AN ANALYSIS OF THE CYBER DIMENSION IN HYBRID OPERATIONS

Cătălin CIOACĂ*, Aurelian RAȚIU, Marian COMAN****

*”Henri Coandă” Air Force Academy, Braşov, Romania (catalin.cioaca@afahc.ro)
**”Nicolae Bălcescu” Land Forces Academy, Sibiu, Romania
(ratiu.aurelian@armyacademy.ro, coman.marian@armyacademy.ro)

DOI: 10.19062/1842-9238.2019.17.2.4

Abstract: *The accelerated technological advances in the field of communications and information systems have produced profound changes in society. Over time, these changes have become prerequisites for good functioning. Moving the area of interest into the virtual space generated by cyber infrastructures represented a migration of threats. Thus, the possibility of remote control of cyber infrastructures, both in peacetime and in conflict, has generated a new type of infrastructure for the national defense system – the critical military cyber infrastructure. Significant contributions are made to the proactive management of critical infrastructures by developing a multi-level architecture model of active cyber defense in the context of hybrid threats.*

Keywords: *hybrid operations, active cyber defense, military critical cyber infrastructures, antifragile*

1. INTRODUCTION

The integration of information and communication technologies (ICTs) in all organizational levels, as an essential condition for progress, has taken the form of "technology push" programs in the military operational field in order to remove the fear of being "left behind".

The notion of cyberspace is not new (Gibsonian Cyberspace) [1], but further developments in the field of ICTs have determined its definition in terms of transversality in relation to the aerial, ground, maritime and space operational environments.

If the traditional military dimension of the national security is national defense, cyber security is an important support for ensuring national security by interconnecting all its domains: national security, critical infrastructure protection, civil protection, public and constitutional order [2].

In this context, cyber defense consists of the set of proactive and reactive measures, military and civilian, which contribute to maintaining the state of normality in the cyber space [3]. The state of normality is disturbed when cyber threats are manifested. Thus, cyber-attacks are persistently initiated throughout the duration of the political-military crises, but also during peace time.

The favorite target of cyber-attacks is represented by the critical assets in the field of ICT (e.g. computer systems, networks, computer programs, electronic communications networks), also known as the critical cyber infrastructure. Criticality is associated with an element or network of elements essential to maintain vital societal functions [4].

The complexity and diversity of both critical cyber infrastructures and cyber threats, involves the development and application of specific complementary protection and resilience measures [5], integrated with the risk management process. The resilience of critical cyber infrastructures, in terms of maintaining the functionality when producing shocks and adapting to changes in the action environment, is possible by following the next principles of risk management [6]:

- the risk cannot be completely eliminated;

- the nature of risk perceptions and behavioral biases should not be ignored;

- a diversified portfolio of measures contributes to efficient risk management and resource efficiency;

- threat identification and risk assessments represent a critical input to the decision-making process;

- risk communication is a critical aspect at organizational level.

Estimating the risk of a cyber-attack on a critical infrastructure is a continuous and complex process capable to identify possible threats, their evolution in terms of probability of manifestation and possible consequences, vulnerabilities and measures to counteract the effects (FIG. 1).

