10.53477/2668-2028-21-49

PROTECTION OF CRITICAL INFRASTRUCTURE FROM EMERGING THREATS

Maj. Răzvan ZMĂDU
Major, Romanian Ministry of National Defense
zmadu@hotmail.com

Abstract: *Today's society is in a continuous transformation towards a digitalized society. The COVID-19 pandemic has accelerated worldwide the transition from the physical to the online environment of services provided by both public and private institutions. With a digitized society in our defense types of risks, threats and risks to critical infrastructures that support digital evolution. Thus, opponents turn their attention to new forms of asymmetric attacks to generate states of terror against states or individuals or groups of people. Thus, among the newest and most developed threats are those that use cyberterrorism, network-based warfare or attacks using technologies imported from the military such as drones carrying improvised explosive devices. Countermeasures and resilient systems must be prepared against them.*

Keywords: *critical infrastructures; emerging threats; cybersecurity threats; National Defense Strategy.*

Introduction

In Romania's National Defense Strategy for 2020-2024, one of the national security objectives, from an internal perspective, is "to develop and strengthen the security and protection of critical infrastructures"[1]. In the current climate where the global security environment is characterized by "a high degree of dynamism and unpredictability, as well as an increased globalization of threats and risks, with various manifestations all over the world"[2], where new challenges arise and state and non-state actors use cyber-attacks, terrorism, hostile information or influence practices in new media in order to exploit the limited protection capabilities of governments, critical infrastructure protection is most crucial to for economic and social stability and territorial integrity of states.

History has shown that the attempts to disruption or destruction of critical infrastructures have led to multiple acts of repression. Perhaps the most representative example in recent history is the attack on Pearl Harbor, Hawaii (or Operation Hawaii[3], as it was called by the Imperial Japanese Navy General Staff), on December 7, 1941, which resulted in the entry of the United States into World War II. The terrorist attacks of September 11, 2001 represent an important moment in the development of the concept of critical infrastructure and national and regional strategies and plans for their protection against emerging threats.

In Romania, the term critical national infrastructure (CNI) is defined by O.U.G. no. 98 of 3 November 2010 on the identification, designation and protection of critical infrastructures, as amended and supplemented. Therefore, critical national infrastructure "is both an element, a system or a component thereof, inside the national territory, which is essential for maintaining the vital functions of society, health, safety, security, social or economic welfare of all individuals in society and whose disruption or destruction would have a significant impact at national level as a result of failure to maintain those functions, as well as the identification of national interests, goals, and objectives that are imperative to protect the national interest"[4]. The same legislative act also defines the term critical infrastructure protection as " the unitary

[1] Administrația Prezidențială, *Strategia Naţională de Apărare a Ţării pentru perioada 2020-2024*, 2020, p. 15.
[2] *Ibidem*, p. 19.
[3] Fukudome Shigeru, *Hawaii Operation*. United States Naval Institute, Proceedings, 81 (December 1955), pp. 1315-1331, available on https://apps.dtic.mil/dtic/tr/fulltext/u2/a283376.pdf.
[4] O.U.G. nr. 61 din 27 august 2019 pentru modificarea și completarea Ordonanței de urgență a Guvernului nr. 98/2010 privind identificarea, desemnarea și protecția infrastructurilor critice, art. 3, lit. a.

set of processes and activities organized and carried out in order to ensure the functionality, continuity of services and integrity of NCI/ECI in order to deter, diminish and neutralize a threat, a risk or a vulnerable point by identifying, implementing and maintaining the security, organizational, technical, procedural and other measures resulting from the risk management processes. The CIP includes, in a non-exhaustive list, the activities carried out for the identification and designation of NCI/ECI, the risk management processes, the protection of sensitive information specific to the domain, the implementation of the security plans of the critical infrastructure operators, hereinafter referred to as the OSP, the establishment of the police officers, liaison for ICN/ICE security, staff training, early communication and warning, as well as exercises, reports, OSP viability tests, reevaluations and updates of prepared documents" [5].

According to the Directive EC 114/2008, critical infrastructure protection means „all activities aimed at ensuring the functionality, continuity and integrity of critical infrastructures in order to deter, mitigate and neutralise a threat, risk or vulnerability"[6].

