Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 6, 1312-1321
2024
Publisher: Learning Gate
DOI: 10.55214/25768484.v8i6.2248
© 2024 by the authors; licensee Learning Gate

Improvement of public management mechanisms in the direction of countering hybrid threats to national security

Serhii Bielai[1*], Vladislav Emanov[2], Volodymyr Trobiuk[3], Kostiantyn Sporyshev[4], Andrii Petik[5]
[1,2,3,4,5]National Academy of the National Guard of Ukraine, Kharkiv, Ukraine; belwz3@ukr.net (S.B.) d1ss@ukr.net (V.T.) spor_kos@ukr.net (K.S.) andrew.avv82@gmail.com (A.P.)

Abstract: The article represents an attempt of conceptual comprehension of the phenomenon of hybrid threats, which, although inextricably linked with hybrid warfare, still may not include armed conflict even with participation of only irregular combatants. Rather, hybrid threats are aimed at undermining adversary' infrastructure or gaining much control over it, and sow internal societal tension. Geopolitical components, drivers and factors of hybrid threats are analyzed. Based on analysis of literature sources and practical cases, it is concluded that anticipatory approach is the only way of effective combatting hybrid threats, but implementation of this approach could be backed by a collective change in mentality and a stronger national narrative, while the initiative should be suggested by public administration. There is a need for fresh thinking while expanding the traditional enemy-centric threat assessment and response.

Keywords: *Conflict, Intelligence, Hybrid threats, National Security, Technology.*

1. Introduction

One of the current risks to any state's national security is hybrid threats. They show how the nature of international security has changed significantly. Numerous non-military instruments are included in certain hybrid warfare approaches. The opponent can concurrently employ mixtures of conventional and irregular warfare techniques, together with political, military, economic, social, and informational means, under the framework of hybrid threats.

Among the the main elements of the hybrid dangers of today, there is the growing assertiveness of non-state actors. Threats, whether or whether they are used as proxies by state actors, are increasingly the product of terrorist organizations or individual citizens. Furthermore, big international tech organizations, multinational enterprises, or powerful people are becoming more and more involved in modern wars, whether knowingly or unknowingly, because many hybrid assaults are executed utilizing novel, frequently dual-use technology. They are employed as resources in addition to being targeted on one hand.

Hybrid threats may involve the use of a combination of conventional and irregular warfare by the enemy, along with political, military, economic, social, and informational means. In this regard, the following best practices of leading states in preparing for, responding to, and countering hybrid threats can be highlighted, which have a number of common features (Hoffman, 2018):

- They cover all systems of state governance while simultaneously engaging the capabilities of the entire society;
- They assess vulnerabilities. First of all, it is necessary to focus on the information sphere, against threats in the telecommunications environment: espionage, digital attacks, and information manipulation;

© 2024 by the authors; licensee Learning Gate
* Correspondence: belwz3@ukr.net

- They pay special attention to cybersecurity, since the cyber sphere, along with social networks, are the main components of hybrid threats;
- They take a creative approach to working with the non-state sector, which controls the telecommunications infrastructure subject to state protection. For example, the Estonian Cyber Defense Unit is part of the Estonian Defense League, a voluntary military organization for national defense;
- They depend on general situational awareness, intelligence, high-quality analysis and proactive counterintelligence activities. In some countries, this has required changing laws to give intelligence services greater powers to collect information both domestically and internationally.

Namely, the measures to counter hybrid threats act as the main tool for managing the risks of a decrease in the level of national security (Kryshtanovych et al. 2024b; 2023c, 2023d, 2923e). However, while national security parameters are the object of management by government bodies, the risks of the emergence of hybrid threats are exogenous factors that are weakly amenable to the corresponding management influence on the part of government bodies. Evidence of this is the vulnerability of states to hybrid threats, which remains even when using an impressive arsenal of measures to counter these threats. The risk of a decrease in the level of national security of a state due to hybrid threats should be understood as the likelihood of negative informational, psychological, cultural, political, and economic consequences of the materialization of threats caused by unreliable assessments of their danger or the objective unpredictability and uncontrollability of certain factors (Regan and Sari, 2024). The development of a methodology for managing the risks of reducing the national security of the state in the context of the impact of hybrid threats requires a consistent justification of the corresponding tasks and functions of public management institutions (Kondur et al., 2024).

