SUBVERTING THE VOTE: HYBRID TACTICS IN DEMOCRATIC DISRUPTION

CZU: 342.841:321.7
https://doi.org/10.59295/eiqd.18

Csongor B. VERESS[*]

Abstract. *Hybrid warfare represents a significant and evolving threat to democratic institutions, particularly electoral processes. By blending traditional military strategies with unconventional tactics such as disinformation campaigns, cyberattacks, and economic coercion, adversaries exploit societal vulnerabilities to destabilize political systems and undermine public trust. Disinformation campaigns amplify societal divisions, manipulate public opinion, and erode confidence in electoral integrity, while cyberattacks target critical infrastructure, creating uncertainty and disrupting democratic processes. The adaptability and ambiguity of hybrid warfare, often blurring the lines between state and non-state actors, further complicates accountability and response mechanisms.*

To counter these threats, democracies must adopt a multifaceted approach. This includes strengthening international cooperation for intelligence sharing and joint responses, investing in media literacy programs to empower citizens against disinformation, and promoting transparency to build resilience within institutions. Civil society organizations also play a vital role in enhancing accountability and fostering civic engagement. As hybrid tactics continue to evolve, democratic nations must remain vigilant and proactive, leveraging technological advancements and fostering international partnerships to safeguard electoral integrity and democratic governance. This article examines these challenges and provides recommendations for developing effective strategies to combat hybrid threats.

Keywords*: Hybrid warfare, democratic resilience, disinformation, cybersecurity, civic engagement*

Introduction to Hybrid Warfare and Democratic Resilience

In the context of an increasingly interconnected global environment, hybrid warfare has emerged as a significant threat to the stability and resilience of democratic institutions. Distinct from conventional warfare, hybrid tactics operate in what is often referred to as the *"grey zone"*. These methods blend traditional military strategies with

[*]LL.M., PhD, University Senior Lecturer, Department of International Law, Faculty of Law of the Károli Gáspár University of the Reformed Church in Hungary. Email: veress.csongor.balazs@kre.hu

unconventional techniques (Hoffman, 2007), such as cyberattacks, disinformation campaigns, and economic coercion, aiming to exploit the vulnerabilities inherent in open societies. By targeting electoral systems, polarizing public opinion, and undermining trust in governance, hybrid warfare destabilizes democracies in ways that are both pervasive and difficult to counter. Its adaptability and inherent ambiguity make hybrid warfare a persistent and evolving challenge for the 21st century.

A striking example of hybrid warfare is the 2016 US. presidential election, during which Russian operatives engaged in a sophisticated disinformation campaign. Using social media platforms, these actors masqueraded as American citizens, disseminating divisive content on sensitive topics such as race, immigration, and gun control (Rid, 2020). The campaign not only sought to influence voter behavior but also revealed structural weaknesses in democratic systems heavily reliant on digital communication. Similarly, the 2007 cyberattacks on Estonia underscored the vulnerabilities of critical infrastructure in the face of state-sponsored aggression. These attacks, which targeted government websites, financial institutions, and media outlets, disrupted the nation's economy and governance, serving as a harbinger of the potential scale and impact of hybrid threats (NATO, 2019).

Hybrid warfare is not confined to major geopolitical players such as the United States or Russia; smaller nations in geopolitically contested regions also face substantial risks. In Eastern Europe, Moldova has been subjected to persistent disinformation campaigns aimed at discrediting its pro-European Union stance (Pomerantsev, 2014). These efforts are often compounded by the nation's reliance on Russian energy supplies, which creates economic and political vulnerabilities during key moments. Similarly, Georgia has experienced extensive propaganda efforts following the 2008 war with Russia. Russian state media narratives portrayed the intervention as a necessary measure to protect ethnic Russians, reshaping public perceptions and influencing regional dynamics. These examples illustrate how hybrid warfare is tailored to exploit the unique vulnerabilities of individual states, adapting its methods to regional political and social contexts.