Profile of the emerging threat

Within the context of this article, threats "are the capacities, strategies, intentions, plans that contribute to the increase of threats to critical infrastructures that might be in the form of attitudes, gestures, deeds that lead to imbalance or instability and generate danger impacting national security"[7].

In Romania, critical infrastructure can be affected by a broad range of threats, such as cyber or physical security threats. For example, some facilities are particularly affected by extreme weather events. Considering the climate change, critical infrastructure protection strategies might change in the future and new concepts might be developed in this regard.

Also, major risks for critical infrastructures may result from damage to their equipment through cyber attacks or due to their poor maintenance management.

In the case of emerging threats, in Romania "we are talking about cyber-attacks and hybrid warfare, which everyone perceives similarly, and measures of collaboration and cooperation have been already taken".[8]

In Romania's National Defense Strategy for 2020-2024 there are mentioned the types of security threats in which "hostile actors multiply the tactics of fighting and involvement in the internal affairs of states, comprising hybrid and cyber threats"[9]. The threat is also defined in the same document "as actions, facts or state of affairs, capabilities, strategies, intentions or plans that may affect national security values, interests and objectives and/or may directly or indirectly endanger national security, by affecting the national character, sovereignty and independence, the unity and territorial integrity, the proper functioning of institutions, the life and physical integrity of citizens and community organization."[10]

Emerging threats are defined by "five attributes that arise from the emergence of novel technologies, namely: radical novelty, relatively fast growth, coherence, prominent impact,

[5] *Lege nr. 225* din 1 august 2018 pentru modificarea și completarea Ordonanței de urgență a Guvernului nr. 98/2010 privind identificarea, desemnarea și protecția infrastructurilor critice, art. 3, lit. c.

[6] *Directiva 2008/114/CE* a Consiliului din 8 decembrie 2008 privind identificarea și desemnarea infrastructurilor critice europene și evaluarea necesității de îmbunătățire a protecției acestora, available on https://www.eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32008L0114&from=EL

[7] Protecția infrastructurilor critice, SRI, available on ww.sri.ro/upload/BrosuraProtectiaInfrastructurilorCritice.pdf;

[8] https://www.mediafax.ro/social/conferinta-mas-generalul-gheorghe-savu-atacurile-cibernetice-si-razboiul-hybrid-sunt-amenintari-emergente-pentru-toata-lumea-18430539

[9] Administrația Prezidențială, *Strategia Națională de Apărare a Ţării pentru perioada 2020-2024*, 2020, p. 17.

[10] *Ibidem*, p. 25.

uncertainty and ambiguity"[11]. In Table 1 there are exemplified some emerging threats, corresponding to a specific infrastructure.

Table 1[12]

Emerging Threats Span Multiple Categories Representing Multiple Dilemmas

Categories	Subcategories	Threat Examples
Advanced technology	computing, engineering, human enhancement, manufacturing	Smart dust, 3D/4D/5D printing
Adversarial (human)	Competence, criminality, espionage, terrorism	Active shooter, hostage-taking, aircraft as a weapon
Autonomous systems	AI, robotics	Adversarial machine learning, AI automated attack or hacking, self-assembling robots
Cyber	Encryption, industrial control systems (ICS) and supervisory control and data acquisition (SCADA), internal controls, data confidentiality, network security	Botnets, ICS/SCADA, back doors
Drones	Enhanced UAS capabilities; intelligence, surveillance, and reconnaissance (ISR) capability; operational disruption; payload delivery; swarming	Swarms, micro drones, nano UASs
Health	Hazardous material release, mass illness	Biological food contamination, mass psychogenic illness
Information warfare	Data and identity manipulation, data confidentiality, social manipulation, spoofing	Faceprints, audio fraud, adaptive camouflage
Physical plant infrastructure and utilities	Electric grid, water, wastewater, design planning, malfunction, network security, regulatory	Smart meter attacks, sensor manipulation, utility supply chain integrity, interruption of service attacks
Natural	climate change, disaster or extreme weather	Extreme weather, natural disasters (if exploited by the adversary)
Political	Globalization, international conflict, migration, polarization, social unrest	Disruption of critical infrastructure, social cohesion, and basic government functions, democracy subversion
Smart cities and internet of things	Attack vectors, capacity overload, cascade effect, competence, data manipulation, device integration, network security	5G security, supply chain risks, grid attacks or tampering, manipulation of data analytics systems, algorithms, and signals
Weapons	electromagnetic pulse (EMP), electronic warfare, ISR platforms, projectiles, satellites	Hypersonic weapons, satellite disruption, communication attacks

Globally, there is a change of approach by including in the online environment the activities carried out exclusively in the physical environment. This influences and generates new security policies that should be implemented in all critical sectors, under European Program for Critical Infrastructure Protection - EPCIP. It should be noted that the European Union initiated several processes to harmonize the legal framework for improving critical infrastructure protection after two terrorist attacks in Madrid (2004) and London (2005).