2. Literature Review

The space between state-on-state (external) and intrastate (internal) conflicts is occupied by the hybrid threat (Sadik, 2017). American General Dempsey (cited in Raugh, 2015, p. 6) defines the hybrid threat as follows: "An area of conflict where actors blend techniques, capabilities, and resources to achieve their objectives… Hybrid conflicts also may be comprised of state and non-state actors working together toward shared objectives…Hybrid conflicts serve to increase ambiguity, complicate decision-making, and slow the coordination of effective responses".

Richard J. Aldrich, a professor of international security at the University of Warwick's Department of Politics and International Studies (cited in Sadik, 2017), claims that hybrid threats take advantage of the transitional spaces that exist between law and illegality, between the public and private spheres, and even between real space and cyberspace. There are helpful differences to be drawn between hybrid warfare and other hybrid threats that are at a lower spectrum, despite the fact that this is a purposefully ambiguous region.

Because hybrid threats offer several rungs on the ladder of escalation, states use them against strategic competitors to force their smaller allies without running the danger of all-out conflict (Nekhai et al., 2024). Major governments on both sides frequently turn a "Nelsonian eye" to such aggression since they are aware that they employ the same hybrid strategies (Searight, 2020).

The Advisory Council on International Affairs in the Netherlands (AIV) addresses the complex issue of hybrid threats from three distinct angles in its advisory report: physical, virtual, and cognitive. The world as we perceive it with our senses is related to the physical dimension. Information processing, protection, and distribution are all part of the virtual dimension. The cognitive component is the sum of social perceptions, observations, and intentions. AIV focuses in particular on the effects of hybrid actions (or assaults) on the virtual and cognitive dimensions, in addition to the apparent risks in the physical dimension. This is because governments find it extremely difficult to properly foresee this sort of threat in terms of policy. Attacks that are physical are typically easier to identify and more noticeable. Moreover, physical security and protection responsibilities are often evident from the start

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 6: 1312-1321, 2024
DOI: 10.55214/25768484.v8i6.2248
© 2024 by the authors; licensee Learning Gate

and are, for the most part, well-organized. On the other hand, there is a great deal of ambiguity around cognitive and virtual attribution and protection (Borch and Heier, 2024).

State security agencies as strategic management bodies (actors) define the principles, tasks, and functions of management of risk of a reduction in the state national security level (Zayats et al., 2024). In turn, state authorities directly implement risk management processes based on the implementation of forecasting, coordination, organization, control, and regulation functions in interaction with authorities (subjects of the national security sector).

The principles of risk management in the plane of a reduction in the national security of the state under the influence of hybrid threats described in scientific and expert literature can generally be systematized as follows (see Table 1):

Table 1.
Principles of managing the risks of reducing the national security of the state in the context of the impact of hybrid threats.

Principles	**Contents of principles**	**Methods for achieving compliance with the principles**
Integration	Prompt and rapid response to the emergence of new risks (Including their individual factors)	Consideration of risk management principles by government bodies
Timeliness and efficiency of response	The most prompt response to the emergence of a risk based on the criterion of assessing the damage caused by this risk	Coordination between government bodies, prompt exchange of information with management bodies, timely implementation of all decisions and recommendations
Consistency of analytical support and information sufficiency	Registration and analysis of the most complete volume of information on the state of factors that determine the level of all identified risks of reducing national security	Resource provision of departments and bodies authorized to provide information support for risk management processes
Systematicity	Emergent interaction of government bodies	Efficient performance of coordinating functions by the authorized national security management body
Continuous improvement of the risk management mechanism	Continuous updating of methods for managing identified risks, taking into account global experience, trends, and the nature of hybrid threats	Regular stress tests, as well as checks on the adequacy of the methods used to identify, assess, and manage risks

Every nation seeks to implement practical countermeasures against hybrid threats. Specifically, in 2019 and 2020, the Institute of International Affairs and the National Security Council of Iceland collaborated to organize a number of events centered around hybrid threats. Numerous specialists from outside and locally took part in the activities. Hybrid threats, the interconnectedness of issues and the variety of conventional and unconventional tactics, hybrid defense and the preservation of democratic ideals, and the significance of building resilience were some of the subjects covered (Herciu, 2019).

However, experts rightly note that modern war is moving from the real world to the virtual world - cyberspace, where the real confrontation of superpowers is unfolding; moreover, war from a purely physical phenomenon is increasingly moving into the spiritual and ideological plane, when modern

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 6: 1312-1321, 2024
DOI: 10.55214/25768484.v8i6.2248
© 2024 by the authors; licensee Learning Gate

technologies are used to control mass consciousness; finally, the global financial and especially banking sectors provide serious economic levers of influence on the state (Costa, 2021).The landscape of hybrid threats is so complex and dynamic that the reaction on it should be even not quick but anticipatory. This is, in fact, the core problem of national public administrations' efforts in combatting hybrid threats – lack of anticipatory approach determine the country' vulnerability to hybrid threats.