The digital revolution has amplified the reach and efficacy of hybrid warfare tactics. Social media platforms, with their algorithmic prioritization of sensationalist and divisive content, have become fertile ground for the dissemination of disinformation (Pomerantsev, 2014). The Brexit referendum in the United Kingdom is a case in point; during the campaign, misleading narratives about immigration and economic policy proliferated, shaping public opinion on critical issues. More recently, the 2024 US. presidential election demonstrated the sophistication of hybrid threats through the use of deepfake technology. Fabricated videos depicting candidates in compromising scenarios eroded trust in the electoral process, underscoring the challenges posed by rapidly advancing technology.

Mitigating the impact of hybrid warfare necessitates a comprehensive and multifaceted approach. Media literacy initiatives have proven effective in enhancing societal resilience by equipping individuals with the skills required to identify and counter disinformation (NATO StratCom COE, 2017). Finland, for instance, has integrated media literacy into its national education curriculum, cultivating a digitally literate population capable of navigating complex information landscapes. Cybersecurity

measures are equally crucial. Estonia's implementation of advanced encryption techniques and real-time threat detection systems has positioned it as a global leader in electoral security, providing a model for other nations (Waltzman. 2017).

International cooperation is another cornerstone of efforts to address hybrid threats. Multilateral organizations such as NATO and the European Union have established specialized task forces to combat disinformation and cyberattacks (Giles, 2016.). These initiatives emphasize intelligence sharing, coordinated responses, and the imposition of sanctions on aggressors, thereby strengthening collective security frameworks. However, their effectiveness hinges on the active participation and commitment of member states, as well as the establishment of clear and enforceable protocols for addressing hybrid operations.

Civil society plays a critical role in countering hybrid warfare by fostering transparency and accountability. Grassroots movements and non-governmental organizations (NGOs) act as watchdogs, exposing disinformation campaigns and advocating for informed public discourse. For example, the Digital Forensic Research Lab has been instrumental in identifying and debunking false narratives, reducing their influence on public opinion. By encouraging civic engagement and strengthening public trust, civil society contributes to the resilience of democratic institutions in the face of hybrid threats.

In conclusion, hybrid warfare presents a multifaceted challenge that requires an equally nuanced and robust response. Through the strategic deployment of disinformation, cyberattacks, and economic coercion, adversaries seek to exploit societal divisions and undermine democratic governance. Addressing these threats demands an integrated approach encompassing media literacy, cybersecurity, international collaboration, and active civil society participation. As hybrid warfare tactics continue to evolve, democracies must remain vigilant and adaptable, ensuring that their institutions and societies are resilient against this complex and persistent threat.

Characteristics of Hybrid Warfare

Hybrid warfare constitutes a sophisticated and dynamic strategy of conflict that integrates traditional military tactics with non-traditional methods, including **cyberattacks, disinformation campaigns, economic coercion, and propaganda**. This strategy operates within the *"grey zone"*, an area that blurs the lines between war and peace, enabling aggressors to achieve political or military objectives without resorting to full-scale armed conflict. The hallmark of hybrid warfare is its ambiguity, which complicates the identification of aggressors and challenges the formulation of appropriate responses, whether military or diplomatic (Mumford, Andrew, Pascal Carlucci. 2022).

Modern hybrid warfare exploits systemic vulnerabilities inherent in interconnected and open societies. Among its most prominent tools is **disinformation**, which manipulates public perception, creates societal discord, and erodes trust in institutions. A notable example is Russia's extensive disinformation campaign during the 2016 US. presidential election. Utilizing social media platforms, Russian operatives disseminated divisive content targeting polarizing issues such as immigration, race relations, and gun control. By tailoring messages to specific demographic groups, these

campaigns successfully deepened political polarization and weakened public confidence in democratic processes. This incident underscores the strategic use of disinformation to undermine societal cohesion and influence political outcomes.

Another key pillar of hybrid warfare **cyberattacks**, which often focus on disrupting critical infrastructure, including communication networks, energy systems, and electoral processes. The 2007 cyberattack on Estonia serves as a paradigmatic example. In this state-sponsored operation, hackers paralyzed government websites, financial systems, and media outlets, significantly disrupting the country's administrative and economic functions. This attack not only demonstrated the potential of cyber warfare to destabilize a nation but also highlighted the vulnerabilities of digitized systems in the face of hybrid threats (Total Military Insight. 2024).