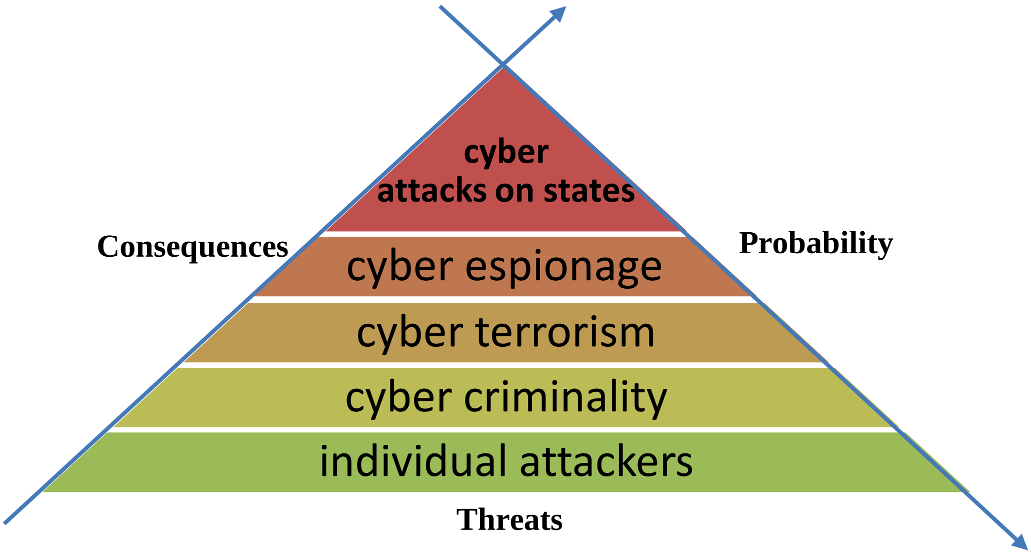


FIG. 1 Elements of risk analysis

A cyberattack on a state can be carried out in peacetime (e.g. Estonia, 2007), before the escalation of a crisis (e.g. Ukraine, 2014) or simultaneously with the military aggression (e.g. Georgia, 2008). Thus, the delimitation between cybercrime actions and cyber attacks as acts of war is difficult and depends more on the context (the crisis' position on the evolution curve).

The risks in the cyber space proliferate due to the interconnected and dependent infrastructures. The management tools and responsibilities must be designed in an integrated manner.

There are enough arguments to declare that cyber security has become the biggest concern of security structures/ organizations, overcoming terrorism. The analysis of the institutional responsibilities in the field of cyber security emphasizes the two-dimensional integrated approach by purpose: good governance (during peace/ stability time) and cyber defense (in crisis situations). Thus, Table 1 shows the main institutions and associated responsibilities at national level from the perspective of good governance [6].

Table 1. The national cyber security system

Institutions	Responsibilities	Priorities 2018
Cyber Security Operative Council (COSC)	-coordinating actions at national level to ensure cyber space security	- ensuring inter-institutional cooperation; - intensifying cooperation actions with international partners
National Center for Response to Cyber Security Incidents (CERT-RO)	- develops and disseminates public policies to prevent and counteract cyber incidents	- the development of technical and human capabilities; - adopting the institutional framework to the new requirements imposed by transposition into national law
Cyberint National Center (CNC)	- managing information capacities to provide beneficiaries with the information they need to prevent, limit and/ or stem the consequences of cyber aggression on national critical infrastructures	- Internet control for the knowledge, prevention and counteraction of Romania's vulnerabilities, risks and threats to cyber security

The Supreme Council of National Defense (CSAT) is the institution that coordinates the activity of the National Cyber Security System (SNSC), and within it, the institutions represented in the COSC develop an intense cooperation with the international institutions in the field of competence [3].

From the operational perspective, cyber defense is the attribute of the Ministry of National Defense, which: defends the cyber systems and infrastructures belonging to the Ministry of National Defense (through the National Technical Center for Cyber Security Incident Response CERTMIL-CTP); plans, conducts and executes operations in the cyber space (through the Defense Staff); ensures cooperation and exchange of information with NATO military entities [7].

At the allied level, the new concepts and policies in the field of cyber defense initiated at the 2014 Summit were perfected in Warsaw in 2016, when the cyber space was recognized as an operational area, as a part of the collective defense, also in the hybrid context. Thus, the cyber defense began to be integrated in the operations planning at all levels (new Cyber Operations Center operational from 2023), the use of the cyber capabilities of the alliance being realized in compliance with the provisions of international law. [8]

NATO Computer Incident Response Capability (NCIRC) is the specialized structure to continuously protect the networks used by NATO. In order to develop and maintain capabilities at national level, cyber defense has also been integrated into the Smart Defense projects (MISP, Smart Defense Multinational Cyber Defense Capability Development - MNCD2, Multinational Cyber Defense Education and Training - MNCDE & T).

