HYBRID CRISIS MANAGEMENT IN CONTEMPORARY SECURITY: INFORMATION WARFARE AND CYBERATTACKS

Ph.D. Student, Laurențiu-Eduard ION
Valahia University of Târgoviște
laurentiu.ion1992@yahoo.com
Ph.D. Professor, Emil GRĂTIANU
Valahia University of Târgoviște
emil_gratianu@yahoo.com
Ph.D. Student, Ana-Rebeca NEAGU (ION)
Valahia University of Târgoviște
rebecaneagu@yahoo.com

Abstract: *In the context of contemporary security, hybrid crises represent one of the most complex challenges for states and institutions, as they combine conventional threats with non-military forms of aggression, such as information warfare and cyberattacks. This article analyzes the management of hybrid crises from the perspective of the interaction between the digital and strategic-informational dimensions of national security, highlighting how these phenomena influence the capacity to react and institutional resilience. The study starts from the premise that, in the era of accelerated digitalization, states' vulnerabilities are no longer exclusively military or territorial in nature, but extend to information infrastructures, media space and public perception. In this sense, information warfare and cyberattacks become complementary tools of destabilization, which can simultaneously affect decision-making processes, the security of critical infrastructures and social cohesion. The theoretical part of the research is complemented by an applicative component, based on the analysis of hybrid crisis scenarios, in which the institutional response mechanisms, the capacity for interagency coordination and the efficiency of strategic communication in risk situations are evaluated. Examples of massive disinformation in the digital space and attacks on critical IT infrastructures are considered to highlight how these phenomena amplify each other. The results indicate that effective hybrid crisis management requires an integrated approach, which combines technological tools to detect and prevent cyberattacks with advanced strategies to combat disinformation and strengthen information resilience. The study's conclusion underlines the need to develop adaptive security models capable of dynamically responding to the fluid and interconnected nature of contemporary hybrid threats.*

Keywords: *cybersecurity, information warfare, crisis management, institutional resilience.*
JEL classification: *H12, H56, M15.*

1. Introduction

The accelerated transformations generated by digitalization and the development of information technologies have significantly changed the nature of contemporary security threats. Today, states and institutions are no longer faced exclusively with conventional, military or territorial risks, but also with complex forms of aggression that combine informational, technological and psychological tools. In this context, hybrid crises have become one of the most important challenges for national and international security, as they simultaneously use information warfare, disinformation and cyberattacks to affect political stability, the functioning of institutions and social cohesion.

Information warfare and cyberattacks are essential components of contemporary hybrid threats, as they allow state and non-state actors to influence public perceptions, disrupt decision-making processes and make critical infrastructures vulnerable without the direct use of military force. The interdependence between these two dimensions generates complex effects on the reaction capacity of states, highlighting the need for modern and integrated crisis management mechanisms.

Starting from these considerations, the research aims to analyze how information warfare and cyberattacks influence hybrid crisis management and institutional response capacity in the context of contemporary security. The main question of the research is: to what extent does the integration of strategies to combat disinformation with the mechanisms for preventing and managing cyber attacks contribute to increasing institutional resilience and making hybrid crisis management more efficient?

The paper is structured in three main chapters. The first chapter presents the literature on hybrid crises, with a focus on information warfare and cyberattacks, highlighting the main concepts, characteristics and vulnerabilities associated with contemporary security. The second chapter is dedicated to the methodology of research and analysis of hybrid crisis scenarios, evaluating the institutional response mechanisms, inter-institutional coordination and the efficiency of strategic communication. In the last chapter, the discussions and interpretation of the research results are presented, highlighting the need to develop adaptive security models, capable of dynamically responding to current hybrid threats.

2. Specialized literature on hybrid crises, information warfare and cyberattacks

The changes produced in the international security environment have led to the emergence of increasingly complex forms of threats, characterized by the combination of conventional instruments with information and technological means. In this context, hybrid crises represent a major challenge for states and institutions, as they involve the simultaneous use of information warfare, disinformation and cyberattacks to influence decision-making processes and destabilize the social and political space.