Not only the transfer of certain activities in the online environment online can be a potential risk to critical infrastructures, but also some particular activities in which a mobile application is used. Thus, in 2017, the Strava fitness application that is very popular among sports enthusiasts unveiled the location of military bases around the world, such as Area 51 or

[11] Daniele Rotolo, Diana Hicks and Ben R. Martin, *What Is an Emerging Technology?*, Research Policy, Vol. 44, No. 10, July 7, 2015, p. 1827.

[12] *The End of Sanctuary – Protenting the Army's Installations from Emerging Threats*, 2020, available on https://www.rand.org/pubs/research_ reports/RRA107-1.html.

military bases in Afghanistan and Syria. In Romania, certain military installations could be detected, such as the anti-missile shield in Deveselu, military exercises polygons and Mihail Kogalniceanu International Airport.

In 2015, BitDefender and members within the intelligence services revealed a cyber-attack vector called APT28[13] (persistent and complex cyber threat targeting state-owned enterprises and state institutions), also known as Sofacy, Fancy Bear, Pawn Storm or Sednit through which cybercrime groups from the eastern Europe aimed to collect strategic data from government institutions, renowned politicians, aerospace companies, telecommunication companies, including in Romania.

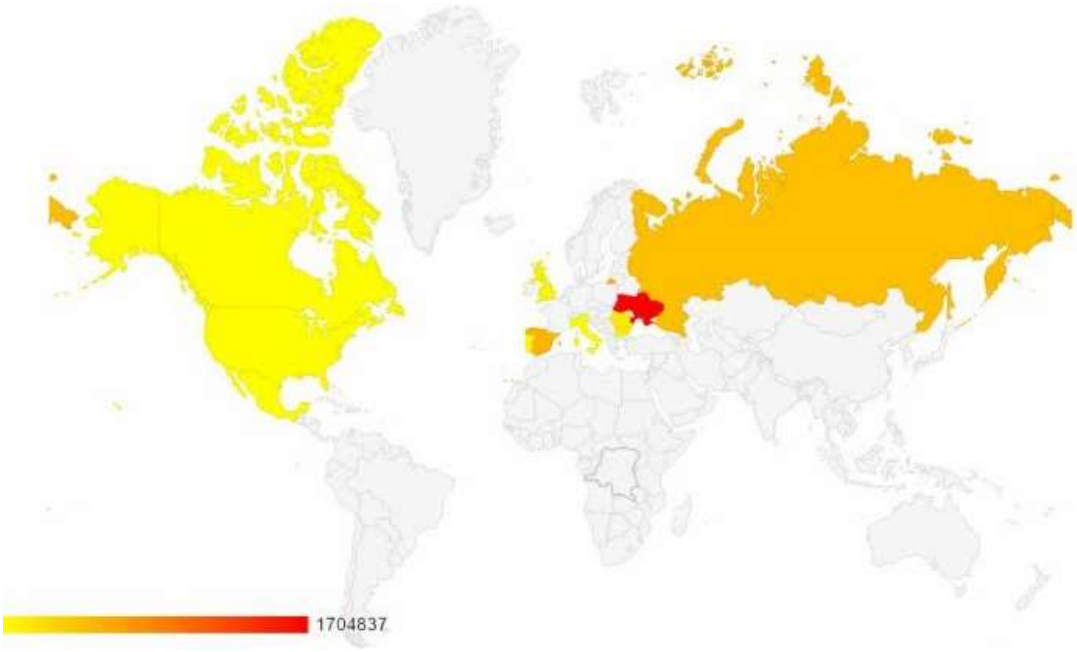

Figure 1 The map of affected countries affected by APT28[14]

Romania has a conceptual, organizational and actional framework necessary for ensuring cyber security and protect cyber infrastructures in accordance with the new concepts and policies on cyber defense developed and adapted to NATO and the European Union. Romania's Cyber Security Strategy is regulated by CSAT Decision No. 16/2013 and GD 271/2013. The internal normative framework of Cyber Security was regulated by Law No. 362/2018 on ensuring a high common level of security of networks and information systems, ensure the harmonization of the national legislation with European legislation in this field and is addressed exclusively to economic operators from important economic categories which are also found in European Program for Critical Infrastructure Protection - EPCIP.