Immediate priorities for the alliance are: strengthening cyber security of national infrastructures and networks (Cyber Defense Pledge), as well as enhancing complementary inter-institutional collaborations in the sense of integrated cyber security (by avoiding unnecessary duplication of effort). NATO-EU collaboration is particularly important in this area in order to achieve the "fit for the future" goal. Thus, the foundation of the Center of Excellence for Hybrid Threats, the signing of the EU-NATO Joint Declaration of Cooperation and the signing of the NATO-EU Technical Cooperation Agreement, are three initiatives aimed at finding solutions, exchanging information and good practices, and at coordinating the actions meant to ensure the cyber defense.

At European level, with the adoption of the security and defense plan (2016), the foundations of permanent structured cooperation (PESCO) were laid, and a first set of 17 collaboration projects that respond to training, development capabilities and operational availability needs have been initiated since 2018.

Romania has established responsibilities for 5 of the 17 projects, one of them being "Teams for rapid response and mutual assistance in the field of cyber security", a project coordinated by Lithuania.

In the case of good governance, as well as for cyber defense, managing these dynamic cross-border and trans-organizational threats involves: trained human resources; a consistent approach to cyber defense capabilities in an allied environment; coordinated response actions.

2. THE CYBER DIMENSION OF HYBRID ACTIONS

At the beginning of the 21st century, the use of the term "hybrid" became a common way to describe the contemporary war, at least from two arguments: the increasingly important role of non-state actors in the dynamics of the security environment and the escalation of cyber operations.

Debates over the concept of *hybrid warfare* have shaped at least two sides: on the one hand, there are specialists who consider hybrid warfare a reality that needs its own approach, and on the other, those who claim that hybrid warfare just defines something that has existed throughout the history of the war.

Thus, it is not surprising that there are many definitions of hybrid warfare. The concept has been shaped in different ways, and these definitions have evolved in a relatively short period of time. Defining hybrid warfare is not just an academic exercise. The way the concept is defined leads to the outline of threat perception and the proactive and reactive manner of action. For this study, we considered three conceptual approaches to hybrid warfare, whose chronology fit the Crimea 2014 moment (Tab. 2).

Less than 7 years after the onset of the crisis in Ukraine, a conceptual approach of the two approaches is outlined, in the sense that:

- the traditional and irregular war is sufficient to describe the current and future operational environment;

- each conflict has its own particularities (in terms of the methods used to exploit the adversaries' vulnerabilities).

Table 2. Definitions of hybrid war

Definition	Author
Threats that incorporate different combat modes, including conventional capabilities, irregular tactics and formations, terrorist acts including violence and coercion, driven by a variety of non-state actors.	Hoffman, 2007 [9]
Using military forces in an auxiliary way to non-military tactics to achieve strategic and political goals amid the creation and exploitation of an environment of worry and permanent conflict.	Gerasimov, 2013 [10]
Using military and non-military instruments in an integrated campaign, designed to surprise, take advantage of the initiative.	The Military Balance, 2015 [11]

The inductive analysis of the operations that Russia has carried out in Crimea and Eastern Ukraine outlines four main stages of the crisis, each of them divided into sections, but without considering a linear development (FIG. 2).

According to some experts, from a chronological point of view, the hybrid operations carried out during the crisis in Ukraine covered only the escalation phase of the crisis, from the second half of February to the second half of May 2014 [12].

According to the presented definitions, the synchronized and coordinated use of power tools (military, political, economic, civil and informational), alternatively or coupled, with varying intensities, was encountered throughout the crisis [13].