The literature highlights the fact that information warfare and cyberattacks have become essential components of contemporary conflicts, as they allow state and non-state actors to exploit digital and information vulnerabilities without the direct use of military force. The development of digital technologies and the expansion of the online space have amplified both the capacity for the propagation of disinformation and the risks associated with attacks on critical infrastructures.

This chapter aims to analyze the main theoretical perspectives on hybrid crises, with a focus on the role of information warfare and cyberattacks in contemporary security, highlighting their characteristics, vulnerabilities and impact on institutional resilience and national security.

1.1. Information warfare in contemporary security

In the context of geopolitical transformations and the accelerated development of digital technologies, information warfare has become one of the main components of contemporary hybrid threats. Recent literature highlights the fact that states and non-state actors use information as a strategic tool to influence public perceptions, manipulate decision-making processes and destabilize democratic societies. Unlike conventional conflicts, information warfare aims to achieve political and social effects without the direct use of military force, by exploiting the informational and cognitive vulnerabilities of the population.

According to Bachmann et al. (2023), disinformation, information manipulation and the propagation of false narratives are essential elements of modern hybrid warfare, being used to influence public opinion and amplify social polarization. The authors point out that information warfare is integrated into so-called "grey zone operations", where the actors involved try to destabilize opponents without crossing the threshold of open military conflict.

In the same vein, recent NATO studies show that information threats have become increasingly sophisticated through the use of artificial intelligence, propagation algorithms and deepfake technologies. NATO Review highlights that information manipulation is used to erode public trust in democratic institutions and to amplify social tensions, especially in states in the vicinity of geopolitical conflicts. At the same time, the organization emphasizes that responding to these threats requires real-time analysis tools and strengthened strategic communication mechanisms (NATO Review, 2025).

Recent literature pays particular attention to the relationship between information warfare and cyberspace. Spaziani (2024) believes that contemporary hybrid warfare combines cyberattacks with propaganda and disinformation to exploit societal and institutional vulnerabilities. The author highlights that the digital environment offers hostile actors the opportunity to conduct operations with high strategic impact and low costs, which makes it difficult to identify and combat threats.

Also, Deppe et al. (2024) introduce the concept of "cognitive warfare", defined as the use of information and digital technologies to influence the cognitive and behavioral processes of individuals and social groups. The study shows that cognitive warfare goes beyond the classic dimension of propaganda, aiming to affect the population's ability to distinguish between real and manipulated information. In this context, social networks and digital platforms become central spaces for strategic confrontation.

At the same time, recent research highlights the fact that disinformation can also be used against critical infrastructures and cybersecurity systems. Alvisi et al. (2024) show that the spread of false information during cyber incidents can amplify social panic, reduce the population's trust in institutions, and make it difficult for authorities to react. The authors argue that information warfare and cyberattacks need to be analyzed together, as they work in tandem within contemporary hybrid threats.

In addition, recent European studies highlight that information warfare poses a direct threat to democratic security. A report analyzed by The Guardian (2024) shows that hundreds of coordinated disinformation campaigns targeting electoral processes, media outlets and vulnerable social groups have been identified in the European space, with the aim of diminishing public trust and amplifying social tensions.

Therefore, the current literature highlights the fact that information warfare has become an essential strategic tool within contemporary security. Its hybrid character, adaptability and interdependence with cyber-attacks generate major challenges for states and international organizations, requiring the development of integrated mechanisms to prevent, combat disinformation and strengthen information and institutional resilience.

1.2. Cyber-attacks and critical infrastructure vulnerabilities

In the context of accelerated digitalization and the interconnection of information systems, critical infrastructures have become increasingly exposed to cyber threats. The literature highlights the fact that sectors such as energy, transport, health, communications or financial systems depend to a significant extent on computer networks and industrial control systems, which amplifies the risk of incidents with a major impact on national security and the functioning of society. Cyberattacks on critical infrastructures are currently one of the most important components of contemporary hybrid threats, with the potential to cause significant economic, social and political disruption.