On the severity spectrum, hybrid attack effects, meanwhile, are in the middle (Ferrag et al., 2023). The element of surprise is one of the causes of this. The purpose of hybrid conflict strategies, whether employed by state actors or non-state actors, is to exploit the ambiguity of their acts. Before international organizations can firmly attribute actions and organize efficient countermeasures, state organizations can achieve significant combat victories through the use of irregular or proxy armies. Thus, anticipatory approach is actually the only effective way today to prevent the implementation of hybrid threat or at least diminish their consequences.

2. Methods

The methodological basis of this study is the phenomenon of "hybrid threats" as a new phenomenon. In the process of studying the research topic, methods of comparative analysis were used, observing the principles of scientificity and objectivity, as well as the unity of theory and practice. The work employs the principles of modern political science applied to the analysis of international political processes, namely the method of system analysis and the scientific paradigm of neorealism.

3. Results

In the ever-changing global setting, all countries and organizations need to be ready to confront hybrid threats to their security. As science and technology advance, nation-states and their leaderships must to be prepared with preventive measures for security on several fronts.

According to Chinese colonels Liang and Xiansui (1980), the enemy may use the following tools to carry out hybrid operations: financial trade, resources, media/propaganda, ideology/religion, forced population shifts/migration, network intelligence, psychological, technological, smuggling, drug warfare, and economic/economic aid incentives. Furthermore, it appears that the primary tool of hybrid warfare is the infamous "fifth column", which consists of enemy-controlled influence agents.

In particular, the EU member states and NATO allies are taking on hybrid threats from both an offensive and defensive standpoint. Since 2015, NATO policy has taken into account the phenomena of hybrid threats, and since 2016, hostile hybrid behavior has been considered a basis for invoking Article 5. To counter hybrid threats, a plethora of new cooperation efforts and investment programs have been introduced. Hybrid threats are taken extremely seriously by the EU. Article 42.7 of the Treaty on European Union, which mandates that EU member states assist one another in the collective defense of the EU, may be activated by a hybrid threat. This holds true for assaults that are hybrid or conventional. Through a number of efforts, such as the development of the EU Hybrid Toolbox, which provides member states with a variety of tools to tackle hybrid threats, the EU hopes to battle these dangers and raise member state awareness of them. Furthermore, strengthening the resistance of European democracies to outside influence is a key component of the Defense of Democracy package, which was unveiled in December 2023, and the specifically crafted 2020 European Democracy Action Plan. In addition, the European Union is funding the acquisition of specialized hardware and software for emerging technologies through the European Defense Agency (EDA), in part to mitigate risks related to the virtual and cognitive domains.

The European Centre of Excellence (CoE) for Countering Hybrid Threats should also be included. A global, independent network-based group called Hybrid CoE advocates for a whole-of-government and whole-of-society strategy to combat hybrid threats. While it is important to comprehend how the security environment is changing, analyzing risks alone is insufficient; one also needs to give practical solutions to resist them (Kussainov al., 2023). Therefore, strengthening member governments' capacities to thwart and fight hybrid threats is the Center's main goal. To do this, best practices are

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 6: 1312-1321, 2024
DOI: 10.55214/25768484.v8i6.2248
© 2024 by the authors; licensee Learning Gate

exchanged, novel concepts and methods are put to the test, and exercises and training programs are offered. Hybrid CoE is particularly crucial since it serves as a venue for strategic talks as well as cooperative training and exercises between the EU and NATO. The excellence is made possible by the cross-governmental and cross-sectoral networks of the Hybrid CoE, which are made up of more than 1,200 practitioners and experts who work on tasks linked to hybrid threats in member nations, the EU or NATO, the commercial sector, and academia. By publishing a wide range of publications and interacting with several partners in the area, the Center hopes to lead the debate on hybrid risks as an actor bridging other players from diverse socioeconomic sectors (Borch and Heier, 2024).

State and non-state actors who employ hybrid tactics to attack political institutions, sway public opinion, and jeopardize the security of NATO people pose risks and challenges to NATO allies simultaneously.