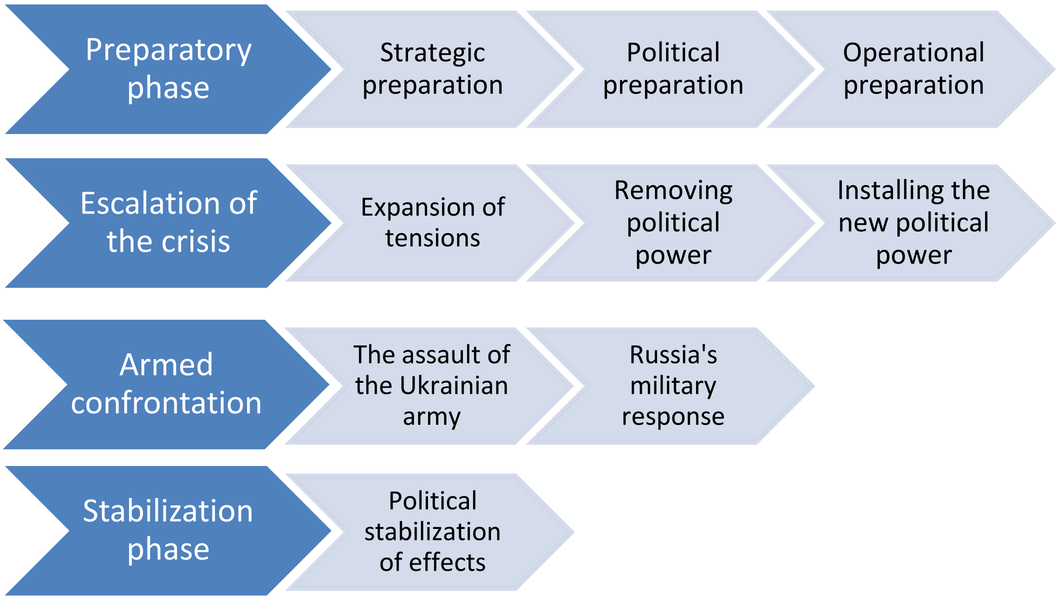


FIG. 2 The stages of the Ukraine crisis

Although it had been successfully tested in the Russian-Georgian conflict of 2008 (when it was used at the same time as the start of military operations), the cyber weapon became the main component of the information instrument in the hybrid war. In Ukraine, cyber-attacks (hacking, denial of service, boot, civilian trolls) were launched before the armed confrontation on both government institutions and the army, with the aim of creating dissensions in society, confusion and imbalance [14].

Russia understood the strategic importance of the cyber space and exploited it beyond the traditional operational capabilities that define the Euro-Atlantic political and military response mechanisms [15]. From the moment of Georgia 2008 to the moment of Ukraine 2014, there is an adaptation of the attack strategies and the targets to the specific objectives (Tab. 3).

Table 3. Features of cyber attacks in Georgia and Ukraine

Attack detail	Georgia	Ukraine
Period	August 2008	February - May 2014
Type of attack	DDoS	DDoS Wipper Bot Physical
Targets	Government agencies Media organizations	government and military websites
Scope	Stopping of communications	Isolation of the region and creation of premises for military operations
Complexity	Simple/ disorganized	Sophisticated/ organized
Context	At the same time with the military operations	before the Crimean invasion and supporting separatists in Eastern Ukraine

Cyber capabilities, within hybrid operations, represent tools at the border between hard power and soft power, with a pronounced offensive character [15].

The cyber weapon can be used not only against institutions with responsibilities in the field of national security (Ministry of National Defense, Ministry of Internal Affairs, Romanian Intelligence Service), but also against other key sectors of the society: financial market, media organizations, science and research, education, health, civil society.

This threat easily crosses the sectorial boundaries in a sequential or simultaneous manner, which leads to a comprehensive approach, based on: common understanding and awareness of the situation; defense planning; efficient leverage of the company's resources; sectorial, national and regional partnerships; lessons learned and best practices.

The inclusion of military objectives/ infrastructure on the target list of aggressive cyber operations by a state using cyber capabilities is the main argument for using the *cyber warfare* concept [16].

3. MODEL OF ACTIVE CYBER DEFENSE ARCHITECTURE

Active cyber defense is a new concept that facilitates the effort unit by integrating, synchronizing and automating cyber defense capabilities across all government networks and critical infrastructure in the US [17]. For this scientific research, in defining the model of active cyber defense in hybrid operations, we used the gradual properties of the cyber systems associated with the three dimensions of the cyber space: technological, informational and socio-cultural (Fig. 3).

The three dimensions of cyber space must be interpreted as a fusion of information systems, the Internet and people in order to create a global virtual domain that provides the premises for competitive advantages [18].

In each dimension, the presence of potential vulnerability factors in terms of cyber security is noted, such as: oversizing investments in knowledge of threats, as compared to investments in protection measures; flexibility in the implementation of standards and sub-optimal use of resources; inadequate human-machine communication; resistance to change.

