BRIDGING THE GAP BETWEEN ANALYSIS AND PREDICTION – TOWARDS THE DEVELOPMENT OF AN INTEGRATED PREDICTIVE MODEL FOR HYBRID THREAT RISK ASSESSMENT –

Colonel Professor Cezar VASILESCU, PhD, Habil, BEng

Associate Professor Aura CODREANU, PhD

Regional Department for Defence Resources Management Studies (DRESMARA) Brașov;
"Carol I" National Defence University", Bucharest

DOI: 10.55535/RMT.2024.4.35

This article analyses the common patterns of recent hybrid threats, highlighting some representative cases such as: the information warfare during the US elections (2020), the COVID-19 vaccine disinformation campaign (2020-2021), and the energy crisis in Europe (2021-2022), in order to identify the existence of potential synergies between different tactics (cyber, information, economic) depending on the specific context. On the basis of these patterns, the article proposes the essential parameters of a predictive hybrid threat analysis model (including geopolitical, cyber, economic, social, media, political and technological factors) with the aim of facilitating proactive responses to this type of threats in modern society.

Keywords: hybrid threats; disinformation; modern conflicts; economic pressure; cyber-warfare operations;

INTRODUCTION

In recent decades, the international security environment has undergone major transformations, becoming increasingly complex and unpredictable. Today, it is defined by instability and uncertainty and is influenced by a number of global factors (rapid digitalization of society, interconnectedness of national economies, increased complexity and interconnectivity between states, intensified competition for strategic resources and geopolitical influence, and political volatility) that have led to new vulnerabilities that can be exploited by state and non-state actors.

The latter are continually adjusting the tactics they use to exploit these vulnerabilities, as the use of hybrid elements offers a significant advantage: relatively low cost, minimized risk, and less likelihood of generating a large-scale military response (Pindják, 2019). For example, the use of social media and other digital communication platforms has become an essential tool in influence and destabilization campaigns (Galeotti, 2019).

In this context, globally, hybrid threats have become a preferred tool to undermine the stability of states and regions. In contrast to conventional armed conflicts, these threats manifest themselves in multiple forms, involving a combination of tools and methods that cover the military, non-military, cyber and informational domains (Hoffman, 2007).

These hybrid threats combine multiple unconventional techniques and tactics (from cyber-attacks against critical infrastructures – such as health or energy – to disinformation campaigns and economic pressure) in an integrated and subtle way to weaken national stability without triggering a traditional military response. A common feature of these cases is the *use of synergy between several forms of aggression*, which complicates the process of detecting and countering them.

The concept of *"hybrid threat"* is not new, but its formal use in the security literature has grown exponentially over the last decade, particularly in the context of modern conflicts. Hybrid threats are defined as a combination of conventional and unconventional methods, including cyber-warfare operations, disinformation, economic attacks, and political and social influence tactics. According to a NATO report, hybrid threats are characterized by the *"Coordinated and synchronized use of different means and activities, aimed at exploiting vulnerabilities in societies and undermining the political and economic stability of target states"* (NATO, 2020).

They manifest themselves in a *"grey space"* of conflict, where it is difficult to distinguish between peace and war, and the responsible actors often remain undetected or officially unidentifiable (Mumford, 2021).

Also, Hoffman (2007) defines hybrid threats as *"A synthesis of conventional and unconventional methods, including terrorism, insurgency, and cyber warfare, which are combined into an integrated campaign".* Another definition of the concept of hybrid threats is offered by Rid and Hecker (2021). According to them, it represents *"operations that combine cyberattacks with other forms of aggression, including economic pressure and disinformation"*, while, as the same authors underline, their multisector dimension needs to be highlighted. The immediate consequence of integrating multiple domains is that responding to such threats becomes a difficult and challenging task.

One of the fundamental characteristics of hybrid threats is the use of a wide range of tactics in a synergistic manner. This approach allows actors to exploit vulnerabilities on multiple fronts simultaneously, thus creating multidimensional pressure on the target. Synergy between cyber, information and economic tactics has become a defining element in recent hybrid conflicts. For example, cyber-attacks can be coordinated with disinformation campaigns to amplify destabilizing effects, while economic pressures can be used to weaken the resilience of states.

According to studies by Wither (2016), the synergy of these threats is characterized by the integration and coordination of multiple domains (including cyber, information and economic). According to the aforementioned author, the essential element in defining a hybrid threat is that the vulnerabilities of a target state are taken advantage of, especially in the context of social, economic and political divisions. Thus, while the nature of the attacks may vary, their common aim is to destabilize order and weaken the response capabilities of the targets.

In this context, the fundamental assumption of the first part of this paper is that *"Hybrid threats use a combination of cyber, informational and economic tactics tailored to the specific context of each target state, and their success depends on the degree of integration and synchronization of these tactics, whose synergy amplifies the destabilizing impact"*.

To test this hypothesis, the current research will use comparative analysis as a method to review several recent cases of hybrid threats, selected on the basis of their geopolitical relevance and impact. By analysing these cases, we will proceed to *identify their individual specific patterns and, in the end, describe possible common patterns*. We will also analyse how different tactics (cyber, informational, economic) have been combined and coordinated to achieve the objectives of the actors involved.

This hypothesis assumes that hybrid tactics are not used in isolation, but synergistically (Otaiku, 2018), tailored to the specific vulnerabilities of each state, whether economic (such as sanctions or energy crises), informational (disinformation and propaganda campaigns), or cyber (attacks on critical infrastructure).

Among the main sources used in this analysis to test the validity of the underlying hypothesis are recent NATO (2020) report studies, as well as theoretical and empirical work on hybrid threats (Hoffman, 2007; Wither, 2016; Pindjak, 2014 and 2019; Galeotti, 2019; Rid, Hecker, 2021).

Ultimately, we will seek to demonstrate that achieving the objectives of these hybrid threats depends on coordination across multiple domains and tailoring tactics to the specific vulnerabilities of each target.

COMPARATIVE ANALYSIS OF HYBRID THREATS

The study of hybrid threats represents a major challenge for international security research, given their complexity and their ability to adapt rapidly to changes in the global security environment. By comparatively analysing several recent cases and identifying common patterns of action, this research aims to provide a better understanding of the mechanisms underlying these threats and to contribute to the development of effective countering strategies.

In the following paragraphs we will briefly examine each of the selected cases, using as analysis parameters the purpose, the tactics used, the vulnerabilities exploited and the patterns identified.

A. Information warfare during the US election (2020) (National Intelligence Council, 2021; Wojnowski, 2021; Menn, 2020).

- Purpose: Undermine confidence in the American electoral process and destabilize politics.
- Tactics used:
  - Disinformation and propaganda: massive spread of conspiracy theories and false information about electoral fraud.
  - Cyber-attacks: hacking attempts on electoral systems and critical infrastructure.
  - Exploiting social divisions: Amplifying racial and political tensions through fake social media accounts.
- Exploited vulnerabilities:
  - Political polarization: the deep divide between political parties and social groups in the USA.

- Low trust in public institutions: at an already low level it was amplified by disinformation campaigns.
- Social platform addiction: Vulnerabilities in social networks used to spread misinformation rapidly.