Propaganda, a longstanding component of hybrid warfare, has been transformed by the advent of digital technology. Social media platforms and state-controlled media outlets now enable aggressors to disseminate carefully crafted narratives on an unprecedented scale. During Russia's annexation of Crimea in 2014, for example, Russian media portrayed the intervention as a liberation effort aimed at protecting ethnic Russians and restoring historical justice. This narrative, amplified through both traditional and digital channels, garnered domestic support and sought to legitimize the annexation in the international arena. Such propaganda not only undermines the sovereignty of targeted states but also manipulates global perceptions to align with the aggressor's strategic objectives.

The ambiguous and multifaceted nature of hybrid warfare makes it a particularly challenging threat for democratic states. By exploiting digital technologies and systemic weaknesses, hybrid strategies can achieve significant disruption without crossing the traditional thresholds of war. *To counter such threats, states must develop comprehensive strategies that combine cybersecurity, media literacy, and international collaboration.* Civil society and independent watchdog organizations also play a crucial role in identifying and combating disinformation, thereby strengthening societal resilience against hybrid operations.

Hybrid warfare exemplifies the evolving nature of conflict in the 21st century, where conventional military engagements are increasingly supplemented or replaced by indirect, covert, and non-linear tactics. By leveraging disinformation, cyberattacks, and propaganda, aggressors exploit the vulnerabilities of interconnected societies, destabilizing governance and eroding trust in democratic institutions. Understanding the mechanisms and objectives of hybrid warfare is essential for developing robust responses and safeguarding the principles of sovereignty and democracy.

Evolution of Hybrid Warfare

The concept of hybrid warfare has undergone significant evolution, adapting to technological advancements and shifting geopolitical dynamics. While hybrid tactics are often associated with contemporary conflicts, their roots can be traced to historical practices that combined direct and indirect methods to achieve strategic objectives (Cheng and others, 2018).

Hybrid warfare is not a modern phenomenon. In ancient conflicts, psychological operations and misinformation were frequently employed alongside traditional combat

strategies. For instance, during the Peloponnesian War, Sparta utilized false narratives and propaganda to sow distrust among Athenian allies, weakening their resolve and undermining the Athenian war effort. This strategic integration of indirect methods highlights the enduring relevance of hybrid tactics in military history (Atkinson, p. 63-75).

The Cold War marked a pivotal period in the formalization of hybrid warfare, as superp-owers sought to exert influence without escalating into direct armed conflict. Both the United States and the Soviet Union engaged in extensive psychological operations, disinformation campaigns, and covert activities. For example, US. interventions in Latin America, such as the support for anti-communist movements in Nicaragua and Chile, reflected a calculated use of indirect strategies to counter Soviet influence. Similarly, the Soviet Union deployed propaganda and subversive activities across Europe to bolster its ideological dominance. These Cold War-era tactics underscored the strategic effectiveness of hybrid methods in achieving geopolitical goals while avoiding overt military confrontation.

The advent of the internet and the proliferation of social media platforms have transformed the landscape of hybrid warfare, amplifying its scope and sophistication. In the 2016 US. presidential election, Russian operatives leveraged digital tools to disseminate disinformation, using automated bots and fake social media accounts to manipulate public opinion. These operations targeted polarizing issues, eroded trust in democratic institutions, and showcased the potential of digital platforms as instruments of hybrid warfare (Colibasanu,2024).

The 2007 cyberattacks on Estonia further illustrate the evolution of hybrid warfare in the digital age. In this case, state-sponsored actors launched a coordinated assault on Estonia's government websites, financial systems, and media outlets. These attacks were designed to destabilize the country's political and economic systems, highlighting the disruptive potential of cyber tools in modern hybrid operations. The incident served as a wake-up call for nations reliant on digital infrastructure, demonstrating the vulnerabilities of interconnected societies.