Resistance is the level of protection against a certain type of threat, being a specific property. Once this capability is developed, the system will avoid the change and risks associated with it, continuing to operate in the same architecture. Resistance also includes elements of redundancy, pending or used concurrently, in order to absorb shocks [19].

Resilience is the ability to adapt in response to the danger of a cyber-attack that allows the system to avoid some potential losses. For this scientific approach, resilient systems contain the following combination of qualities: flexibility, adaptability, inclusivity and integration.

Antifragility, according to Taleb's theory (2014), captures the positive impact of shocks on the system after it has become resilient (adaptable to changes in the operational environment) [20]. Antifragile systems, without the ability to learn from incidents, become fragile over time due to the changes that occur both inside and in the environment in which they operate [21]. Thus, by activating antifragility in the cyber domain, a better understanding of the sectoral interrelationships and the premises for a functional security is ensured.

The properties of active cyber defense can be interpreted in terms of successive levels of capacity (Fig. 4). On the first level, resistance, there are passive defense mechanisms that serve to strengthen and fortify the critical infrastructure. At the next level there are the defense capabilities resulting from the use of defensive cyber weapons and dual-use weapons: communications camouflage, content camouflage, disaster recovery systems. They give the network resilience through adaptation, thus ensuring the continuation of operations despite ongoing attacks.

At the last level, the technical operations of cyber defense are innovative: AI, machine learning, threat intelligence. The resistance and resilience of critical cyber infrastructures ensure their survival by acquiring capabilities with a defensive profile that will lead to reducing the chances of success of a malicious attack.