In 2011, the National Cyber Security Incident Response Center - CERT-RO was founded through GD 494/2011. CERT-RO "is the national competent authority for the security of networks and information systems that provide essential services or digital services, designated in accordance with Law no. 362/2018, with subsequent amendments and completions, with regulatory, authorization, attestation, monitoring and control attributions; it includes in its structure a national team that is responsible for preventing and counteracting the

[13] APT (Advanced Persistent Threat), complex cyber threats, popular term after Stuxnet's discovery in Iran's nuclear power plant.

[14] *APT28 Under the Scope – A Journey into Exfiltrating Intelligence and Government Information*, accessed on 15.01.2021, available on https://labs.bitdefender.com/2015/12/apt28-under-the-scope-a-journey-into-exfil trating-intelligence-and-government-information.

incidents that occur within national cyber infrastructures and is the national contact point for similar structures.[15]" "CERT-RO" is also an independent structure for expertise, research and development in the field of cyber-security and critical infrastructure protection.[16]"

In other words, since 2004, The National Alert System has been operating in our country, and from the date of its establishment until today, the level of terrorist alert has been BLUE-CAUTIOUS. The only period when it was decided to raise the level to YELLOW-MODERATE[17] for a period of 30 days was in April 2008, on the occasion of the NATO Summit in Bucharest. In view of these aspects, we can say that the national terrorism threat level in Romania remains low.

The National Center for Coordination of Critical Infrastructure Protection operates within the Ministry of Internal Affairs and its primary goal is to support the responsible public authorities and the owners, operators or administrators of critical infrastructures in our country.

Therefore, we can say that Romania has the necessary mechanisms to prevent and combat emerging threats that may affect its critical infrastructures.

Critical infrastructure protection

The document Multi-Domain Battle: Evolution of Combined Arms for the 21st Century 2025-2040, issued by U.S. Army Training and Doctrine Command (TRADOC) defines a new combat space, namely the strategic support area[18], which is the space where military installations and the communities around them are deployed.

Therefore, this new concept can also be extrapolated to critical infrastructures in other sectors than defense, public order and national security sectors. Thus, the areas around critical infrastructure become a new battleground, which requires Preparedness and Response Planning for the implementation of measures and actions carried out by national institutions to defend themselves against threats of any kind. Critical infrastructure protection plans also contain a variety of hypothetical threats and potential vulnerabilities, and their advantages and disadvantages can only be presented as possible response actions against them.

However, some state and non-state actors are using modern technologies to attack critical infrastructures, such as the placement of explosives using drones or cyber-attacks using artificial intelligence.

The US military has developed a framework that mitigates emerging threats to critical infrastructure (Figure 2). It is staged in six steps, in order to determine and counter emerging threats. Although it looks like a planning process from military books, it can also be used successfully in civil society, only if each step is intended to be coordinated by an independent entity at different intervals.

Thus, in the first step, "*Identify Innovative and Emerging Threats*", there will be established and managed the continuous process for the purpose of identifying ways in which emerging threats can be used against critical infrastructures. It should be mentioned that step no. 1 identifies a threat, but also provides how it might be used and what the destructive effects on critical infrastructure are. The second step, "*Determine Critical Functions and Processes of Army Installation Mission Requirements*", will identify the critical functions and processes that, in the event of an interruption, would reduce the capacity of critical infrastructures to operate at optimal parameters. The third step, "*Identify Key Enablers of Critical Functions*", refers to the identification of critical functions of critical infrastructures, personnel and systems that play

[15] *Regulament de organizare și funcționare a centrului național de răspuns la incidente de securitate cibernetică – CERT-RO*, București, 06.09.2019.
[16] *Idem*.
[17] *The National Alert System has been updated as of March 5*, 2020 by the Supreme Council.
[18] U.S. Army Training and Doctrine Command, *Multi-Domain Battle: Evolution of Combined Arms for the 21st Century 2025–2040*, version 1.0, Newport News, Va.: Fort Eustis, December 2017.

a key role in continuing its mission. Step four is very important, as it involves understanding the existing vulnerabilities in the previous analysis, namely the "*Key Enablers*". In addition, the risks posed by these threats are also estimated. In step five, risk mitigation strategies are developed, and in the last step, activities inspired by the military planning process are performed, such as "*war game*" and "*red team*" activities.