According to Riggs et al. (2023), the expansion of the integration of information technologies into critical infrastructures has considerably increased the cyberattack surface, which facilitates the exploitation of existing vulnerabilities in industrial systems and digital networks. The authors highlight that modern infrastructures are plagued by issues such as outdated software, lack of network segmentation, and insufficient security measures, which allows high-impact attacks on essential services to be carried out (Riggs et al., 2023).
Maglaras et al. (2018) also point out that critical infrastructures are vulnerable both to direct attacks on information systems and to complex operations that combine technical, informational and organizational elements. The study highlights that protecting critical infrastructures requires integrated security measures, based on institutional cooperation, attack attribution mechanisms, and the development of cyber incident response capabilities (Maglaras et al., 2018).

In recent literature, attention is also focused on the vulnerabilities of cyber-physical systems and automated industrial infrastructures. Oliveira de Sá et al. (2024) show that the use of artificial intelligence and automated attack tools is leading to the emergence of increasingly sophisticated cyber threats, capable of affecting critical infrastructures such as energy grids, industrial facilities and maritime systems. The authors highlight that intelligent attacks on critical infrastructures can produce both digital effects and direct physical consequences on the functioning of essential services (Oliveira de Sá et al., 2024).

At the same time, Maynard et al. (2020) analyze some of the most important cyberattacks on industrial control systems, highlighting their complex and coordinated nature. The study shows that incidents such as attacks on energy networks in Ukraine or Operation Stuxnet have demonstrated the vulnerabilities of critical infrastructures and the difficulty of protecting them from state actors and advanced groups of attackers (Maynard et al., 2020).

In addition to the technical and economic impact, the literature also highlights the psychological and social effects generated by cyberattacks on critical infrastructures. Backhaus et al. (2020) argue that attacks that affect essential infrastructure, such as water or energy systems, can generate strong emotional reactions, panic and diminishing the population's confidence in the ability of institutions to manage crisis situations. In this sense, cyberattacks are perceived not only as technological threats, but also as tools of psychological influence and social destabilization (Backhaus et al., 2020).

Recent studies and institutional reports confirm that critical infrastructures continue to be priority targets for state actors and cybercrime groups. FBI and CISA data show that ransomware attacks on critical infrastructure have increased significantly in recent years, affecting areas such as energy, healthcare, public administration and industrial systems. In parallel, attacks attributed to state-backed groups demonstrate the use of cyberspace as a strategic tool in contemporary geopolitical competition.

The literature reveals that critical infrastructure vulnerabilities are a major problem for contemporary security, as the interdependence between digital systems and the functioning of essential services amplifies the impact of cyberattacks. The complexity of these threats highlights the need to develop integrated strategies for protection, resilience and management of cyber incidents, capable of responding to the dynamic and multidimensional nature of today's hybrid threats.

2. Research methodology and analysis of hybrid crises

The analysis of hybrid crises in contemporary security requires an integrated methodological approach, as these phenomena combine technological, informational, organizational and geopolitical dimensions. Unlike traditional security risks, hybrid crises cannot be understood from a single analytical perspective, but require the correlation of technical data on cyberattacks with their effects on the information environment and on the functioning of critical infrastructures.

In this context, this chapter aims to present the research methodology used to investigate hybrid crises, as well as the applicative analysis of real case studies, relevant to highlighting the way in which information warfare and cyberattacks interact in producing complex destabilizing effects. The focus is on identifying the recurrent patterns of these crises and assessing their impact on the institutional resilience and security of critical infrastructures.

Also, concrete hybrid crisis scenarios are analyzed, selected based on their relevance in the specialized literature and in the reports of the security institutions, in order to highlight the mechanisms of production, propagation and management of these events.

2.1. Research methodology and tools

The present research uses a qualitative approach, based on documentary analysis and comparative case study, specific to the field of security studies. This method allows the investigation of hybrid crisis phenomena by correlating the cyber dimension with the informational dimension, based on real events documented in academic sources, institutional reports and cybersecurity analyses.

The methodological approach is based on the content analysis of official documents developed by organizations such as CISA, ENISA or NATO, as well as on the interpretation of recent academic studies in the field of cybersecurity and information warfare. In parallel, the research uses the comparative analysis of relevant cyber incidents, with the aim of highlighting the similarities and differences between different types of hybrid crises.

It also applies the chronological analysis of the main attacks on critical infrastructures, in order to identify the evolution of the tactics used by the actors involved and to capture how they have adapted with technological development. The interpretation of the data is carried out through a triangulation approach, which combines academic, institutional and journalistic perspectives, thus ensuring a more robust validation of the information used.