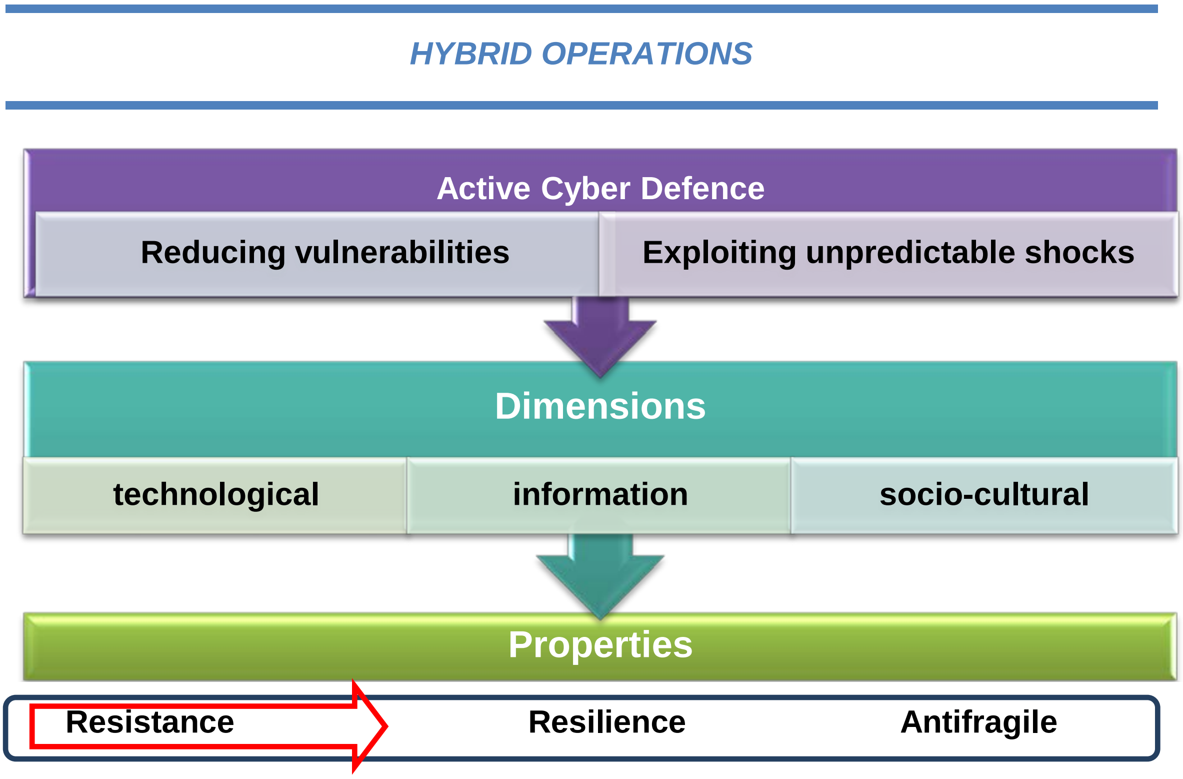


FIG. 3 The architecture of the active cyber defense model

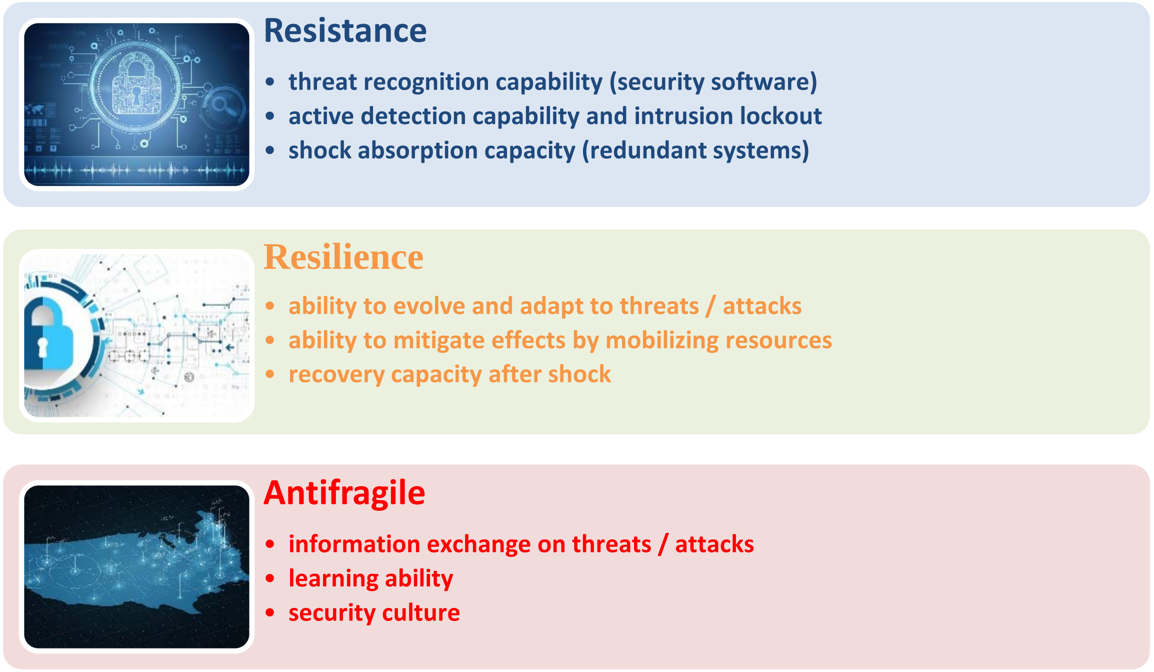
This is achieved technically with the help of: firewall, network monitoring, vulnerability scanning, penetrability testing, encryption, content camouflage, communications camouflage, disaster recovery systems.

These technical measures, though effective against a large register of attacks, are ultimately defeated by innovative exploitation of vulnerabilities, including human factor. The security culture at the individual level represents a combination of experience, knowledge, values and security procedures. The vulnerability at the human factor level is not in the local security environment (eg the government institution), but rather in its manifestation in the virtual social environment, where the constraints are lower.

Therefore, through a strategy of optimal use of resources and unitary implementation of standards, operational efficiency can be ensured. Under the conditions of hybrid operations, the challenge related to the share of cyber defense expenditures, compared to those for high-performance weapon systems, out of the total defense expenditures, is perpetuated.

For the first two levels of active cyber defense, it is essential to develop a model of continuity of services, even in breakdown mode, and the rapid return after attack (eg start redundant systems, identification and blocking of the attack vector). It is also important to establish a framework for identifying vulnerable critical nodes, where enhanced resistance and resilience capabilities are implemented. The dynamic modification of the network configuration through modularity, redundancy and diversity reduces the chances of success of the attack.