The international community regards the United States as less respectable when it does nothing about hybrid wars. When it comes to countering hybrid dangers like Russia in the Ukraine and ISIL in Iraq and Syria, many people look to the United States for leadership and safety. Unfortunately, because hybrid action lacks attribution and identification for targeting, it is misleading and ambiguous, making it impossible for the United States and its allies to take decisive action. Unchecked hybrid threats raise security tensions throughout the region, which may persuade erstwhile partners to switch from the United States' bandwagoning policy to a regional balancing approach (Regan and Sari, 2024). The choice made by Saudi Arabia to spearhead military operations against terrorists in Yemen is a clear illustration of this. In order to defend its territory, the United States is compelled to step up defensive border-securing measures as concerted international efforts are insufficient to counter hybrid threats outside.

In the Indo-Pacific region, hybrid threats are growing in scope, applicability, and severity due to the combined influence of geopolitical competition and digital technology. Weakening institutions, upended social structures and economies, and increased susceptibility to coercion - particularly from revisionist powers like China - are among the repercussions for individual countries (Regan and Sari, 2024). However, the effects of growing hybrid activities in the Indo-Pacific region go well beyond national boundaries. The Indo-Pacific region is home to a diverse range of political systems and interests, as well as several centers of influence, flashpoints, and an authoritarian force that is becoming more aggressive. Because of its vital role as a hub for social and economic dynamism worldwide, instability in the Indo-Pacific region, whether brought on by hybrid threats or not, has far-reaching effects.

Because hybrid threats operate outside of established frameworks for the exercise of state power and employ unconventional means of accomplishing their goals, governments have frequently encountered difficulties recognizing the activity, defining the danger, and developing appropriate countermeasures. It is difficult to be precise and timely since hybrid threats change over time, are frequently concealed or integrated into regular company operations, and have the potential to reinforce or leverage more established types of coercion. The majority of the time, hybrid threat activity aims to weaken national capacity and confidence as well as interfere with government decision-making processes. These actions diminish national and regional resilience, which might enhance security and stability in the area.

Van Veen et al. (2022) correctly point out that during the past 20 years, regional geopolitical rivalry has benefited from at least three significant boosts: the US invasion of Iraq in 2003, which eliminated the nation as a major Arab power and allowed Iran to gain more influence; the Arab Uprisings in 2011, which prompted Iran and the Gulf states to seek the restoration of the conservative authoritarian status quo; and the US's abrupt withdrawal from the nuclear deal in 2018, which heightened tensions between the US, the UAE, Israel, Saudi Arabia, and the US on the one hand, and an up until then-compliant Iran on the other. Three opposing actor alignments comprise the Middle East today, combining traditional interstate cooperation with the addition of looser networks composed of state, hybrid, and non-state players (refer to Figure 1).

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 6: 1312-1321, 2024
DOI: 10.55214/25768484.v8i6.2248
© 2024 by the authors; licensee Learning Gate

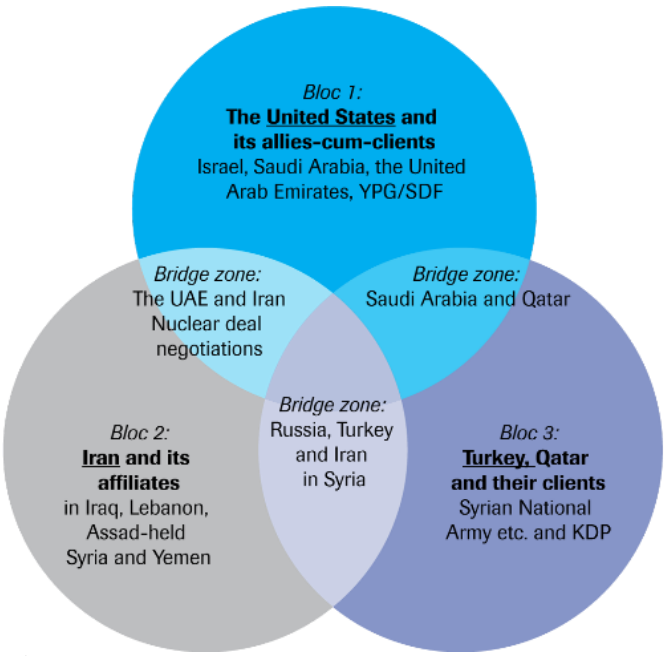

Figure 1.
Key regional blocs shaping geopolitical competition in the Middle East (van Veen et al., 2022)

Hybrid threats are also prevalent in other areas (such as the Asia-Pacific area and, more recently, the former USSR's territory), making it very challenging for state actors to effectively and strategically handle them in order to maintain the sustainability of national security.