The selection of case studies was made based on relevant criteria aimed at the impact on critical infrastructures, the existence of a confirmed cyber component, the presence of informational effects such as panic or disinformation and the recognition of these incidents in international security reports. This approach allows for an integrated analysis of hybrid crises and facilitates the identification of recurring patterns specific to this type of threat.

2.2. Analysis of hybrid crisis scenarios

Within the applicative analysis, three case studies considered relevant for understanding the manifestation of hybrid crises in the contemporary security environment were selected. These include the attacks on Ukraine's energy infrastructure in 2015–2016, the ransomware attack on Colonial Pipeline in 2021, and the NotPetya cyber incident in 2017. The selection of these cases is justified by the significant impact on critical infrastructures, the

existence of complex cyber components and the indirect effects of an informational and social nature.

The first case analyzed is represented by the cyberattacks on the electricity grid in Ukraine, carried out in 2015 and 2016, considered the first confirmed incidents in which a cyberattack led to the effective interruption of the electricity supply. According to US-CERT reports and analysis by E-ISAC, the attackers used spear phishing techniques to initially compromise the systems, followed by the deployment of malware variants such as BlackEnergy and Industroyer. Subsequently, they gained access to industrial SCADA systems, managing to control electrical switches and cause significant power supply disruptions. The impact of this attack was considerable, affecting approximately 225,000–250,000 consumers and generating power outages that lasted up to six hours, with similar attempts on rail and energy infrastructure later being reported.

The second relevant case is the ransomware attack on Colonial Pipeline in the United States, produced in 2021 and attributed to the DarkSide group, which operated in a ransomware-as-a-service model. This incident had a major impact on the energy infrastructure, causing the operations of the largest fuel pipeline in the US to come to a complete halt and generating a fuel supply crisis on the East Coast. The situation was serious enough that it led to the declaration of a state of emergency in several American states. FBI and CISA investigations indicated that the attack was possible as a result of the compromise of a VPN password, in the context of a lack of multi-factor authentication and insufficient segmentation between IT and OT networks, vulnerabilities frequently encountered in modern critical infrastructures.

The third case analyzed is the NotPetya cyberattack in 2017, considered one of the most destructive cyber incidents globally. Although initially presented as ransomware, analysis by Microsoft and the National Cyber Security Centre in the United Kingdom showed that the real purpose of the malware was the irreversible destruction of data, which was later classified as a wiper attack. The propagation was achieved through a compromised software update, which allowed it to spread rapidly globally and affect major companies such as Maersk, Merck or FedEx TNT. The total economic impact was estimated at over 10 billion dollars, while the geopolitical dimension of the attack was also highlighted, which is associated in the literature with the logic of hybrid warfare.

The comparative analysis of these three case studies (see Table 1) highlights that cyberattacks on critical infrastructures not only produce technical effects, but also generate economic, social and security consequences, often amplified by organisational vulnerabilities and the interdependence of digital systems.

Table no. 1. Comparative table of the hybrid crises analysed

Criterion	**Ukraine 2015–2016**	**Colonial Pipeline 2021**	**NotPetya 2017**
Attack Type	ICS/SCADA malware	Ransomware	Wiper malware
Infrastructure	Electricity	Energy (fuel)	Global logistics
Information component	(panic, blackout)	average (panic public)	Medium
Impact economic	Environment	high	very high
Attributed actor	state-sponsored	criminal (DarkSide)	state-linked (assigned)

Source: authors' personal creation

The methodological analysis and case studies presented in this chapter have highlighted how hybrid crises manifest themselves in practice through the interaction between cyberattacks and critical infrastructure vulnerabilities. The investigation of the incidents in Ukraine (2015–2016), Colonial Pipeline (2021) and NotPetya (2017) allowed the observation of various forms of compromise of digital systems, with direct effects on the continuity of essential services and on the operational stability of the affected organizations.

At the same time, the analysis showed that these events cannot be reduced to simple technical incidents, but represent complex manifestations of the contemporary security environment, in which technological, organizational and geopolitical factors interact constantly. From the strictly descriptive perspective of this chapter, the main characteristics of attacks and their immediate impact on critical infrastructures have been highlighted, without an in-depth interpretation of the systemic implications being made.