The level of antifragility is based on the following pillars: awareness of the benefits obtained by applying the theory of optionality for investments in volatile environments; weak interconnections between nodes to prevent attack propagation [21]; developing technical capabilities for feedback, memory and learning; cyber education and research.



Resistance

- threat recognition capability (security software)
- active detection capability and intrusion lockout
- shock absorption capacity (redundant systems)

Resilience

- ability to evolve and adapt to threats / attacks
- ability to mitigate effects by mobilizing resources
- recovery capacity after shock

Antifragile

- information exchange on threats / attacks
- learning ability
- security culture

FIG. 4 Multi-level capabilities of active cyber defense

Two main arguments have been identified for defining this architecture:

1. the massive expenses in ensuring cyber security led to ensuring the resistance and resilience of the systems, which proved to be fragile;

2. determining the costs associated with the effects of cyber attacks is a particularly difficult task (includes unknown variables or difficult to estimate), without being able to capture the context [22].

Thus, investments to reduce the risk of survival of critical cyber infrastructures are justified, and what must be changed is the share of these investments in relation to investments in innovation. These investments, although made in volatile conditions, create the premises for small shocks benefits/ gains by incorporating learning from continuous change.

It remains valid the hypothesis developed within the concept of interdependent security [23], which shows the contagion of proximity of security (in an allied context, the level of vulnerability of a national network depends on the level of vulnerability of the other members, and at national level, it depends on the level of vulnerability of the different sectors of the critical infrastructure).

CONCLUSIONS

The guarantee of peace suggested by Harari (2018) through the "lost art of winning wars" [24], does not seem as convincing in the case of hybrid operations: the Russian Federation has felt the "taste of victory" and is expected to have a tailor-made behavior.

In critical cyber and cyber infrastructures (which are complex adaptive systems), according to the theory of shocks, the following logical reasoning is outlined: information is transmitted from the system to the component elements through stress factors, volatility means information, and security cannot exist without volatility. The investment projects for active cyber defense of critical infrastructures under the conditions of hybrid actions prove a great potential for bidirectional multiplication of the investment: in financial terms and operationally (performance level).

Through such a security approach, a "cyber 9/11" is not possible: even if the effects are significant, they will not be able to reach the catastrophic level. The ability to gain dominance in the cyber space over critical infrastructures is the key to future hybrid actions, and the RESISTANCE - RESILIENCE - ANTIFRAILABILITY architecture will not only ensure their survival, but will make them stronger.

Future research will lead to the introduction of elements that detail the area of innovative technological impact and the ability to learn from continuous change in an analytical model that captures system shocks (cyber attacks that do not affect its survival) with the help of Poisson distribution.

REFERENCES

[1] Gibson William, *Burning Chrome*, 1982. Available on: http://www.liberatormagazine.com/kiotd/ burning_chrome10272010.pdf (accessed on January 5, 2019);

[2] Udeanu Gheorghe, *Managementul Securității Naționale*, Editura Academiei Forțelor Terestre “Nicolae Bălcescu”, Sibiu, 2012;

[3] Guvernul României, *Strategia de Securitate cibernetică a României*, Monitorul Oficial, Partea I nr. 296 din 23.05.2013. Available on: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/StrategiaDeSecuritateCiberneticaARomaniei.pdf (accessed on January 7, 2019);

[4] Guvernul României, *Strategia națională privind protecția infrastructurilor critice*, Monitorul Oficial, Partea I nr. 555 din 04.08.2011. Available on: http://ccpic.mai.gov.ro/docs/HGR718_2011.pdf (accessed on January 7, 2019);

[5] Cîrdei Alin, *Rolul rezilienței în activitatea de protecție a infrastructurilor critice*. Mircea Boşcoianu şi Dorel Badea Coord., Managementul situațiilor de risc în contextul crizelor de Securitate, Editura Academiei Forțelor Terestre “Nicolae Bălcescu”, Sibiu, 2017;