Hybrid warfare has also expanded beyond traditional political and military domains to exploit emerging vulnerabilities in public health and social stability. During the COVID-19 pandemic, state-sponsored disinformation campaigns targeted vaccine distribution efforts, health policies, and public trust in government institutions. These campaigns prolonged the crisis by undermining coordinated responses and fostering societal divisions. This example underscores the adaptability of hybrid warfare, which seeks to exploit any fissure within societies to achieve strategic objectives.

The evolution of hybrid warfare reflects its adaptability to changing historical, technological, and societal contexts. From ancient psychological operations to Cold War-era covert activities and the sophisticated cyber and disinformation campaigns of the digital age, hybrid tactics have proven to be a durable and effective strategy. By exploiting systemic vulnerabilities and leveraging emerging technologies, aggressors continue to challenge the stability of nations and institutions. Understanding this historical evolution is essential for developing robust defenses against the multifaceted threats posed by hybrid warfare.

Contemporary Challenges and Implications

Hybrid warfare poses profound challenges for democratic societies, primarily due to its reliance on ambiguity and deniability. Unlike conventional conflicts, hybrid strategies often deploy proxy actors, such as criminal networks or cyber mercenaries, to obscure the involvement of state sponsors. This tactic complicates attribution and accountability, allowing aggressors to achieve strategic objectives while minimizing the risk of direct reprisal. A prominent example of this approach was Russia's interference in the 2016 US. presidential election, where groups such as *"Fancy Bear"* and coordinated troll farms were employed to manipulate public opinion and disrupt democratic processes. These methods demonstrate how hybrid warfare blurs the boundaries of responsibility, exploiting the legal and political constraints of targeted nations (Colibasanu, 2024).

The economic dimension of hybrid warfare has gained increasing prominence, highlighting its multifaceted nature. Economic coercion has become a powerful tool for exerting influence over adversaries without resorting to overt military action. Manipulating trade relations, imposing sanctions, or controlling energy supplies are common tactics used to pressure nations into compliance. A clear illustration is Russia’s control over European gas supplies, which has been strategically employed during political disputes to coerce policy changes in affected states. This integration of economic instruments within hybrid operations underscores the sophistication and adaptability of such tactics, complicating traditional approaches to conflict resolution.

Democratic systems are particularly vulnerable to hybrid threats due to their inherent openness, transparency, and reliance on free communication. These very strengths, foundational to democratic governance, can be exploited to create societal divisions and erode trust in institutions. Disinformation campaigns are a cornerstone of hybrid warfare, often targeting contentious societal issues such as immigration, racial inequality, or political polarization. By amplifying existing divisions and disseminating false narratives, adversaries seek to undermine public confidence in governance, destabilize political systems, and weaken social cohesion. This form of manipulation demonstrates the interplay between technological advancements and the vulnerabilities of democratic societies.

Responding to the challenges of hybrid warfare requires a comprehensive and multifaceted approach. Enhancing cyber resilience is essential to protect critical infrastructure from increasingly sophisticated attacks. Investments in advanced cybersecurity measures, such as real-time threat detection systems and encryption protocols, are vital to reducing vulnerabilities and minimizing damage. At the same time, societal resilience must be strengthened through initiatives such as media literacy programs. By equipping citizens with the tools to critically evaluate information, nations can mitigate the effects of disinformation and promote a more informed electorate.

International cooperation is equally critical in countering the transnational nature of hybrid threats. Multilateral organizations play a pivotal role in fostering collaboration, sharing intelligence, and coordinating responses. Joint efforts through institutions such as NATO and the European Union have demonstrated the importance of collective action in addressing hybrid aggression. The establishment of specialized bodies, such as NATO's Strategic Communications Centre of Excellence, underscores the significance

of analyzing disinformation trends and formulating effective countermeasures. These collaborative frameworks enhance the ability of nations to respond cohesively and decisively to hybrid challenges.