In this regard, the results presented create the necessary premise for the analysis in the next chapter, in which the implications of these patterns on hybrid crisis management, on institutional resilience and on how the interaction between the cyber and information dimensions redefines contemporary security will be discussed.

3. Discussions on hybrid crisis management

Following what has been analyzed and presented in the second chapter of this paper, a series of recurrent patterns that characterize the manifestation of hybrid crises in the contemporary security environment are highlighted. First of all, there is an increasingly pronounced convergence between information technology and operational (IT-OT) infrastructures, which leads to an increase in the attack surface and the amplification of systemic vulnerabilities. The interconnection of these two environments means that an attack initiated in the digital space can produce direct effects on critical physical processes, such as energy distribution or the operation of logistics chains.

Another relevant pattern is the constant exploitation of the human factor in the initial phase of cyberattacks. In most of the cases analyzed, the compromise of systems was facilitated by actions such as phishing or the use of compromised credentials, which indicates that organizational and behavioral vulnerabilities remain a critical point in the security architecture of modern infrastructures.

The analysis also highlights the existence of a dual dimension of the impact of hybrid crises, which goes beyond the strictly technical component. In addition to the direct effects on the affected infrastructures, these incidents generate significant consequences at a psychological and social level, manifested by the amplification of the state of uncertainty, the decrease of trust in the responsible institutions and the increase in the level of public anxiety. In this sense, hybrid crises cannot be interpreted exclusively as technical events, but must be understood as phenomena with a systemic impact on society.

In addition, it is found that attacks on critical infrastructures frequently produce cascading effects, in which the disruption of one strategic sector generates dysfunctions in other interdependent areas. This feature is particularly relevant in the case of modern systems, where the temporary interruption of an essential service, such as energy or communications, can have a rapid impact on transport, the economy and the functioning of public administration.

3.1. Assessment of institutional response capacity and resilience

The analysis of the case studies presented in the previous chapter highlights the fact that institutional resilience in the face of hybrid crises directly depends on the ability of organizations and states to respond quickly, coordinated and adaptively to cyber incidents impacting critical infrastructures. In all three situations analysed (Ukraine 2015–2016, Colonial Pipeline 2021 and NotPetya 2017), the institutional response was characterised by rapid interventions, but significantly differentiated in terms of coordination, prevention and recovery.

In the case of attacks on Ukraine's energy infrastructure, the response capacity was initially limited by the lack of advanced incident detection and isolation mechanisms at the level of SCADA industrial systems. Although the outages were relatively short-lived, subsequent analysis showed that the response was predominantly reactive, based on manual system restoration and post-incident technical interventions, which showed a low level of maturity in terms of the security of critical infrastructures at the time of the attack.

In the case of Colonial Pipeline, the institutional response was more structured, and a cooperation mechanism was quickly activated between the company and the US federal authorities, including the FBI and CISA. The decision to preventively halt operations reflected a precautionary approach aimed at limiting the spread of risks, but simultaneously generated significant economic and social effects. Subsequently, investigations highlighted the importance of basic security measures, such as multi-factor authentication and network segmentation, as essential elements for preventing such incidents.

In the case of the NotPetya attack, the responsiveness was strongly affected by the global and rapid spread of the malware. Affected companies have had to resort to complex systems recovery and data recovery processes, and in many situations operational activity has been disrupted in the medium term. This case highlighted the limits of traditional response mechanisms to destructive and self-propagating attacks on a global scale.

From the perspective of institutional resilience, the comparative analysis shows that the level of preparedness and responsiveness are influenced by the maturity of the security infrastructure, the existence of incident response procedures and the level of cooperation between institutional and private actors. It also finds that resilience does not depend exclusively on the technical component, but also on the ability of organizations to ensure decision-making and operational continuity in crisis conditions.

Overall, the results indicate that, although response mechanisms have progressively improved over time, hybrid crises continue to test the limits of institutional resilience, especially as attacks combine technical effects with operational and strategic implications on critical infrastructures.