[6] Sayers P., Galloway G., Penning-Rowsell E., Shen F., Wang K., Chen Y., LeQuesne T., *Flood Risk Management: A strategic approach – consultation draft*. Paris, UNESCO, 2013;

[7] CCS146 – *Securitatea Cibernetică – Securitatea Reţelelor şi a Sistemelor Informatice: “Scenarii şi soluţii privind soluţionarea incidentelor de Securitate – gestionarea incidentelor la nivel national cu potential impact la scară largă”*, 2015. Available on: https://www.comunicatii.gov.ro/wp-content/uploads/2016/02/CyberSec_nov2015.pdf;

[8] NATO, The Secretary General’s Annual Report, 2018. Disponibil la: https://www.nato.int/ nato_static_fl2014/assets/pdf/pdf_publications/20190315_sgar2018-en.pdf;

[9] Hoffman, F. G., *Conflict in the 21st Century: The Rise of Hybrid Wars*, Potomac Insti-tute for Policy Studies Arlington, Virginia, 2007;

[10] Gerasimov, V., *Tsennost Nauki V Predvidenii*. Military-Industrial Kurier, 2013. Disponibil la: https://vpk-news.ru/sites/default/files/pdf/VPK_08_476.pdf;

[11] The International Institute for Strategic Studies (IISS), The Military Balance. The Annual Assessment of Global Military Capabilities and Defence Economics 2015, 1st Ed., 2015, pp. 9-20;

[12] Popescu,N., *Hybrid tactics: neither new nor only Russian*, 2015, Disponibil la: https://www.files.ethz.ch/isn/187819/Alert_4_hybrid_warfare.pdf;

[13] Iordan, O., *Război hibrid şi atacuri cibernetice*, 2017. Disponibil la: https://intelligence.sri.ro/razboi-hibrid-si-atacuri-cibernetice/;

[14] Cristescu, G.A., *Ce a învaţat Georgia în urma războiului cibernetic declanşat de Rusia împotriva sa în 2008 şi cum poate ajuta acum în lupta contra ştirilor false*, Adevărul Internațional, 3 septembrie 2018. Disponibil la: https://adevarul.ro/international/europa/ce-invatat-georgia-urma-razboiului-cibernetic-declansat-rusia-2008-ajuta-lupta-stirilor-false-1_5b8d2479df52022f75158c99/index.html;

[15] Cederberg, A., Eronen, P., *How can Societies be Defended against Hybrid Threats? Geneva Centre for Security Policy*, Strategic Security Analysis, no. 9, 2015;

[16] Ventre, D., *Cyber Conflict: Competing National Perspective*, ISTE Ltd., London, 2012;

[17] Herring M.J. and Willett K.D., *Active Cyber Defense: A Vision for Real-Time Cyber Defense*, Journal of Information Warfare, vol. 13, no 2, 2014, pp. 46-55.

[18] Mbanaso, U.M., Dandaura, E.S., *The Cyberspace: Redefining A New World*, IOSR Journal of Computer Engineering (IOSR-JCE), e-ISSN: 2278-0661, p-ISSN: 2278-8727, Volume 17, Issue 3, Ver. VI (May – Jun. 2015), pp. 17-24;

[19] Bucovechi, O., Badea, D., Oancea, R., Stanciu, R., *Considerations on modelling resilience governance for decision support systems*, University Politehnica of Bucharest Scientific Bulletin Series B-Chemistry and Materials Science, vol. 80, no 2, 2018, pp. 181-192;

[20] Taleb, N. N., *Antifragile: Things that Gain from Disorder*, New York: Random House, 2014;

[21] Hole, K.J., *Anti-fragile ICT Systems*, Simula SpringerBriefs on Computing, 2016, pp. 37-40;

[22] Baxter, L., *An Antifragile Approach to Preparing for Cyber Conflict, Air War College*, Research Report, 2017;

[23] Heal, G. and Kunreuther, H., *IDS Models of Airline Security*, Journal of Conflict Resolution, 49(2): 201–17.

[24] Harari, Y.N., *21 Lessons for the 21st Century*, JONATHAN CAPE, London, 2018, pp. 171-180.