Hybrid warfare remains a dynamic and evolving threat, characterized by its combination of conventional and unconventional tactics designed to exploit the vulnerabilities of modern societies. Its emphasis on ambiguity and deniability ensures that it remains a persistent challenge for policymakers, defense strategists, and international institutions. A comprehensive understanding of its historical evolution, operational mechanisms, and current applications is essential to developing effective countermeasures. As technology continues to advance and global interconnectivity deepens, hybrid warfare is likely to remain a defining issue in national and international security for the foreseeable future, demanding sustained vigilance, adaptability, and innovation in response strategies.

Undermining Democratic Elections Through Hybrid Tactics. The Role of Disinformation Campaigns

Disinformation campaigns are a cornerstone of hybrid warfare, serving to distort political discourse and undermine trust in democratic institutions. These operations are meticulously designed to propagate false or misleading information, thereby diminishing the credibility of legitimate media outlets and public officials. By exploiting existing societal divisions, disinformation fosters polarization, exacerbates tensions, and creates an atmosphere of uncertainty, complicating citizens' ability to differentiate between fact and falsehood.

One of the most striking illustrations of disinformation's impact occurred during the 2016 US. presidential election. Russian operatives, disguising themselves as American citizens, used social media platforms such as Facebook and Twitter to amplify contentious narratives surrounding race, immigration, and gun control. These campaigns targeted specific demographic groups with precision, tailoring content to influence opinions, suppress voter turnout, or shift political allegiances. African-American communities, for instance, were bombarded with messaging intended to discourage participation in the electoral process. By disseminating fabricated stories and sensationalist material, these operations successfully manipulated public discourse and eroded trust in the electoral system. This case highlights the effectiveness of disinformation in exploiting vulnerabilities within open societies to achieve strategic objectives (Postma, Šafář, 2024).

Disinformation campaigns often function in concert with other elements of hybrid warfare to enhance their overall impact. During the COVID-19 pandemic, state-sponsored disinformation targeted public health initiatives, focusing on vaccine distribution and government-imposed health measures. These efforts sought to undermine public trust in official responses, amplify doubts about vaccine efficacy, and exacerbate societal divisions over pandemic management. By leveraging the global health crisis, such campaigns demonstrated the flexibility of disinformation tactics in adapting to current events and exploiting vulnerabilities in public confidence. This example underscores how hybrid warfare can weaponize real-world challenges to destabilize democratic societies further.

The adaptability and pervasiveness of disinformation make it a particularly insidious tool in hybrid warfare. By combining digital technology with psychological manipulation, adversaries can reach vast audiences rapidly and at minimal cost. These campaigns are not merely designed to misinform but to destabilize, polarize, and weaken democratic structures from within. Understanding and countering the strategic use of disinformation is critical to safeguarding democratic institutions and ensuring societal resilience in the face of hybrid threats (Bennett and others, 2021).

Cyberattacks on Electoral Infrastructure

Cyberattacks have emerged as a defining feature of hybrid warfare, aiming to undermine the technological foundations of democratic processes. By infiltrating electoral systems, hackers can compromise voter databases, manipulate results, or simply foster the perception of fraud. These operations, often carried out by state-sponsored actors or their proxies, exploit vulnerabilities in digital infrastructure to disrupt democratic governance and sow distrust among citizens.

The 2020 US. presidential election provides a compelling example of cyberattacks as a tool in hybrid warfare. In the months preceding the election, US. intelligence agencies identified numerous attempts by foreign actors, including Russia, China, and Iran, to interfere with the electoral process. These efforts involved a range of techniques, from phishing campaigns targeting election officials to sophisticated hacking attempts on voter registration databases. Although no evidence suggested that votes were altered, the mere existence of these activities was sufficient to raise public concerns about the security of the electoral system. This case underscores how cyberattacks, even when unsuccessful in achieving their immediate goals, can erode trust in democratic institutions by exploiting the fear of manipulation.