4. Discussion

Although crucial, the issue of how to combat hybrid dangers using legal methods is far from simple. Adjectives like "hybrid", "grey", "asymmetric", "unbalanced", and "unconventional" are employed here, although they are not always interchangeable and show how unstable this field is. In fact, we frequently discover that the legal landscape changes as we attempt to address such dangers (Ramskyi et al., 2023). Furthermore, the character of the global environment is become more hybrid. Hybrid operations serve the opposite purpose of those intended by international law, which is to advance security, justice, collaboration, predictability, and common values. In this way, "the tragedy of international law" is mentioned by Aurel Sari in his writing (Sari, 2019, p. 4).

There is a school of thought that suggests the legal tools, procedures, and institutions that are in place today may not be entirely appropriate to stop the extremely unsettling and intricate covert operations of the so-called grey zone, as they were primarily designed to prevent and mitigate Cold War controversies. The latter can be understood as a malicious expression of the idea of peace and can include actions performed by one state that are destructive to another, even if they are not authorized acts of war. It is noteworthy that the post-Cold War era has been marked by far more volatility, characterized neither by open confrontation nor by lasting peace, than it was during the relatively calm pre-Cold War era when all the actors knew where their adversaries lay. In this way, the area of legal ambiguity is where hybrid dangers naturally reside. Because of their modest intensity, they stay below the fighting threshold (Sanz-Caballero, 2023).

As Busol (2020) correctly points out, military might alone is no longer adequate to ensure a state's security in the modern day. China is a prime illustration of this claim, using IT technologies to attack US infrastructure and engaging in aggressive soft power - a tactic that scientists referred to as a "magic weapon" a decade ago (Arghire, 2024). The Five Eyes alliance, an intelligence coalition made up of the

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 6: 1312-1321, 2024
DOI: 10.55214/25768484.v8i6.2248
© 2024 by the authors; licensee Learning Gate

United States, Australia, the United Kingdom, Canada, New Zealand, and New Zealand, was primarily motivated by hybrid threats posed by China.

Critical infrastructure organizations are alerted by government agencies in the Five Eyes nations about the Chinese state-sponsored hacking outfit Volt Typhoon. The attacker, identified as "Volt Typhoon", used stealth tactics to take advantage of pre-existing resources in compromised networks. This tactic is known as "living off the land", and it suggests that malware utilizes pre-existing resources in the target operating system rather than creating a new (and more detectable) file (Davidson, 2024).

Indeed, digitalization also creates vulnerabilities in the physical domain. Most modern infrastructure can be accessed and interfered with through cyberattacks (Alieksieienko et al. 2022; Kryshtanovych et al., 2023a, 2023b; Kryshtanovych et al., 2024). Cyberattacks are difficult to attribute and relatively low-cost in comparison to their impact, making them attractive hybrid tactics. Cyberattacks are also not a new phenomenon; however, since 2020, the number of cyberattacks has climbed steeply, as shown in Figure 2.

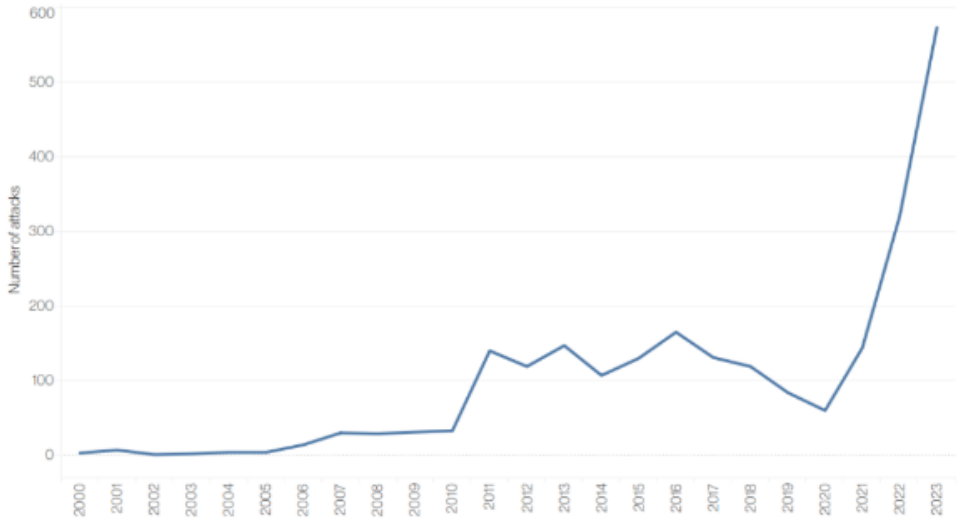

Figure 2.
Number of cyberattacks over time (Romansky et al., 2024).