- Patterns identified:
  - Multi-modal coordination: the combined use of online (disinformation and cyber-attacks) and offline techniques – as a result of the former (protests and social tensions).
  - Long-term goals: creating an atmosphere of widespread distrust in democratic institutions.

B. COVID-19 vaccine misinformation campaign (2020-2021) (Tsiklauri, 2021; Suarez-Lledo et al., 2021; Stokel-Walker, 2024)

- Purpose: To weaken the global response to the pandemic and increase distrust in health authorities.
- Tactics used:
  - Spreading misinformation: false information about the effectiveness and safety of vaccines was amplified on social networks.
  - Exploiting fears and emotions: messages that exploited fear of the unknown and suspicion of governments and corporations.
  - Informal alliances: using alternative media channels and influencers to spread anti-vaccination messages.
- Exploited vulnerabilities:
  - Distrust in health authorities: fear and confusion over new virus and vaccines.
  - Uncontrolled access to information on social platforms: it allowed conspiracy theories to spread rapidly.
  - Fragmentation of the information ecosystem: access to alternative channels of information undermining scientific consensus.
- Patterns identified:
  - Information fragmentation: creating and feeding alternative information ecosystems that undermine scientific consensus.
  - Time as a critical factor: use of critical periods (start of vaccination campaign) to maximize negative impact.

C. Europe's energy crisis (2021-2022) (Gilbert et al., 2021; Popkostova, 2022; Gross et al., 2024)

- Purpose: To exert political pressure on Europe in order to influence the geopolitical and economic positions of member states.

- Tactics used:
  - Manipulating energy prices: deliberately cutting natural gas deliveries, thus creating an energy price crisis.
  - Economic pressures: threats of complete disruption of supplies amid political tensions.
  - Misinformation and media messaging: amplifying narratives blaming European governments for the energy crisis, thus dividing public opinion.
- Exploited vulnerabilities:
  - Energy dependence on Russia: European countries were vulnerable because of their dependence on Russian natural gas.
  - Economic structure and fragility of the energy sector: lack of immediate alternatives for energy supply.
  - Domestic political sensitivities: growing public discontent over high energy costs.
- Patterns identified:
  - Economic influence: using critical economic resources as a geopolitical weapon.
  - Synchronization of actions: coordination between different hybrid tactics (economic, informational) to maximize impact.

D. Cyber interference in the French election campaign (2017) (Vilmer et al., 2018; O'Connor et al., 2020; Ferrara, 2017)

- Purpose: To undermine the electoral process and influence the outcome of the presidential elections.
- Tactics used:
  - Cyber-attacks: hacking and publication of sensitive emails and documents of Emmanuel Macron's campaign team.
  - Disinformation: spreading false information and conspiracy theories on social networks and in the media in order to discredit the candidate favoured by the West.
  - Message amplification: using social media networks and fake accounts to amplify the impact of disinformation.
- Exploited vulnerabilities:
  - Poorly protected cyber infrastructure: political and campaign systems vulnerable to cyber-attacks.
  - Tense electoral period: the attacks were coordinated at key moments, when destabilization could have had the greatest impact.

- Rapid spread of disinformation online: effective use of social networks to amplify exfiltrated information.

- Patterns identified:
  - Concerted cyber-attacks: coordination between hacking and rapid dissemination of information to cause chaos before the vote.
  - Pre-election targeting: exploiting the sensitive period before elections to maximize the destabilizing impact.

E. Hybrid operations in Ukraine (2014-present) (Starodubtseva, 2021; Wentzell, 2021; Nübel, 2020)

- Purpose: To divide the territorial integrity of Ukraine and influence political decisions.
- Tactics used:
  - Unconventional military aggression: the use of unmarked troops, known as *"little green men"*, to seize control of Crimea.
  - Disinformation and propaganda: creating and disseminating narratives to justify intervention and generate confusion concerning the events.
  - Economic pressure: using Ukraine's dependence on Russian natural gas to exert political pressure.
- Exploited vulnerabilities:
  - Ethnic and political divisions: exploiting tensions between the pro-Russian eastern regions and the rest of Ukraine.
  - Energy dependence on Russia: Ukraine was vulnerable because of its dependence on Russian gas.
  - Military and political weaknesses: lack of military preparedness and non-existent internal political consensus in the face of aggression.
- Patterns identified:
  - Combined use of military and informational means: combining subtle military tactics with a powerful disinformation campaign to create ambiguity and prevent a unified international response.
  - Pressure on critical resources: using energy resources as economic leverage to influence the political decisions of the target state.

F. The migrant crisis in Europe (2015-2016) (Kuvekalović et al., 2017; Braghiroli et al., 2026; Karolewski et al., 2018)

- Purpose: Destabilization of European states by exacerbating the migration crisis and increasing social tensions.

- Tactics used:
  - Manipulating migration flows: facilitating or directing migrant flows towards European borders, using human trafficking networks and providing incentives.
  - Disinformation and media bias: spreading disinformation about the nature and reasons for the migration crisis, amplifying fears and social tensions in host countries.
  - Exploiting social vulnerabilities: fuelling xenophobic and anti-immigrant sentiments among the European population, thus dividing societies and putting pressure on local governments.
- Exploited vulnerabilities:
  - Lack of a common migration policy: Europe was vulnerable due to the lack of a unified mechanism to manage the migration crisis.
  - Social tensions and fear of immigration: exacerbation of xenophobia among European populations.
  - Exposure to misinformation: using media and social networks to amplify the perception of a major crisis.
- Patterns identified:
  - Exploiting humanitarian crises: using real humanitarian crises to destabilize target countries by creating social and political divisions.
  - Media amplification: using the media and social networks to amplify the perception of a crisis that is much worse than the reality, and thus intensifying public reactions.

G. The migrant crisis on the Polish-Belarusian border (2021) (Zdanowicz, 2023; Bodnar et al., 2023; Jędrzejczyk-Kuliniak, 2023)

- Purpose: Destabilize the European Union and create internal tensions by using migrants as an instrument of political pressure.
- Tactics used:
  - Forced migration: Belarus has orchestrated flows of migrants to EU borders, especially Poland, to create a humanitarian crisis and force a reaction.
  - Propaganda: using state-controlled media to blame the EU for the humanitarian crisis, while Belarus denied any involvement.
  - Coercive diplomacy: threat of escalation if political demands were not met, including sanctions against the Lukashenko regime.

- Exploited vulnerabilities:
  - Poorly controlled borders: the lack of a solid border control infrastructure on Poland's border with Belarus at that time.
  - Internal EU tensions: exploiting EU divergences on migration policy.
  - Slow reaction from the authorities: the EU has been slow to react to Belarus' manipulation of migration.
- Patterns identified:
  - Migration as a weapon of destabilization: using migrant flows to exert political pressure on a regional entity.
  - The combination of coercion and propaganda: amplification of an artificially created crisis through disinformation and propaganda campaigns.