The protection of critical infrastructures can be improved by increasing cooperation and collaboration between national and international national institutions, but also between the population and economic operators who hold critical infrastructures. It should be noted that the protection of sensitive information is an important factor in keeping critical infrastructures operational, data leakage through any means can offer advantages to potential attackers.

Last but not least, the training of those who operate critical infrastructure is essential. Although emerging technologies were introduced later, it should be taken into account that the use of robots and artificial intelligence can lead to more efficient operation of critical infrastructure equipment.

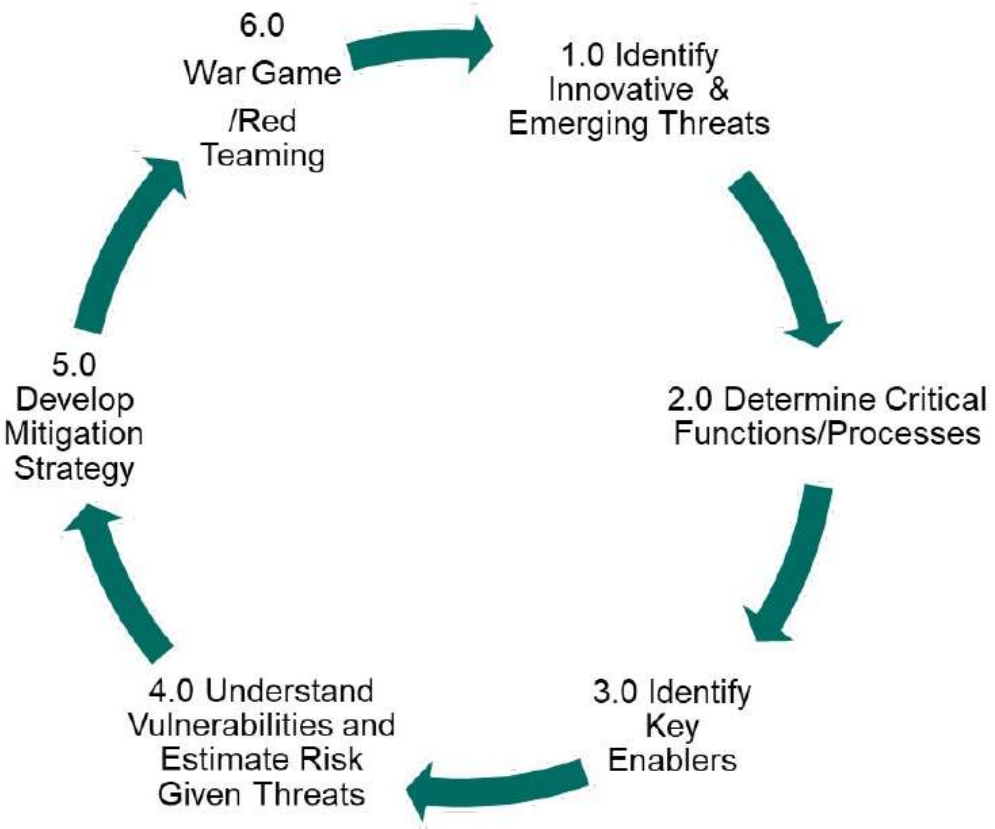

Figure 2 Stages of determining and countering emerging threats[19]

It is well known that modern armies are the first organizations that have standard operating procedures in the case of current known threats. When addressing emerging threats (similar to asymmetric warfare), there needs to be a more comprehensive approach in order to identify and mitigate the risks and vulnerabilities involved.

[19] *The End of Sanctuary – Protenting the Army's Installations from Emerging Threats*, 2020, available on https:// www.rand.org/pubs/research_ reports/RRA107-1.html.