3.2. Adaptive security perspectives and models

The attacks on energy infrastructure in Ukraine (2015–2016), the Colonial Pipeline incident (2021) and the NotPetya attack (2017) – show that traditional security models, based predominantly on post-incident response, are insufficient in the face of contemporary hybrid threats. In all three situations, the exploited vulnerabilities were related either to human error, or to the lack of segmentation between information and operational systems, or to the absence of robust early detection mechanisms, which indicates the need to move towards adaptive security models.

With regard to Ukraine, the limitations of security systems have been amplified by the lack of advanced real-time monitoring capabilities of industrial networks. From this perspective, an adaptive model would involve the integration of anomaly-based detection systems, capable of identifying deviations in the operation of SCADA systems before they produce operational effects. This case also highlights the need to develop operational redundancy mechanisms that allow critical functions to be maintained even in conditions of partial compromise of infrastructure.

In the case of Colonial Pipeline, the analysis shows that the exploitation of an unauthorized VPN access vulnerability led to the paralysis of an entire critical infrastructure, mainly due to the lack of adequate segmentation between IT and OT networks. From an adaptive security perspective, this incident highlights the importance of implementing the "Zero Trust Architecture" model, in which no access is considered secure by default, and continuous authentication and verification of user identity become central elements of infrastructure protection. In addition, the adaptive model assumes an increased capacity to quickly isolate the compromised segments to limit the propagation of the incident.

Regarding NotPetya, the extremely fast and destructive nature of malware propagation demonstrated the limits of defense models based solely on prevention. This incident highlights the need to adopt a resilient security model focused on rapid recovery resilience, in which isolated backups, automated system restoration and distributed architectures play a critical role. At the same time, the global dimension of the impact suggests that adaptive security must also include international cooperation mechanisms for the rapid sharing of indicators of compromise (IOCs).

Taken together, these cases indicate that adaptive security cannot be reduced to a single technology or solution, but is an integrated set of technical, organisational and strategic measures. This involves moving from a static defense model to a dynamic one, capable of learning from previous incidents, adjusting in real time to new types of threats, and ensuring the continuity of the operation of critical infrastructures even under conditions of complex hybrid attack.

3.3. Proposals and recommendations

In all the situations analyzed, the identified vulnerabilities were amplified by technical, organizational and procedural deficiencies, which indicates that the response to hybrid threats needs to be addressed in an integrated way.

First of all, it is necessary to strengthen security architectures by implementing modern "Zero Trust" models, especially in critical infrastructures that combine IT and OT systems. This type of approach significantly reduces the risk of unauthorized access, by continuously verifying identities and limiting access privileges to what is strictly necessary. The Colonial Pipeline case directly highlights the consequences of the lack of such mechanisms, where the compromise of a single VPN account was enough to affect a major energy infrastructure.

Secondly, there is a need to develop and expand early detection capabilities based on artificial intelligence and behavioural network analysis. The experience of attacks on energy infrastructure in Ukraine shows that the late identification of intrusions significantly reduces the ability to respond, which is why anomaly detection systems and continuous monitoring of industrial traffic become essential to prevent the escalation of incidents.

Another important direction is to strengthen operational resilience through redundancy mechanisms and robust business continuity plans. The NotPetya case demonstrated that destructive attacks can completely cripple global organizations, which is why offline backup architectures, rapid system restoration and advanced network segmentation must become mandatory standards in critical infrastructures.

In addition, the analysis highlights the need to strengthen institutional and international cooperation, in particular with regard to the rapid exchange of information on indicators of compromise and active attack campaigns. The cross-border nature of hybrid threats makes isolated response at national level insufficient, requiring coordination mechanisms between states, international organisations and the private sector.

Last but not least, the human dimension of security remains essential, as most of the incidents analyzed involved the exploitation of human errors or vulnerabilities. From this perspective, continuous training programs, periodic simulations of cyberattacks and the development of a security-oriented organizational culture are fundamental elements for reducing operational risk.

Overall, these recommendations highlight that effective hybrid crisis management cannot be achieved through isolated measures, but requires a systemic, adaptive and multidimensional approach that integrates technological, institutional and human components into a unified security framework.