H. Intervention in the Catalan independence referendum (2017) (Vakarchuk, 2020; Arcos, 2021; Barberà, 2020)

- Aim: Amplify regional divisions and weaken Spain's national unity.
- Tactics used:
  - Disinformation and manipulation: spreading narratives supporting Catalan independence and encouraging confrontation between the central government and separatists.
  - Cyber-attacks: sabotaging websites and digital infrastructure associated with the Spanish government to hamper the response to the political crisis.
  - Protests and social unrest: encouraging and organizing mass protests and civil disobedience actions to amplify social tensions.
- Exploited vulnerabilities:
  - Nationalist and regional tensions: the historical conflict between Catalonia and the Spanish central government.
  - Institutional weaknesses: the central government had difficulties in managing the crisis, which aggravated tensions.
  - Exposure to disinformation: exploiting nationalist narratives and disinformation campaigns to fuel protests.
- Patterns identified:
  - Exploiting regional political divisions: focus on regional nationalist tensions to destabilize the nation state.
  - Synergy between disinformation and social mobilization: combining disinformation with direct social action to create a major political crisis.

I. Intervention in the political crisis in Venezuela (2019) (Rouvinski, 2019; Aulia et al., 2024; Rozental et al., 2022)

- Purpose: To influence the political balance in favour of the government in Caracas, despite international opposition.
- Tactics used:
  - International disinformation: spreading narratives legitimizing Nicolás Maduro's government and delegitimizing the Western-backed opposition.
  - Economic intervention and sanctions: using economic resources and trade relations to support the regime in the face of international sanctions.
  - Alliances and military support: providing military and logistical support through external allies to maintain regime's control.
- Exploited vulnerabilities:
  - Fragile economy: the severe economic crisis in Venezuela has been fertile ground for manipulation and disinformation.
  - Political polarization: deep division between regime supporters and opposition.
  - International isolation: the regime has benefited from the support of some foreign states, thwarting international sanctions.
- Patterns identified:
  - Sanctions and economic countermeasures: use of economic means to counter sanctions and support regime stability.
  - Information War: a global disinformation campaign targeting not only the local public but also the international perception of the political crisis.

J. Hybrid threats in Venezuela (2019-present) (Cañizález et al., 2020; Beaton, 2021; Chaguaceda et al., 2023)

- Purpose: To maintain Nicolás Maduro's regime in power despite economic and political crisis and international pressure.
- Tactics used:
  - Internal repression: the use of security forces to suppress protests and neutralize political opposition.
  - Information control: restricting access to information through censorship, media control and limiting internet access.
  - Disinformation: spreading narratives blaming foreign powers for the economic and political crisis, strengthening domestic support.

- Exploited vulnerabilities:
  - Authoritarian political system: using repression and information control to stay in power.
  - Resource dependence: control over natural resources (oil) has allowed the regime to resist sanctions.
  - Weakness of the opposition: the fragmentation and lack of a strong opposition leader was exploited by the regime.
- Patterns identified:
  - Internal repression and information control: simultaneous use of force and censorship to maintain control over the population.
  - Disinformation to legitimize the regime: spreading disinformation to counter international criticism and mobilize domestic support.

K. Political crisis in Belarus (2020-present) (Hardy, 2022; Giannakopoulou, 2022; Astapova et al., 2022)

- Purpose: Maintain Alexander Lukashenko's regime in power despite internal and external pressure for change.
- Tactics used:
  - Repression and human rights violations: use of force against protesters and pro-democracy activists to suppress opposition movements.
  - Disinformation: propagation of narratives delegitimizing opposition movements and presenting the regime as the only stabilizing force.
  - External support: recourse to Russian support, including military and economic support, to keep the regime in power despite international sanctions.
- Exploited vulnerabilities:
  - Authoritarian system: Lukashenko used repression and disinformation to suppress opposition movements.
  - Dependence on Russia: Belarus' vulnerability to Russian economic and military influence.
  - Internal social tensions: exploiting fear of change among the conservative population.
- Patterns identified:
  - Internal repression combined with disinformation: the simultaneous use of brute force and disinformation to discourage opposition and maintain control.
  - External support for stability: dependence on the support of a strong ally to survive to international and domestic pressure.

L. China's influence in Southeast Asia (2020-present) (Schmidt, 2008; Pal, 2021; Ferchen et al., 2023)

- Purpose: Expand China's economic and political influence in the region and counter Western influence.
- Tactics used:
  - Coercive diplomacy: the use of economic levers, such as investment and debt, to exert political influence over Southeast Asian states.
  - Disinformation and propaganda: promoting pro-China narratives in the region through state-controlled media and social networks.
  - Aggressive maritime activities: expanding territorial claims in the South China Sea by building artificial islands and militarizing the area.
- Exploited vulnerabilities:
  - Economic dependence: Southeast Asian states are vulnerable due to Chinese debt and investment.
  - Territorial disputes: states in the region are vulnerable because of territorial disputes in the South China Sea.
  - Democratic weaknesses: weaker or authoritarian regimes are easily influenced by economic levers.
- Patterns identified:
  - Using economic power as a political weapon: using economic dependencies created through investment and borrowing to control the political decisions of other states.
  - Non-military and military aggression: combining economic tactics with military presence to dominate a strategic region and limit the influence of rivals.

M. Chinese interference in Taiwan's politics (2019-present) (Chang et al., 2021; Hung et al., 2022; Hartnett et al., 2021)

- Purpose: Undermine Taiwan's political independence and reduce international support for the government in Taipei.
- Tactics used:
  - Disinformation: spreading fake news and conspiracy theories to weaken Taiwanese citizens' trust in their government.
  - Cyber-attacks: attacks on government institutions and critical infrastructure in Taiwan to destabilize the political and economic system.
  - Economic pressure: restricting Taiwan's access to international markets and pressuring other states not to recognize Taiwanese sovereignty.

- Exploited vulnerabilities:
  - Economic dependence: Taiwan is vulnerable to economic pressure from China on its trading partners.
  - Diplomatic isolation: Taiwan has few international allies and is under constant pressure from China.
  - Internal political tensions: exploiting Taiwan's internal political divisions.
- Patterns identified:
  - Synergy between cyber-attacks and disinformation: the combined use of cyber-attacks and disinformation campaigns to destabilize a democratic regime.
  - Economic pressure targeting political isolation: using economic influence to limit international support for a target country.

N. Political and security crisis in Mali (2012-present) (Thurston et al., 2013; Cox et al., 2018; Maza et al., 2020)

- Purpose: Maintain power and control over natural resources by destabilizing the region and limiting the influence of the central government and international peacekeeping forces.
- Tactics used:
  - Insurgency and terrorism: jihadist groups use guerrilla tactics, bombings and kidnappings to destabilize the region.
  - Disinformation and propaganda: spreading extremist ideology through social networks and local channels, strengthening public support for insurgent groups.
  - Exploiting social vulnerabilities: Manipulating ethnic and religious tensions to undermine social cohesion and weaken government.
- Exploited vulnerabilities:
  - Weakness of the central government: the Malian government has not been able to control all regions of the country.
  - Ethnic and religious tensions: exploiting tribal and ethnic rivalries in Mali.
  - Presence of extremist groups: vulnerability to the influence of jihadist groups active in the region.
- Patterns identified:
  - Combining insurgency with disinformation: the synergy between field operations and online propaganda to recruit and legitimize violent actions.
  - Exploiting social divisions: using ethnic and religious conflicts to intensify instability and prevent effective centralized government.