An "advanced persistent threat group" that has been operational since at least mid-2021 is called Volt Typhoon. It is aimed against US critical infrastructure groups and is thought to be supported by the Chinese government. Guam has received a lot of the group's attention. This US island territory, which is in the Western Pacific, is home to a sizable and expanding military presence, which includes US Air Force, US Marine Corps, and US Navy nuclear-capable submarines. The attackers behind Volt Typhoon most likely wanted to penetrate networks linked to vital US infrastructure in order to interfere with command and control and communications systems and to remain present on the networks for an extended period of time. With the latter strategy, China would be able to control operations in the event of a South China Sea confrontation (Desmond, 2023).

Furthermore, according to UK intelligence, Chinese agents have reportedly made over 20,000 covert internet approaches to UK citizens to date (Corera, 2023). It coincides with a fresh alert to tens of thousands of British companies about the possibility of intellectual property being pilfered. More than 20 instances of Chinese companies considering or actively attempting to obtain sensitive technology developed by UK companies and universities through investments or other means - often through intricate company structures - have also been reported to MI5 intelligence.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 6: 1312-1321, 2024
DOI: 10.55214/25768484.v8i6.2248
© 2024 by the authors; licensee Learning Gate

Using both gentle and forceful power at the same time is not a new idea _ it has been used for millennia. However, globalization and newly developing technology have given rise to new tools for hybrid threats, heightened vulnerabilities across several sectors, and expanded the scope, velocity, and reach of hybrid assaults.

Five higher-level themes in the contemporary global hybrid threat scenario are presented by the Hague Center for Strategic Studies (Romansky et al., 2024): 1) Economic dependency exploitation; 2) weaponization of mass digitalization; 3) reality distortion; 4) manipulation of polarization in society; and 5) diversification of instruments and players. The horizon scan takes into account the vulnerabilities that give rise to risks for each trend, the factors that drive hybrid players, and the hybrid activities or modes of operation that are possible for the future.

According to Coldea (2022), intelligence challenges in countering hybrid threats can be depicted as a scheme (see Fig. 3 below).

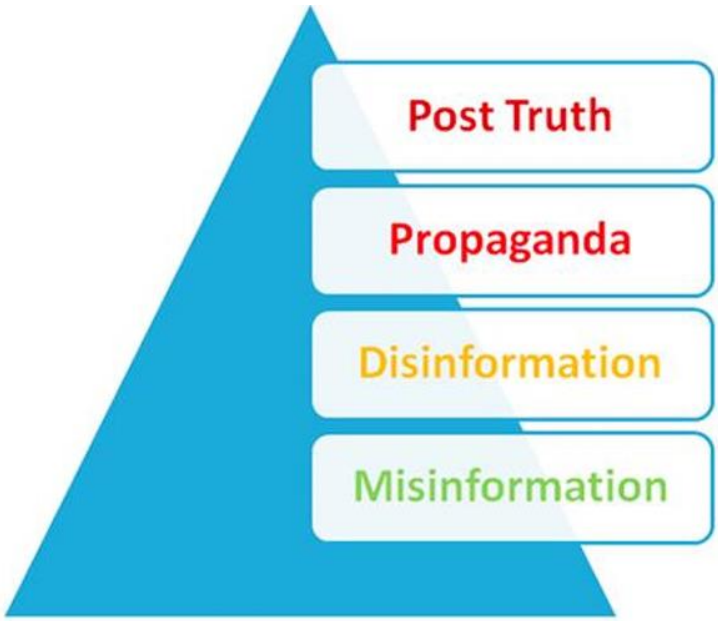

Figure 3.
Intelligence challenges in countering hybrid threats (Coldea, 2022).

An approach including the entire government and society is necessary to counter hybrid threats. This includes:

- Novel policies and doctrine
- Situational understanding of multifaceted, protracted hybrid campaigns
- Increased military and civil readiness
- Creative resiliency and reaction techniques to lessen subversive acts

Approaches to combat hybrid threats, as it was mentioned above, should bear first of all anticipatory nature, based on forecasting and foresight technologies, combining the possibilities of AI to process big data on the one hand and human high-level analytics on the other hand. Moreover, the set of approaches should have matrix systemic form and address the issues of societal resilience, since hybrid threats concern far not only physical infrastructure and military capacities but also the society, in attempts to transform the society into factor of internal tension capable of undermining the country from inside.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 6: 1312-1321, 2024
DOI: 10.55214/25768484.v8i6.2248
© 2024 by the authors; licensee Learning Gate