Conclusions

Through this paper, the authors aimed to analyze how the interaction between information warfare and cyberattacks influences hybrid crisis management and institutional resilience in the context of contemporary security. Starting from this research question, the results obtained indicate that the effectiveness of hybrid crisis management directly depends on the degree of integration between cybersecurity and countering disinformation mechanisms, as well as on the ability of institutions to respond in a coordinated manner in dynamic and interconnected threat environments.

Case studies have shown that cyberattacks on critical infrastructures are rarely isolated events, as they are often accompanied by indirect informational and social effects, which amplify the initial impact of the incident. In this regard, the crises analysed have shown that technical vulnerabilities are often exploited in parallel with organisational and cognitive vulnerabilities, which transforms cyber incidents into crises of a systemic nature.

The answer to the research question can be formulated as follows: the integration of strategies to combat disinformation with the mechanisms for preventing and managing cyber-attacks contributes significantly to increasing institutional resilience, as it allows the simultaneous reduction of the technical and informational impact of hybrid crises. In the absence of this integration, the capacity to respond remains fragmented and the effects of crises tend to be amplified by the rapid propagation of uncertainty and operational disruptions.

In conclusion, the research confirms that hybrid crisis management can no longer be approached through sectoral perspectives, but requires a unitary vision, in which the cyber and information dimensions are treated as interdependent elements of the same security system.

References

1. Aftabi, N., et al., 2023. *An Integrated Cyber-Physical Risk Assessment Framework for Worst-Case Attacks in Industrial Control Systems*. arXiv.
2. Alvisi, L., et al., 2024. *Disinformation and Cyber Crisis Amplification in Hybrid Conflicts*. arXiv.
3. Ball, J., 2017. *The Kremlin's Information War*. NATO Defense College Foundation.
4. Bachmann, S.-D., et al., 2023. Hybrid Warfare and Disinformation: A Ukraine War Perspective. *Global Policy*, 14 (4), pp. 858–869.
5. Backhaus, S., et al., 2020. Psychological and Societal Impacts of Cyber Attacks on Critical Infrastructure. *Cyberpsychology, Behavior, and Social Networking*, 23 (8), pp. 526–533.
6. Bjola, C., 2025. Algorithmic Invasions: How Information Warfare Threatens NATO's Eastern Flank. *NATO Review*, 7 February.
7. CISA, 2022. Shields Up: Guidance for Critical Infrastructure Organizations. *Cybersecurity and Infrastructure Security Agency.*
8. ENISA, 2023. ENISA Threat Landscape 2023. *European Union Agency for Cybersecurity.*
9. Maglaras, L., et al., 2018. Cyber Security of Critical Infrastructures. *ICT Express*, 4(1), pp. 42–45.
10. Maynard, P., et al., 2020. Industrial Control Systems and Cyber Security: A Review of Attacks and Defenses. *Cybersecurity*, 3(1), pp. 1–18.
11. NATO, 2023. Hybrid Threats: A Comprehensive Overview. *North Atlantic Treaty Organization.*
12. Oliveira de Sá, A., et al., 2024. Artificial Intelligence and Cyber Threats Against Critical Infrastructures. *International Journal of Critical Infrastructure Protection*, 45, 100683.
13. Rahimpour, H., et al., 2023. Cybersecurity Challenges of Power Transformers. arXiv.
14. Rid, T., 2012. Cyber War Will Not Take Place. *Journal of Strategic Studies*, 35(1), pp. 5–32.
15. Riggs, H., et al., 2023. Impact, Vulnerabilities, and Mitigation Strategies for Cyber-Secure Critical Infrastructure. *Sensors*, 23(8), 4060.
16. Romaniuk, S. N., et al., 2021. NATO's Evolving Cyber Security Policy and Strategy. *Connections: The Quarterly Journal*, 20(1), pp. 57–76.
17. Segovia-Ferreira, M., et al., 2023. A Survey on Cyber-Resilience Approaches for Cyber-Physical Systems. arXiv.
18. Spaziani, A., 2024. Hybrid Warfare and Information Manipulation in Cyberspace. *DPCE Online*, 58(1), pp. 233–248.
19. Yigit, Y., et al., 2024. Critical Infrastructure Protection: Generative AI, Challenges, and Opportunities. arXiv.