O. Iran's cyber interference campaign (2018-present) (Spataro, 2019; Elswah et al., 2021; Lehto, 2022)

- Purpose: Undermine the political stability of enemies and gain strategic advantage through cyber-attacks and disinformation.
- Tactics used:
  - Cyber-attacks: Iran orchestrated attacks on critical infrastructure in the US and its allies, including energy networks and financial systems.
  - Intellectual property theft: the theft of sensitive data and intellectual property from critical industries to develop its own technological capabilities.
  - Disinformation campaigns: launch of online campaigns to spread pro-Iranian narratives and discredit Western governments.
- Exploited vulnerabilities:
  - Unprotected critical infrastructure: cyber systems in the US and other allied countries were exposed to cyberattacks.
  - Poorly protected intellectual property: Iran exploited unprotected systems to steal critical data.
  - Negative perception of Western governments: amplifying anti-Western narratives.
- Patterns identified:
  - Strategic cyber aggression: the persistent use of cyber-attacks to destabilize adversaries and gain economic and military advantage.
  - Disinformation in support of cyber-attacks: spreading disinformation to amplify the effects of cyber-attacks and create confusion among the target population.

P. Russian influence in the Western Balkans (2014-present) (Lika, 2021; Cipan et al., 2024; Kase, 2024)

- Aim: To prevent the integration of Western Balkan states into the EU and NATO and maintain the Russian sphere of influence in the region.
- Tactics used:
  - Supporting pro-Russian parties: financial and logistical support to pro-Russian political parties and movements to influence national policies.
  - Disinformation: spreading disinformation to delegitimize the European Union and NATO while promoting pro-Russian narratives.
  - Ethnic and religious tensions: Exploiting ethnic and religious sensitivities to create instability and impede regional cooperation.

- Exploited vulnerabilities:
  - Political instability: the Balkan regions have been marked by simmering ethnic and political conflicts.
  - Energy dependence: Balkan states depend on Russian natural gas.
  - Economic weakness and corruption: exploiting poverty and corruption to gain influence.
- Patterns identified:
  - Political influence through financial support: use of material support to directly influence the domestic policies of target states.
  - Exacerbating social divisions: using historical and ethnic tensions to prevent European integration and destabilize the region.

*

The analysis of these cases allows highlighting some common patterns in the use of hybrid threats, which underline their complex nature, as follows:

- **Synergy between different fields of action:** In all the cases analysed, several types of actions/tactics (cyber, informational, economic) were combined to create multidimensional pressure on adversaries and to achieve the proposed objectives. This synergy is essential for the effectiveness of a hybrid threat.
- **Exploitation and manipulation of existing social and/or political crises:** Whether political, economic or territorial, social and psychological vulnerabilities (such as fear, political divisions or distrust of institutions) have been exploited to destabilize target states.
- **Propaganda and disinformation as a key tactic:** Propaganda and disinformation have been widely used to shape public perceptions and legitimize questionable international actions. Control and manipulation of information were key to influencing perceptions and destabilizing society.
- **Flexibility and adaptability**: The cases analysed demonstrated the ability of actors behind hybrid threats to adapt quickly to changing situations, using different means depending on the specific context (e.g. the rise of cyber-attacks during an election campaign or the manipulation of the energy market in the context of a political crisis).
- **Long-term influence**: Most of the hybrid actions analysed were designed to have long-term effects, aimed at gradually destabilizing trust in international institutions and alliances.

*

With regard to the hybrid tactics used, we note that they were not used in isolation, but in synergy. Thus, in *table 1*, we summarize them in order to identify how they were combined and coordinated to achieve the objectives of the actors involved and the type of synergy applied.

Table 1: Hybrid tactics used for each case analysed (authors' design)

Hybrid threat	Tactics used			Synergy type
	cyber (C	Information (I)	Economic (E)	
Information war during the US elections (2020)	Cyber-attacks on electoral infrastructure	Disinformation and propaganda campaigns	-	C-I
Disinformation campaign against COVID-19 vaccines (2020-2021)	-	Disinformation and propaganda on the effectiveness and safety of vaccines through anti-vaccination messages	-	I
Europe's energy crisis (2021-2022)	-	Disinformation and media messages blaming European governments	Energy price manipulation and economic pressures	I-E
Cyber interference in the French election campaign (2017)	Cyber-attacks on Macron campaign team	Disinformation and propaganda	-	C-I
Hybrid operations in Ukraine (2014-present)	Cyber-attacks on government infrastructure	Disinformation and propaganda	Economic pressures on energy resources	C-I-E

Hybrid threat	Tactics used			Synergy type
	cyber (C	Information (I)	Economic (E)	
The migrant crisis in Europe (2015-2016)	-	Migration crisis misinformation	Manipulating migration flows to create economic and social pressures	I-E
Migrant crisis on the Polish-Belarusian border (2021)	-	Anti-EU propaganda	Forced migration as political pressure	I-E
Intervention in the Catalan independence referendum (2017)	Cyber-attacks on government infrastructure	Disinformation and manipulation	-	C-I
Intervention in the political crisis in Venezuela (2019)	-	International disinformation	Economic interventions and sanctions	I-E
Hybrid threats in Venezuela (2019-present)	-	Internal disinformation to strengthen the regime	Economic pressure and internal repression	I-E
Political crisis in Belarus (2020-present)	-	Disinformation and propaganda to delegitimize the opposition	Economic and military support from Russia	I-E
China's influence in Southeast Asia (2020-present)	-	Regional disinformation and propaganda	Economic coercive diplomacy	I-E

Hybrid threat	Tactics used			Synergy type
	cyber (C	Information (I)	Economic (E)	
China's interference in Taiwan's politics (2019-present)	Cyber-attacks on institutions in Taiwan	Disinformation	Economic pressure on Taiwan	C-I-E
Political and security crisis in Mali (2012-present)	-	Jihadist disinformation and propaganda	Exploitation of natural resources and social tensions	I-E
Iran's cyber interference campaign (2018-present)	Cyber-attacks and intellectual property theft	Disinformation campaigns	-	C-I
Russia's influence in the Western Balkans (2014-present)	-	Disinformation to exacerbate ethnic tensions	Economic and logistical support for pro-Russian parties	I-E

We will also graphically present *table 1* in the form of a *"heat map"* diagram, which will represent the presence or absence of specific tactics for all 16 hybrid threats (a to p) in a two-dimensional way. This new representation allows a more intuitive analysis of the prevalence of each tactic within the hybrid threats and facilitates the rapid identification of patterns and trends in the use of these tactics.

In this representation:

- Each column represents a hybrid threat from the table above, labelled with the corresponding letter (a-p).
- The rows represent the three types of tactics: C (Cyber), I (Information), E (Economic).
- Red cells indicate the presence of a tactic for a particular threat.
- White cells indicate no tactic.