5. Conclusions

There is a general understanding around the globe that hybrid threats constitute an expanding security issue, although the unresolved discussion that continues to surround the necessity of defining hybrid threats. Fighting these dangers is extremely difficult since, in addition to being a never-ending endeavor, doing so weakens democracy from the inside out. The area where actors operate on the edge of legality is known as the "grey zone". Because threats in the gray area are always changing, we need to be proactive and adaptable in our answers. The functionality of states is continuously and covertly undermined by hybrid activities. A state will be operating against international law, the concept of good faith, and in a non-transparent way if it employs hybrid capabilities. Furthermore at odds with the noninterference concept in domestic matters are hybrid dangers. Therefore, it is evident that hybrid threats violate the concept of peaceful conflict settlement even though they do not involve open violence.

Although laws are necessary to combat these same concerns, hybrid threats take advantage of the absence of them. In order to combat hybrid threats, prevention, social awareness, and education are also necessary, but the law is especially important since actors who utilize these threats blur the lines between what is lawful and criminal. Law-abiding governments should refrain from using the law of armed conflict in response to hybrid tactics unless the attack is deadly. It is imperative that this regulation not be altered. Furthermore, it is not essential to redefine the meaning of the phrases "force", "aggression", "war", "intimidation", or "conflict", since doing so would simply increase misunderstanding.

However, society as a whole is impacted by the problem of hybrid dangers. Public administration should take the lead in suggesting this undertaking, which calls for a stronger national narrative and a shift in collective mindset. While extending the conventional enemy-centric threat assessment and response, new ideas are required.

Highlights:

The article asserts the necessity of anticipatory matrix approach in combatting modern hybrid threats, due to their latent and sudden

Copyright:

© 2024 by the authors. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

References

[1] Alieksieienko, T. et al. 2022. The use of modern digital technologies for the development of the educational environment in the system for ensuring the sustainable development of the region. International Journal of Sustainable Development and Planning 17(8): 2427-2434. https://doi.org/10.18280/ijsdp.170810

[2] Arghire, I. 2024. Five Eyes agencies issue new alert on Chinese APT Volt Typhoon. Security Week. March 20. https://www.securityweek.com/five-eyes-agencies-issue-new-alert-on-chinese-apt-volt-typhoon/

[3] Borch, O., and Heier, T., eds. 2024. Preparing for hybrid threats to security: Collaborative preparedness and response. Routledge.

[4] Busol, O. 2020. The phenomenon of hybrid threats to national security. Legal Ukraine 4: 6-15.

[5] Coldea, F. 2022. Intelligence challenges in countering hybrid threats. National Security and the Future 23(1). DOI: https://doi.org/10.37458/nstf.23.1.2

[6] Corera, G. 2023. MI5 head warns of 'epic scale' of Chinese espionage. BBC. October 18. https://www.bbc.com/news/uk-67142161

[7] Costa, R. 2021. Hybrid threats in the context of European security. Instituto da Defesa Nacional.

[8] Davidson, H. 2024. Explainer: what is Volt Typhoon and why is it the 'defining threat of our generation'? The Guardian. February 13. https://www.theguardian.com/technology/2024/feb/13/volt-typhoon-what-is-it-how-does-it-work-chinese-cyber-operation-china-hackers-explainer

[9] Desmond, D. 2023. Five Eyes publicizes China-backed hackers' attack. Asia Times. May 27. https://asiatimes.com/2023/05/five-eyes-publicizes-china-backed-hackers-attack/

[10] Ferrag, M. et al. 2023. Hybrid threats, cyberterrorism and cyberwarfare. CRC Press.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 6: 1312-1321, 2024
DOI: 10.55214/25768484.v8i6.2248

© 2024 by the authors; licensee Learning Gate

[11] Herciu, A. 2019. Adapted strategies for countering hybrid threats: Consideration on hybrid conflict. LAP LAMBERT Academic Publishing.

[12] Hoffman, F. 2018. Examining complex forms of conflict gray zone and hybrid challenges. Prism 7(4): 30-47.

