processes, and technologies. In this way, the term does not only refer to the aspects related to information and communication technologies that an organisation uses, but also to the way in which people interact with the technology in order to provide support for processing processes. The information system represents a complex set of data flows and information circuits organised in a unitary conception.

The development of information and communication technologies over the last 20 years has served as a powerful and accelerating catalyst for changing the distribution of power in the international system, as well as how to use it. The dominance of related technologies is increasingly changing the physiognomy of the current operational environment, as technological capacity and economic power invested in the military sector are closely linked. The emergence of cyberspace has added new ground for conflicts between states of the world or between non-state organisations. In terms of global governance and the right balance between individual freedom and state control, the challenges are growing as states' monopoly on certain types of information has been eroded in favour of individuals and non-state actors. The technological revolution is disrupting military concepts and doctrines in ways that seem to reduce the contribution of the human factor in the event of conflict and diminish some of the advantages that Western armed forces had at the end of the Cold War.

Information and communication technologies shape all the power tools of states, including diplomacy, information and the use of force. Advances in technology and the digitisation of information have made it possible to collect information more intelligently and the emergence and involvement of a wide range of actors. The existence of a large volume of information stored in databases controlled by large private concerns is inherently viewed as insecure by Western governments, while social media content serves as a repository of personal information about potential information targets that have so far remained untouched for state institutions. The great powers have a significant advantage in controlling information, but any state with a telecommunications agency has the ability to develop ways to collect such signal information – SIGINT. China is a prime example of a state whose information gathering, processing and storage capabilities have been dramatically transformed over the past 20 years through the use of cyber espionage for both commercial and military purposes. Many countries in Africa, Asia and Latin America use improved collection capacities to more effectively monitor or repress dissent among their own populations. Meanwhile, North Korea has used its substantial cyber capabilities to attack both its opponents and its revenue from cybercrime, a case of the theft of US $ 81 million from the central bank of Bangladesh in 2016.

The fact that espionage levels have become so ubiquitous has probably created a new and unprecedented set of circumstances. It has often been observed that when it comes to digital networks, the distinction between espionage and sabotage can only be determined by intention. This is not strictly true, given that any digital exploitation aimed at espionage will necessarily have a specific sabotage component. There will always be a fear that any discovered exploitation – and the average discovery time can range from 146 days in the US to over 400 days in the EU (www.iiss.org/publications/strategic-survey) – can have a sabotage component that is too sophisticated to be easily identified. States are increasingly using their intelligence capabilities (both in the form of state agencies and non-state entities) to penetrate enemy networks in order to identify vulnerabilities that can be activated in time of tension or conflict, in order to affect the functioning of the company itself. Such exploitations may also have a signalling function, designed to discourage states from taking hostile actions for fear of a harmful response.

This is a challenge for decision-makers both in states engaged in cyber espionage and in those that are targets of such activities. The picture is still quite blurry, with the risk of undesirable consequences, as in 2017 NotPetya, a highly virulent ransomware virus, mainly directed against Ukrainian government agencies, spread widely in Australia, Europe, Russia and the US, causing billions of dollars in damage. The CIA has attributed the GRU virus to Russia's military intelligence agency, which appears to have used the conflict with Ukraine as a test ground for a number of cyber exploits. The impact of such exploits highlights the so-called *"connectivity paradox"*, whereby the most advanced network-dependent technologies are also the most vulnerable to significant cyber disruptions.

Such disruptions are becoming a familiar part of a new approach to competition between states, in the form of what has been called grey area operations. These operations were described by the US Special Forces Command as *"a competitive interaction among between and within state and non-state actors that falls between the traditional war and the state of peace"* (Special Operations Forces within the Competition Continuum, 2020). They are characterised by ambiguity about the nature of the conflict, the opacity of the parties involved and uncertainty about the relevant policies and legal frameworks. There is nothing intrinsically new about such operations, but the development of technologies has greatly facilitated them, allowing actors to undertake (at low cost and with the possibility of denying) a series of activities that cause damage without amounting to a level that would easily justify a kinetic response. An example of this type of operation is the attacks by entities that acted on behalf of the Iranian state between 2011 and 2013 against the US banking and financial system, undertaken in response to US sanctions related to the Iranian nuclear program.