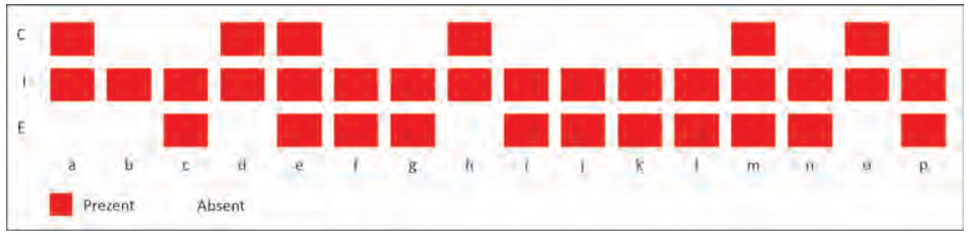

Figure 1: Hybrid tactics used for each hybrid threat.
(Heat map diagram) (authors' design)

Henceforth, based on the two graphical representations, we present a number of observations. Regarding the use of combined tactics, we observe the presence of C-I (cyber and informational only) in 3 cases, I-E (informational and economic only) in 8 cases, C-I-E (all three tactics) in 3 cases and I (informational only) in one case. The informational tactic (I) is also the most frequently used, forming an almost continuous line of red cells, and is applied in almost all but one case. This emphasizes the crucial importance of the informational component in hybrid threats.

Cyber tactics (C) are less common (occurring in only 6 out of 16 cases) and occur in combination with informational tactics in several cases. This suggests that, although important, cyber-attacks are not always a universal component of hybrid threats. Economic (E) tactics are present in about half of the threats, often in combination with informational tactics, forming an alternating pattern. This suggests that economic pressure is a significant but not universal component of hybrid threats. Last but not least, there are a few threats that use all three types of tactics (the fully red rows).

It becomes evident that information tactics play a central role in all hybrid threats, while economic and cyber tactics are used selectively depending on the specific nature of the threat.

As regards the hypothesis that hybrid tactics were tailored to the specific vulnerabilities of each individual target state/entity, *table 2* substantiates such a conclusion.

Table 2: Adaptation of tactics used in hybrid threats to the vulnerabilities characteristic of the cases analysed (authors' design)

Hybrid threat	Vulnerabilities	How to adapt tactics
Information war during the US elections (2020)	Political polarization, low trust in media, massive use of social networks	Disinformation exploited political divisions and racial tensions, while cyber-attacks targeted election infrastructure

Hybrid threat	Vulnerabilities	How to adapt tactics
Disinformation campaign against COVID-19 vaccines (2020-2021)	Lack of accurate information about vaccines, mistrust in authorities and medical institutions	Disinformation messages targeted reluctant groups and used social media to amplify mistrust
Europe's energy crisis (2021-2022)	Energy dependence on Russia, European market vulnerable to price fluctuations	Russia's cutting of gas supplies was used as an economic weapon along with disinformation to amplify public discontent with governments
Cyber interference in the French election campaign (2017)	Fragmented political system, strong social media presence in campaigns	Cyber-attacks and leaks targeting Macron's team accompanied by disinformation campaigns
Hybrid operations in Ukraine (2014-present)	Ethnic and linguistic divisions, economic instability and corruption	Russia has combined propaganda, unofficial military support and cyber-attacks to destabilize the country
Europe's migrant crisis (2015-2016)	Overburdened immigration system, rise of populist anti-immigration parties	Misinformation has heightened fears about immigration and manipulation of migrant flows has created economic and social pressures
Migrant crisis on the Polish-Belarusian border (2021)	Geopolitical tensions between EU and Belarus, anti-immigration rhetoric in Eastern Europe	Belarus used migration as political pressure and propaganda to divide EU countries
Intervention in the Catalan independence referendum (2017)	Regional tensions between Spanish government and Catalan authorities	Disinformation campaigns amplified separatist-propagandist narratives and cyber-attacks aimed to destabilize the government

Hybrid threat	Vulnerabilities	How to adapt tactics
Intervention in the political crisis in Venezuela (2019)	Collapsing economy, political instability, lack of popular support for Maduro	Economic tactics included international sanctions and disinformation to manipulate international opinion
Hybrid threats in Venezuela (2019-present)	Dysfunctional economy, tight government control over institutions and media	Disinformation was used for internal control and economic sanctions were used to weaken the economy and the opposition
Political crisis in Belarus (2020-present)	Lack of a well-organized opposition, external support from Russia	Disinformation has been used to discredit the protests and Russian support has strengthened the regime
China's influence in Southeast Asia (2020-present)	Economic dependence on China, territorial disputes in the South China Sea	China has used economic coercive diplomacy and propaganda to control regional states
China's interference in Taiwan's politics (2019-present)	Taiwan's limited international recognition, economic dependence on China	China has stepped up economic pressure and cyber-attacks on Taiwan, accompanied by disinformation
Political and security crisis in Mali (2012-present)	Political instability, presence of jihadist groups, dependence on international aid	Jihadists used disinformation for recruitment and exploited social tensions by manipulating access to natural resources
Iran's cyber interference campaign (2018-present)	Geopolitical tensions, severe economic sanctions, vulnerable cyber infrastructure	Iran deployed sophisticated cyber-attacks and disinformation campaigns to destabilize its external adversaries
Russia's influence in the Western Balkans (2014-present)	Ethnic tensions, political instability, low EU economic interest	Russia used propaganda to exacerbate ethnic tensions and logistical support for pro-Russian parties in the region

These cases show that each state was vulnerable to certain types of hybrid tactics, and the actors involved adapted their actions to the local context and specific weaknesses.

In conclusion, the study of these cases allows to formulate a recommendation on the need for an integrated and proactive approach to counter the sophisticated strategies of modern hybrid threats. It also emphasizes the need and importance of multidisciplinary monitoring, as authorities and experts need to constantly monitor a wide range of factors (from cyber activities to media narratives) in order to detect and respond effectively to hybrid threats. In terms of response strategies, it is essential to develop countermeasures that are as synergistic and interconnected as adversaries' hybrid tactics, combining cyber security, public communication strategies and economic resilience.

PARAMETERS OF A POSSIBLE INTEGRATED PREDICTIVE MODEL FOR HYBRID THREAT RISK ASSESSMENT

The implementation of a predictive model for hybrid threat analysis requires an integrated methodological approach able to combine and correlate variables from multiple domains (Valenza et al., 2022). The model needs to function as an adaptive mechanism that evolves with changes in the international security, economic and technological environment, thus enabling the anticipation and early detection of potential hybrid attacks. At the same time, it is generally accepted that *"Hybrid threats are traditionally difficult to anticipate ... but it is essential to analyse them in order to execute responses in a timely manner"* (Bertolini et al., 2023).

In a predictive hybrid threat analysis, the model used must be based on a set of essential parameters that reflect both the current context and previously identified patterns. These parameters are essential for creating a comprehensive situational awareness and for assessing the likelihood of a hybrid threat and its impact. Taking into account the typology of tactics described above, as well as the fact that *"Geopolitical cyberspace issues are closely linked to political, economic, social and cultural considerations"* (Douzet, 2014), we believe that such a model should include parameters that can be grouped into the following categories: ***geopolitical, cyber, economic, socio-cultural, media and informational, political*** and ***technological***.

We present in the following paragraphs the main parameters that we believe should be included in such a model, as well as details on the content of each of them, as follows.