Conclusion

The evolution of society along with technology has influenced the dependence of contemporary society on critical infrastructure. The COVID-19 pandemic has accelerated the electronic transition of many face-to-face services. The Authority for the Digitalization of Romania was found in 2020 and has as primary object to support the digital transformation of Romania's economy and society

The transition to a digital society will also influence the potential threats, vulnerabilities and risks to critical infrastructures, and potential attackers who will develop their capabilities to exploit them.

Therefore, it is necessary to develop protection mechanisms that incorporate resilience measures of critical infrastructure protection through "awareness of the population, public institutions at the central and at the local level and the business environment on the importance of critical infrastructure protection measures for the continuous and safe operation of public utilities and services." [20]

So finally at the end, we can say that the use of emerging technologies poses emerging threats to critical infrastructures.

BIBLIOGRAPHY

1. *Strategia Naţională de Apărare a Ţării pentru perioada 2020-2024*, București, 2020.
2. *The End of Sanctuary – Protenting the Army's Installations from Emerging Threats*, 2020, available on https://www.rand.org/pubs/research_ reports/RRA107-1.html
3. *Investigatie Bitdefender: Romania, pe lista statelor spionate de amenintarea cibernetica „APT28" operata de rusi*, 17 decembrie 2015, available on https://www.bitdefender.ro/ news/investigatie-bitdefender:-romania-pe-lista-statelor-spionate-de-amenintarea-ciber netica-%E2%80%9Eapt28-operata-de-rusi-3095.html
4. APT28 Under the Scope – *A Journey into Exfiltrating Intelligence and Government Information*, 17 decembrie 2015, available on https://labs.bitdefender.com/ 2015/12/ apt28-under-the-scope-a-journey-into-exfiltrating-intelligence-and-government-information/
5. *Protecţia Infrastructurilor Critice – provocarea unei lumi complexe şi interconectate*, 20 martie 2019, available on https://monitorulapararii.ro/protectia-infrastructurilor-critice-provocarea-unei-lumi-complexe-si-interconectate-1-12876
6. *Aplicația de fitness Strava a devoalat bazele militare americane din toată lumea*. Cum apar pe hartă bazele de la Deveselu și Mihail Kogalniceanu, plus poligonul NATO de la Cincu, 29 ianuarie 2019, available on https://www.libertatea.ro/stiri/ aplicatia-de-fitness-strava-devoalat-locatia-bazelor-militare-americane-bazele-de-la-deveselu-si-mihail-kogalniceanu-plus-poligonul-de-la-cincu-pe-harta-2124054
7. *Regulament de organizare și funcționare a centrului național de răspuns la incidente de securitate cibernetică – CERT-RO*, București, 06.09.2019, available on https:// cert.ro/vezi/document/rof-cert-ro
8. *Protecía infrastructurilor critice*, SRI, available on https://www.sri.ro/upload/Bro suraProtectiaInfrastructurilorCritice.pdf
9. Directiva 2008/114/CE a Consiliului din 8 decembrie 2008 privind iden-tificarea și desemnarea infrastructurilor critice europene și evaluarea necesității de îmbunătățire a protecției acestora, available on https://eur-lex.europa.eu/legal-content/RO/TXT/ PDF/?uri=CELEX:32008L0114&from=EL

[20] Administrația Prezidențială, *Strategia Națională de Apărare a Ţării pentru perioada 2020-2024*, 2020, p. 11.

10. *Legea nr. 225* din 1 august 2018 *pentru modificarea și completarea Ordonanței de urgență a Guvernului nr. 98/2010 privind identificarea, desemnarea și protecția infrastructurilor critice*.
11. FUKUDOME, Shigeru, "Hawaii Operation". United States Naval Institute, *Proceedings*, 81 (December 1955), pp. 1315-1331, available on https://apps.dtic.mil/ dtic/tr/ fulltext/ u2/a283376.pdf
12. O.U.G. nr. 61 din 27 august 2019 pentru modificarea și completarea Ordonanței de urgență a Guvernului nr. 98/2010 privind identificarea, desemnarea și protecția infrastructurilor critice
13. *Conferința MAS. Generalul Gheorghe Savu: Atacurile cibernetice și războiul hybrid sunt amenințări emergente pentru toată lumea*, 03.10.2019, available on https:// www.mediafax.ro/social/conferinta-mas-generalul-gheorghe-savu-atacurile-ciber netice-si-razboiul-hybrid-sunt-amenintari-emergente-pentru-toata-lumea-18430539