The most eloquent example is Russia's alleged interference in the 2016 US presidential election, which focused on the exploitation of social media platforms. Russians claiming to be US citizens have opened a large number of fake social media accounts, predominantly on social media platforms Facebook and Twitter. These accounts were used to spread messages focused on social issues at the time, which were then amplified by robots (software applications that perform simple repetitive tasks at a much faster rate than humans can). This created the impression of a real national debate on certain issues of interest, from immigration and racial issues to the behaviour of candidates in the election campaign. In this way, American politicians felt compelled to address the issues of debate and the traditional media in order to fill the void of credible information, thus creating a further amplification of false propaganda. A few days before the election, Russian hackers also tried to hack into the US voting systems by sending malware-infected emails to state election officials' computers.

The objectives of this Russian campaign evolved from an initial intention to discredit one of the presidential candidates and to generate distrust in the US political process to promote the candidacy of the other politician, considered the most suitable person to raise or lower sanctions on Russia. This approach exemplifies the Russian concept of reflexive control, defined as *"a means of transmitting to a partner or adversary information specially prepared to voluntarily incline him to take the predetermined decision desired by the initiator of the action"* (Kowalewski, 2017). In fact, it has allowed Russia to cause significant damage to the integrity of the US democratic process at minimal cost by digitally exploiting existing cracks in American society, using computer systems available to the general public and home users. Although the US government was well aware of what was happening and who was responsible, its ability to respond to such behaviour in a timely manner or to effectively sanction such actions was limited.

Although China has not yet tried to mimic the type of information operations used by Russia, the state has used technological advances in research in this area to expand its influence in a variety of ways to shape the operational environment in its own interests. In the international diplomatic arena, China has taken on the role of supporting the concept of cyber sovereignty and the need for new forms of global governance of the cyber realm. China's cyber operations reflect a continued focus of state intelligence agencies' efforts on espionage, with some coercive intentions as a secondary objective.

Unlike China, Iranian cyber activity is much more focused on retaliation against regional and Western neighbours than serving a direct coercive purpose. Cyberattacks on Saudi oil companies began with a destructive attack in 2012, which destroyed about 30,000 computers in the networks of the Saudi state oil company (ARAMCO), but did not have a noticeable impact on oil operations. In 2017, the same malware caused similar damage to the petrochemical company Tasnee; that attack was followed by a subsequent attack on ARAMCO in August 2017, involving TRITON intrusion malware.

The information environment is a construction based on the idea that the existence and proliferation of information systems create a distinct dimension or operating environment. As a combination of tangible elements (physical information systems and networks) and intangible elements (information and decision-making), the information environment is both a resource for military operations and an environment in which the armed forces operate. In any operational environment, the intangible element, information, is of paramount importance. This is because, despite its lack of physical existence, the content and flow of information in a specific geographical area produce real, tangible effects on the physical world and on the military forces present in the operating environment. For these reasons, the understanding of the information environment must ultimately include how the content and flow of information affect the conduct of military operations.

Finding the author of cyberattacks is difficult, requiring a process of collecting large volumes of information, analysing them, and making a decision to identify who is responsible. Very rarely do the traces left by a cyberattack provide clear evidence for IT specialists so that the source of the attack, either a state institution or a person, can be indicated in order to be able to provide evidence in a court of law.

The proliferation of information and communication technologies, both in terms of the widespread use of these technologies and the increased availability of destructive means, have generated new ways of projecting power tools (Paleta et al, 2008). Political and economic differences between states now involve solutions through cyberattacks on the utilities, financial networks, electoral infrastructure and governance systems of other countries. Cyberattacks that involve the deliberate use of a software product specially designed and targeted to exploit or modify computer code, data, or algorithms to cause damage provide new ways to target Internet infrastructure, telecommunications networks, information systems, and computers and computer systems. Such activities could be aimed at destroying or affecting the proper functioning of these systems with negative effects on their users, whether they are states, companies, public service providers or individuals.