A. Geopolitical parameters

These can be described by a set of specific sub-indicators, such as ***international tensions*** (the level of tension between states or regional blocs – e.g. latent conflicts, economic sanctions, territorial competition), the ***stability and cohesion of international alliances and agreements*** (NATO or the EU, and the effect of possible

ruptures on regional security), ***changes in national politics*** (legislative or policy changes that could influence a state's position on the international stage: elections, changes of government or economic policies that may provoke international reactions) and ***humanitarian/social crises*** (humanitarian crisis situations, mass migrations or internal social tensions that may be exploited by hybrid actors for societal destabilization).

B. Cyber parameters

They can be described by a set of specific sub-indicators, such as the ***volume and nature of cyber-attacks*** (the frequency and type of cyber-attacks – phishing, ransomware or DDoS attacks – detected against a specific target), ***known cyber-vulnerabilities*** (the level of exposure of critical infrastructure to cyber-attacks, including lack of software updates, unauthorized access or weak security practices), ***cyber capabilities of the actors involved*** (associated indicators ensue from the assessment of technical capabilities and resources available to known hybrid actors – nation states or cyber groups – that could launch an attack).

C. Economic parameters

These can be described by a set of specific sub-indicators, such as ***economic dependence on critical resources*** (economic vulnerabilities related to dependence on certain resources or suppliers – energy and raw materials, which could be leveraged in hybrid strategies), ***economic fluctuations and crises*** (economic indicators such as inflation, currency fluctuations, stock market declines or financial crises that can be exploited by hybrid actors for destabilization), and ***economic sanctions and trade*** (the impact of international sanctions or trade restrictions on a country or region and the way they could amplify existing economic vulnerabilities).

D. Social and cultural parameters

Those can be described by a set of specific sub-indicators, such as ***social divisions*** (the degree of social and political polarization, ethnic or religious tensions and other forms of fragmentation that can be exploited by disinformation and propaganda), ***public sentiment and trust in institutions*** (population's level of trust in government institutions, media and other key institutions – declining trust may facilitate hybrid disinformation actions), and ***social media activity and influence*** (monitoring dominant narratives on social networks and identifying disinformation or coordinated influence campaigns).

E. Media and information parameters

For this indicator, the set of specific sub-indicators can include the ***spread of disinformation*** (the frequency and extent of identified disinformation campaigns

and the types of narratives used to manipulate public opinion), ***media control and manipulation*** (the degree of control over the media and influence over the public agenda, including tactics to amplify messages through alternative channels and fake accounts) and ***public resilience*** (the level of media literacy and public resilience to disinformation, which influences the effectiveness of hybrid information campaigns).

F. Policy Parameters

These can be described by a set of specific sub-indicators, such as ***internal political stability*** (internal stability and unity of government, risk of revolts or opposition movements that could be encouraged by external actors), ***national security policies*** (effectiveness of security policies and the ability of the state to respond to hybrid threats through institutions such as the military, police and intelligence services), ***relations with external actors*** (level of cooperation or conflict with other states that may influence the likelihood of external hybrid action, and strategic alliances).

G. Technological parameters

For this indicator, the set of specific sub-indicators may include ***access to advanced technologies*** (the ability of actors to access advanced technologies – artificial intelligence, drones and advanced encryption that can be used in hybrid operations), ***innovations in communications and media*** (the role of emerging technologies in facilitating or countering hybrid campaigns, including the use of decentralized platforms or encrypted messaging applications).

CONCLUSIONS

Based on these parameters and the sets of specific sub-indicators identified, a predictive model can be built to provide a risk assessment for various hybrid threat scenarios. This paper aims only to suggest how it can be implemented and the essential elements to be considered, leaving further aspects for future research.

For this model to be functional, a fundamental aspect is the continuous collection and integration of data from various sources. According to Shan et al. (2024*) "A predictive analytics mechanism, integrated with threat intelligence platforms, utilizes historical data and current trends to forecast which attack vectors and potential targets are likely".* Ideally, implementation begins by building a data infrastructure that gathers information from a variety of relevant sources: geopolitical reports, real-time economic data, cybersecurity analytics, and social data (including analytics based on social network intelligence). This data infrastructure can be supported by a centralized system capable of harmonizing and constantly updating datasets in a dynamic way, reflecting recent developments.

A key element in this process is machine learning algorithms, which give the model the ability to identify patterns in historical and contemporary datasets. By training the algorithms with data from past hybrid scenarios (both successful and unsuccessful), a model can be built that detects correlations between different risk factors. These factors are found in geopolitical, cyber, economic, political and informational parameters, which together form the structure of a hybrid attack. For example, sudden changes in international relations or geopolitical tensions, combined with increased cyber activity in a particular region, can be early indicators of a coordinated hybrid attack.

Another key aspect is how the data is analysed to simulate potential scenarios. The model should be able to generate multiple simulations exploring different directions of hybrid threat evolution based on changes in geopolitical or economic parameters. These simulations can consider not only an isolated event, but also the synergy between different tactics commonly used in hybrid attacks: cyber-attacks combined with disinformation campaigns or the use of economic pressures to destabilize vulnerable targets.

For this model to be successfully implemented, an early warning system must also be developed. It should be programmed to trigger automatic alerts when the combination of factors reaches certain critical thresholds. For example, a rise in social tensions combined with an increase in cyber-attacks and disinformation campaigns may suggest that a hybrid crisis is imminent. Critical thresholds should be defined based on the analysis of past scenarios, and constant adjustments should be built into the system as new information becomes available.

Another important dimension in implementation is the resilience component. Once the model identifies a possible threat, it is important that the responsible authorities have a set of proactive measures in place, including building cyber resilience, implementing campaigns to increase public trust in national and international institutions, and working with international partners to counter the effects of hybrid threats in a coordinated manner.

In this way, the predictive model has the potential to become an essential tool for political and military decision-makers to plan their resources to prevent and mitigate the impact of hybrid threats before they cause significant damage. With a flexible structure and constant updating of data, the model can provide a comprehensive framework for anticipating threats, mitigating risks, and enhancing the safety of critical infrastructure and national security.

BIBLIOGRAPHY:

1. Arcos, R. (2021). *Information influencing in the Catalan illegal referendum and beyond*. In: Hybrid Warfare. DOI:10.5040/9781788317795.0023.
2. Astapova, A., Navumau, V., Nizhnikau, R., Polishchuk, L. (2022). *Authoritarian co-optation of civil society: The case of Belarus*. Europe-Asia Studies, 74(1), pp. 1-30.
3. Aulia, J.D., Kurniati, E. (2024). *Analysis of Russian factors supporting Nicolas Maduro in the Venezuelan crisis from Alexander Wendt's constructivist perspective.* Siyar Journal, 4(1), pp. 59-73, https://jurnalfisip.uinsa.ac.id/index.php/siyar/article/download/584/334, retrieved on 12 June 2024.
4. Barberà, O. (2020). *All fake? Information disorders and the 2017 referendum in Catalonia*. In Misinformation in Referenda (pp. 281-298). Routledge.
5. Beaton, A.C. (2021). *Social Media in Venezuela: A Tool for Authoritarians, a Boost to Social Movements, or Both?* Doctoral dissertation, Monterey, CA; Naval Postgraduate School, https://apps.dtic.mil/sti/trecms/pdf/AD1164874.pdf, retrieved on 12 August 2024.
6. Bertolini, M., Minicozzi, R., Sweijs, T. (April 2023). *Ten Guidelines for Dealing with Hybrid Threats. A Policy Response Framework*. The Hague Centre for Strategic Studies, https://hcss.nl/wp-content/uploads/2023/04/Guidelines-for-the-Deterrence-of-Hybrid-Threats-HCSS-2023.pdf, retrieved on 17 June 2024.
7. Bodnar, A., Grzelak, A. (2023). *The Polish–Belarusian border crisis and the (lack of) European Union response*. Białostockie Studia Prawnicze, 28(1), pp. 57-86, https://intapi.sciendo.com/pdf/10.15290/bsp.2023.28.01.04, retrieved on 17 June 2024.
8. Braghiroli, S., Makarychev, A. (2018). *Redefining Europe: Russia and the 2015 refugee crisis.* Geopolitics, 23(4), pp. 823-848
9. Cañizález, A., Hernández, L., Torrealba, L. (2020). *Disinformation as a Society-Wide Threat: Journalism and 'Fakecracy' in Venezuela*. In *Fake news is bad news – hoaxes, half-truths and the nature of today's journalism*, https://www.intechopen.com/chapters/73501, retrieved on 12 May 2024.
10. Chaguaceda, A., Pelaez, J.C., Puerta, M.I. (2023). *Illiberal Narratives in Latin America: Russian and Allied Media as Vehicles of Autocratic Cooperation*. Journal of Illiberalism Studies, vol. 3, no. 2 (2023): pp. 111-123.
11. Chang, H.C H., Haider, S., Ferrara, E. (2021). *Digital civic participation and misinformation during the 2020 Taiwanese presidential election*. Media and Communication, vol. 9, no. 1, pp. 144-157, DOI: 10.17645/mac. v9i1.3405, retrieved on 12 May 2024.
12. Cipan, V., Kirichenko, D. (2024). *Russian influence and disinformation operations in the Balkans*. Georgetown Security Studies Review, vol. 11, no. 2, pp. 65-85.
13. Cox, K., Marcellino, W., Bellasio, J., Ward, A., Galai, K.&Meranto, S., Paoli, G. P. (2018). *Social media in Africa*. *A double-edged sword for security and development.* RAND Europe, https://www.undp.org/sites/g/files/zskgke326/files/migration/africa/UNDP-RAND-Social-Media-Africa-Research-Report_final_3-Oct.pdf, retrieved on 22 May 2024.
14. Douzet, F. (2014). *Understanding cyberspace with geopolitics*. Hérodote, 2014/1, no. 152-153, pp. 3-21, https://shs.cairn.info/journal-herodote-2014-1-page-3?lang=en, retrieved on 17 June 2024.

15. Elswah, M., Alimardani, M. (2021). *Propaganda chimera: Unpacking the Iranian perception information operations in the Arab world*. Open Information Science, 5(1), pp. 163-174.
16. Ferchen, M., Mattlin, M. (2023). *Five modes of China's economic influence: Rethinking Chinese economic statecraft*. The Pacific Review, 36(5), pp. 978-1004, https://www.tandfonline.com/doi/pdf/10.1080/09512748.2023.2200029, retrieved on 22 May 2024.
17. Ferrara, E. (2017). *Disinformation and social bot operations in the run up to the 2017 French presidential election*, SSRN First Monday 22(8), http://dx.doi.org/10.2139/ssrn.2995809, retrieved on 22 May 2024.
18. Galeotti, M. (2019). *Russian political war: moving beyond the hybrid*. Routledge.
19. Giannakopoulou, S. (2022). *How social media mobilize the social and political reaction in authoritarian regimes: The Belarus experience*. Faculty of Economic and Political Sciences, https://ikee.lib.auth.gr/record/341645/files/GRI-2022-36486.pdf, retrieved on 13 June 2024.
20. Gilbert, A., Bazilian, M.D., Gross, S. (2021). *The emerging global natural gas market and the energy crisis of 2021-2022*. Foreign Policy, Brookings, 1, pp. 1-10, https://www.brookings.edu/wp-content/uploads/2021/12/FP_20211214_global_energy_crisis_gilbert_bazilian_gross.pdf, retrieved on 22 May 2024.
21. Gross, S., Stelzenmüller, C. (18 June 2024). *Europe's messy Russian gas divorce*, Brookings Institution, https://www.brookings.edu/articles/europes-messy-russian-gas-divorce/, retrieved on 22 August 2024.
22. Hardy, J. (2022). *Moving the goalposts: A Comparative case study analysis of the Belarusian regime*. Sciences, 10(9), pp. 100-107.
23. Hartnett, S.J., Su, C. (2021). *Hacking, debating, and renewing democracy in Taiwan in the age of "post-truth" communication*. Taiwan Journal of Democracy, 17(1), pp. 21-43.
24. Hoffman, F. (2007). *Conflict in the 21st Century: The rise of hybrid wars*. Potomac Institute for Policy Studies.
25. Hung, T.C., Hung, T.W. (2022). *How China's cognitive warfare works: A frontline perspective of Taiwan's anti-disinformation wars*. Journal of Global Security Studies, 7(4), pp. 1-18, https://doi.org/10.1093/jogss/ogac016, retrieved on 22 June 2024.
26. Jędrzejczyk-Kuliniak, K. (2023). *Polish-Belarus Border in the Political Narrative During the Migration Crisis in 2021-2022*, in Producing Cultural Change in Political Communities: The Impact of Populism and Extremism on the International Security Environment (pp. 159-181). Cham: Springer Nature Switzerland.
27. Kase, L.M. (2024). *The European Case for Kosovo, Serbia, and North Macedonia: A Western Balkan Focus*, https://digitalcommons.liberty.edu/cgi/viewcontent.cgi?article=1461&context=hsgconference, retrieved on 22 August 2024.
28. Karolewski, I.P., Benedikter, R. (2018). *Europe's refugee and migrant crisis: Political responses to asymmetrical pressures*. Politique européenne, (2), pp. 98-132, https://shs.cairn.info/revue-politique-europeenne-2018-2-page-98?lang=fr, retrieved on 22 May 2024.
29. Kuvekalović, J., Stojanović, G., Filipović, M. (2017). *Security implications of the migrant crisis in Europe 2015-2016*, Faculty of Security Studies.