[13] Kondur, A., et al. 2024. Economic and environmental component in the field of sustainable development management. Quality. 25(201): 7–14. DOI: 10.47750/QAS/25.201.02

[14] Kryshtanovych, M. et al. 2024a. Increasing the effectiveness of state policy in ensuring energy security and environmental protection. International Journal of Energy Production and Management, 9(1): 9-17. https://doi.org/10.18280/ijepm.090102

[15] Kryshtanovych, M. et al. 2024b. Formation of drivers of sustainable development: Administrative and legal support to ensure information security. International Journal of Sustainable Development and Planning, Vol. 19, No. 4, pp. 1611-1619. https://doi.org/10.18280/ijsdp.19043

[16] Kryshtanovych, M. et al. 2023a. Formation of social leadership in the system of public safety and security through the use of modern modeling techniques. International Journal of Safety and Security Engineering 13(2): 317-324. https://doi.org/10.18280/ijsse.130213

[17] Kryshtanovych, M. et al. 2023b. Modeling effective interaction between society and public administration for sustainable development policy. International Journal of Sustainable Development and Planning 18(8): 2555-2561. https://doi.org/10.18280/ijsdp.180827

[18] Kryshtanovych, M. et al. 2023c. Marketing in public administration in the system of ensuring economic security. Financial and Credit Activity Problems of Theory and Practice 5(52): 532-542. https://doi.org/10.55643/fcaptp.5.52.2023.4167

[19] Kryshtanovych, M. et al. 2023d. Optimization of state regulation in the field of safety and security of business: a local approach. Business: Theory and Practice 24(2): 613-621. https://doi.org/10.3846/btp.2023.19563

[20] Kryshtanovych, M. et al. 2023e. An intelligent multi-stage model for countering the impact of disinformation on the cybersecurity system. Ingénierie des Systèmes d'Information 28(1): 41-47. https://doi.org/10.18280/isi.280105

[21] Kryshtanovych, M. et al. 2022. Influence of COVID-19 on the functional device of state governance of economic growth of countries in the context of ensuring security. International Journal of Safety and Security Engineering 12(2): 193-199. https://doi.org/10.18280/ijsse.120207

[22] Kryshtanovych, S. 2022. Modeling ways of counteraction to external threats to corporate security of engineering enterprises in the context of COVID-19. International Journal of Safety and Security Engineering 12(2): 217-222. https://doi.org/10.18280/ijsse.120210

[23] Kussainov, K. et al., 2023. Anti-corruption Management Mechanisms and the Construction of a Security Landscape in the Financial Sector of the EU Economic System Against the Background of Challenges to European Integration: Implications for Artificial Intelligence Technologies. Econ. Aff. (New Delhi), 68(1): 509-521.

[24] Liang Q., and Xiangsui, W. 1980. Unrestricted warfare. PLA Literature and Arts.

[25] Nekhai, V., et al., 2024. Economic Consequences of Geopolitical Conflicts for the Development of Territorial Communities in the Context of Economic and National Security of Ukraine. Econ. Aff. (New Delhi), 69 (1): 551-563.

[26] Ramskyi, A. et al. 2023. Formation of the security environment through minimization of the negative impact of threats in the socio-economic system. Financial and Credit Activity Problems of Theory and Practice 3(50): 256-264. https://doi.org/10.55643/fcaptp.3.50.2023.4074

[27] Raugh, D. 2016. Is the Hybrid Threat a True Threat?. Journal of Strategic Security 9(2): 1-13.

[28] Regan, M., and Sari, A. 2024. Hybrid threats and grey zone conflict: The challenge to liberal democracies. Oxford University Press.

[29] Romansky, S. et al. 2024. New technologies, changing strategies: Five trends in the hybrid threat landscape. The Hague Center for Strategic Studies.

[30] Sadik, G. 2017. Europe's hybrid threats: What kinds of power does the EU need in the 21st century? Cambridge Scholars Publishing

[31] Sanz-Caballero, S. 2023. The concepts and laws applicable to hybrid threats, with a special focus on Europe. Humanities & Social Sciences Communications 10: 360 https://doi.org/10.1057/s41599-023-01864-y

[32] Sari, A. 2019 Legal resilience in an era of grey zone conflicts and hybrid threats. In: Exeter Centre for International Law Working Paper Series 1. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3315682

[33] Searight, A. 2020. The nature of China's influence activities. In Countering China's Influence Activities: Lessons from Australia (pp. 3-4). Center for Strategic and International Studies (CSIS). http://www.jstor.org/stable/resrep25685.4

[34] van Veen, E. et al. 2022. Cassandra calling? Development, governance and conflict trends in the Middle East. Clingendael.

[35] Zayats, D., et al., 2024. Economic Aspects of Public Administration and Local Government in the Context of Ensuring National Security. Econ. Aff. (New Delhi), 69(2): 979-988.

© 2024 by the authors; licensee Learning Gate