CONCLUSIONS

The United Allied Doctrine for Information Operations defines the information environment as one that *"includes information, actors and systems that allow the use of information"* (AJP-3.10, 2009, p. 1-1). In this context, the information environment has become the system in which entities, means of communication, communication systems and volumes of data transmitted act simultaneously for a single purpose, communication. The distances between information generators and receivers or users have dissipated with technological development, so that the ideas promoted by anyone in the virtual environment can be accessed instantly by using a wide range of terminals or computer systems, thus becoming a global issue. The global information environment has the advantages of advanced technologies, offers unlimited access to resources, but is a vulnerable space in the face of cyber aggression. Basically, this double-edged sword offers government entities and individuals as well niches of penetration and ways to convey data of a disinformation nature. *"Information warfare, according to a definition of the concept, is the creation of alternative realities by perverting the truth based on real data, facts and arguments and interpreting it by using a combination of facts, syllogisms, sophistry, propaganda, forced interpretation and a multitude of lies. Alternative reality perverts the perception of a target population, in a combination of psychological operations – PSYOPS, along with misinformation and propaganda, using fundamental beliefs, feelings and strong images, in order to lead the target audience to a pre-defined perception"* (Chifu, 2015).

BIBLIOGRAPHY:

1. Chifu, I. (2015). *Război hibrid, Lawfare, Război informațional. Războaiele viitorului*. "Strategii XXI" International Scientific Conference. "The Complexity and Dynamism of the Security Environment". Bucureşti: Centrul de Studii Strategice de Apărare şi Securitate.
2. Chifu, I., Țuțuianu, S. (2017). *Torn between East and West: Europe's Border States*. London and New York: Routledge Publishing House.
3. Chifu, I. (2018). *Războiul hibrid şi reziliența societală. Planificarea apărării hibride*. In *Infosfera Review*.
4. Chifu, I. (2019). *Technology and Democracy. The Impact of the Evolution of Security and International Relations*. In "Strategii XXI" International Scientific Conference. Strategic Changes and International Relations. Bucureşti: Universitatea Națională de Apărare "Carol I".
5. Chifu, I. (2020). *Ameninţări neconvenţionale și noile tipuri de conflicte de natură hibridă în secolul 21*. In *Gândirea militară românească* Journal, no. 1.
6. Kowalewski, A. (2017). *Disinformation and Reflexive Control: The New Cold War*, https://georgetownsecuritystudiesreview.org/2017/02/01/disinformation-and-reflexive-control-the-new-cold-war/, retrieved on 17 August 2020.
7. Paleta et al. (2008). *Information Technology and Communication and Best Practices in IT Life Cycle Management*. In Journal of Technology Management & Innovation, vol. 3, no. 4.
8. Williams, P. (2008). *Violent Non-State Actors and National and International Security*. International Relations and Security Network. Zurich: Swiss Federal Institute of Technology, http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?id=93880, retrieved on 15 August 2020.
9. AJP-3.10, *Allied Joint Doctrine for Information Operations*, 2009.
10. *The Global Risks Report 2016*, the 9th edition, http://www3.weforum.org/docs/GRR/WEF_GRR16.pdf, retrieved on 10 June 2020.
11. *The Impact of the ICT Revolution on International Relations* (2018), www.iiss.org/publications/strategic-survey, retrieved on 12 August 2020.

12. *Special Operations Forces within the Competition Continuum*, https://www.doctrine.af.mil/Portals/61/documents/Annex_3-05/3-05-D03-SOF-Competition-Continuum.pdf, retrieved on 13 August 2020.

13. TRADOC G-2. (2012). *"Operational Environments to 2028: The Strategic Environment for Unified Land Operations".*

14. https://www.iiss.org/publications/strategic-survey/strategic-survey-2018-the-annual-assessment-of-geopolitics/ss18-04-strategic-policy-issues-2, retrieved on 11 June 2020.

15. https://www.globalpolicy.org/nations-a-states/failed-states.html, retrieved on 11 June 2020.