30. Lehto, M. (2022). *Cyber-attacks against critical infrastructure.* In Cyber security: Critical infrastructure protection (pp. 3-42). Springer International Publishing. Methods in Applied Sciences, 56, https://doi.org/10.1007/978-3-030-91293-2_1, retrieved on 22 May 2024.
31. Lika, L. (2021). *The Western Balkans at the crossroads of European integration and the emerging powers' projection of influence*. The Journal of Cross-Regional Dialogues, no. 2/2021, pp. 7-30, https://orbi.uliege.be/bitstream/2268/265217/1/Article%20Liridon%20Lika%20JCRD.pdf, retrieved on 22 May 2024.
32. Maza, K.D., Koldas, U., Aksit, S. (2020). *Challenges of countering terrorist recruitment in the Lake Chad region: The case of Boko Haram.* Religions, 11(2), p. 96.
33. Menn, J. (2020). *Russian-backed organizations amplifying QAnon conspiracy theories, researchers say*, Reuters, https://www.reuters.com/article/us-usa-election-qanon-russia-idUSKBN25K13T, retrieved on 12 May 2024.
34. Mumford, A. (2021). *Hybrid Warfare: Past, Present, and Future*. Polity Press.
35. National Intelligence Council (10 March 2021). Foreign Threats to the 2020 US Federal Elections, https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf, retrieved on 22 May 2024.
36. NATO (2010). *A hybrid warfare strategy*. NATO Review.
37. NATO (2020). *NATO's Approach to countering hybrid warfare*. NATO Strategic Communications Centre of Excellence.
38. Nübel, K. A. (2020). *THE rise of new types of war: A case study on Russian hybrid warfare in the Ukrainian crisis in 2014*, Master's thesis, University of Twente, https://essay.utwente.nl/82683/1/N%C3%BCbel_MA_BMS.pdf, retrieved on 22 May 2024.
39. O'Connor, S., Hanson, F., Currey, E., Beattie, T. (2020). *Cyber-enabled foreign interference in elections and referendums* (vol. 28). Canberra: Australian Strategic Policy Institute, https://ad-aspi.s3.amazonaws.com/2020-10/Cyber%20enabled%20foreign%20interference_0.pdf, retrieved on 22 May 2024.
40. Otaiku, A.A. (2018). *A framework for hybrid warfare: threats, challenges and solutions*. Journal of Defense Management, https://www.longdom.org/open-access/a-framework-for-hybrid-warfare-threats-challenges-and-solutions-25432.html, retrieved on 22 May 2024.
41. Pal, D. (2021). *China's influence in south Asia. Carnegie Endowment for International Peace*, https://carnegie-production-assets.s3.amazonaws.com/static/files/202110-Pal_SouthAsiaChina_final1.pdf, retrieved on 22 May 2024.
42. Pindjak, P. (2014). *Deterring hybrid warfare: A NATO Perspective*. NATO Defense College Research Paper, 123, pp. 1-8.
43. Pindják, P. (2019). *The Hybrid threat: Blurring the line between war and peace*. Journal of Strategic Studies, 42(3-4), pp. 271-292.
44. Popkostova, Y. (2022). *Europe's energy crisis conundrum*. European Union Institute for Security Studies, https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief_2_Energy%20Crisis.pdf, retrieved on 12 May 2024.
45. Rid, T., Hecker, M. (2021). *The rise of hybrid warfare*. Oxford University Press.
46. Rouvinski, V. (2019). *Russian-Venezuelan relations at a crossroads*. Woodrow Wilson International Center for Scholars, Latin American Program, 1.

47. Rozental, D., Jeifets, L. (2022). *Russia and Venezuela: Russia's Gateway to Latin America*. In Rethinking Post-Cold War Russian – Latin American Relations (pp. 193-205). Routledge.
48. Schmidt, J.D. (2008). *China's soft power diplomacy in Southeast Asia*. The Copenhagen Journal of Asian Studies, 26(1), pp. 22-49.
49. Shan, A., Myeong, S. (2024). *Proactive threat hunting in critical infrastructure protection through hybrid machine learning algorithm application*. Sensors, 24(15):4888, p. 5, https://doi.org/10.3390/s24154888, retrieved on 12 May 2024.
50. Spataro, J.G. (2019). *Iranian Cyber Espionage*. Utica College ProQuest dissertations & theses, https://www.proquest.com/openview/7816e26f17ba341674713046f4a249fa/1?pq-origsite=gscholar&cbl=18750&diss=y, retrieved on 22 May 2024.
51. Starodubtseva, A. (2021). *Russian hybrid warfare in Ukraine: Comparative analysis of two cases and identification of critical elements in the successful application of hybrid tactics*. Master thesis, Praga: Charles University, Faculty of Social Sciences, Department of Security Studies, https://dspace.cuni.cz/bitstream/handle/20.500.11956/124589/120381167.pdf?sequence=1&isAllowed=y, retrieved on 22 May 2024.
52. Stokel-Walker, C. (2024). *Medical misinformation on social media – are the platforms equipped to be the judge?,* The BMJ, 2024, DOI: 10.2196/17187.
53. Suarez-Lledo, V., Alvarez-Galvez, J. (2021). *Prevalence of health misinformation on social media: systematic review*. J. Med Internet Res 2021; 23(1): e17187, https://www.jmir.org/2021/1/e17187, retrieved on 22 May 2024.
54. Thurston, A., Lebovich, A. (2013). *A handbook on Mali's 2012-2013 crisis*. Institute for the Study of Islamic Thought in Africa, https://sahelresearch.africa.ufl.edu/wp-content/uploads/sites/170/ISITA-13-001-Thurston-Lebovich.pdf, retrieved on 12 May 2024.
55. Tsiklauri, G. (2021). *Hybrid Warfare in Cyber domain: Case Study of hybrid threats in cyberspace.* Master thesis, Praga: Charles University, Faculty of Social Sciences, Department of Security Studies, pp. 42-48, https://dspace.cuni.cz/bitstream/handle/20.500.11956/127657/120387067.pdf?sequence=1&isAllowed=y, retrieved on 22 May 2024.
56. Vakarchuk, K.V. (April 2020). *The impact of the media on the Catalonia referendum*. Rhetoric and Communications, nr. 43, ISSN 1314-4464, https://rhetoric.bg/wp-content/uploads/2020/06/Vakarchuk-issue-April-2020-pp.83-95.pdf, retrieved on 12 May 2024.
57. Valenza, F., Karafili, E., Steiner, R.V., Lupu, E.C. (2022). *A hybrid threat model for smart systems*. In: IEEE transactions on dependable and secure computing, vol. 20, nr. 5, pp. 440 -4417, ISSN 1545-5971, Elettronico.
58. Vilmer, J.B.J., Conley, H.A. (2018). *Successfully countering Russian electoral interference*. Washington: Center for Strategic & International Studies, https://www.jbjv.com/IMG/pdf/180621_Vilmer_Countering_russiam_electoral_influence.pdf, retrieved on 12 May 2024.
59. Wentzell, T.D. (2021). *Russia's Green Men: The Strategic Storytellers of Hybrid Warfare*. Canadian Military Journal, 22(1), pp. 42-48, https://www.journal.forces.gc.ca/PDFs/CMJ221Ep42.pdf, retrieved on 22 May 2024.

60. Wither, J.K. (2016). *Making sense of hybrid warfare*. Connections: The Quarterly Journal, 15(2), pp. 73-87.
61. Wojnowski, M. (2021). *Russian interference in the U.S. Presidential elections in 2016 and 2020 as an attempt to implement a revolution-like information warfare scheme*, în US democracy as the target of Russian secret services, Warsaw Institute, Polonia, https://warsawinstitute.org/wp-content/uploads/2021/07/RS_06-2021_EN.pdf, retrieved on 22 May 2024.
62. Zdanowicz, M. (2023). *The migration crisis on the Polish-Belarusian border.* Białostockie Studia Prawnicze, 1(28), pp. 103-115, https://intapi.sciendo.com/pdf/10.15290/bsp.2023.28.01.06, retrieved on 22 May 2024.