The 2007 cyberattacks on Estonia remain a seminal example of how cyber operations can destabilize a nation. Over the course of several days, coordinated attacks targeted Estonia's government websites, banking systems, and media outlets, effectively paralyzing the country’s digital infrastructure. Allegedly orchestrated by Russian actors, this assault demonstrated the capacity of cyberattacks to disrupt essential services, undermine public confidence, and destabilize societal functioning. This event is widely regarded as one of the first large-scale instances of cyber warfare and has since served as a model for hybrid warfare strategies targeting electoral and governmental systems (Lawson and others, 2024).

Countering such threats requires a proactive and comprehensive approach. Governments must invest in advanced cybersecurity measures, including end-to-end encryption, robust firewalls, and real-time threat detection systems, to safeguard critical infrastructure. Additionally, enhancing coordination between public and private sectors is essential for identifying vulnerabilities and mitigating potential risks. However, as cyberattacks grow increasingly sophisticated, defensive measures must evolve in parallel to ensure the resilience of democratic processes against hybrid warfare tactics.

Cyberattacks in hybrid warfare highlight the intersection of technology, strategy, and psychological manipulation. By exploiting digital vulnerabilities, adversaries seek not only to disrupt systems but to erode trust and stability within democratic societies. Understanding the methods and objectives of these operations is essential for developing

effective countermeasures and protecting the integrity of democratic institutions in an era of rapidly advancing technological threats (Whyte, 2020).

Propaganda and Societal Polarization

Propaganda is a fundamental component of hybrid warfare, strategically deployed to deepen societal polarization and manipulate public sentiment. By constructing narratives that exploit existing societal tensions, hybrid actors aim to exacerbate divisions, weakening the social cohesion that underpins democratic institutions. This deliberate manipulation of information enables aggressors to destabilize target societies while pursuing broader geopolitical objectives.

State-sponsored propaganda has been particularly influential in polarizing societies, both domestically and internationally. During the annexation of Crimea in 2014, Russian state media, including outlets like RT and Sputnik, framed the intervention as a humanitarian mission to protect ethnic Russians. This narrative was carefully constructed to resonate with domestic audiences while simultaneously targeting international observers to legitimize Russia's actions and undermine Ukraine's sovereignty. These campaigns demonstrate the effectiveness of weaponized information in shaping perceptions, fostering division, and achieving geopolitical goals without direct confrontation (Ivančík, 2023).

In democratic societies, propaganda often manifests in subtler forms, leveraging the reach and influence of social media platforms. Algorithms designed to prioritize engagement inadvertently amplify divisive content, creating echo chambers that reinforce preexisting biases and discourage constructive discourse. The 2016 US. presidential election provides a vivid example, where propaganda tactics blurred the lines between legitimate political debate and deliberate manipulation. By disseminating polarizing material, hybrid actors were able to influence public opinion and expose the vulnerabilities of open, information-rich societies to hybrid threats (Lemmon, 2024).

The potency of propaganda lies in its ability to exploit emotional triggers such as fear, anger, and nationalism, provoking irrational and reactionary responses. During the Brexit referendum in the United Kingdom, widely circulated falsehoods about immigration and economic consequences were instrumental in stoking anti-EU sentiment. Although the role of foreign interference in these efforts remains debated, the referendum underscored the ability of targeted propaganda to shape public opinion on critical issues, ultimately altering the trajectory of a nation's political landscape. This case illustrates how hybrid actors exploit democratic processes to sow discord and advance their strategic aims.

Combating the challenges posed by propaganda requires a comprehensive and multifaceted response. Media literacy programs are essential for equipping citizens with the tools to critically evaluate information and recognize manipulative narratives. Regulatory oversight of digital platforms is also crucial to reduce the dissemination of harmful content and ensure transparency in content algorithms. Furthermore, international cooperation is needed to address the transnational nature of propaganda campaigns, enabling states to share intelligence and develop coordinated responses.

Hybrid warfare tactics, including propaganda, disinformation campaigns, and cyberattacks, pose a direct and multifaceted threat to the integrity of democratic systems.

By distorting political discourse, undermining trust in institutions, and exacerbating societal divisions, these strategies erode the foundations of democracy. Understanding the mechanisms of propaganda and its broader implications is critical for developing effective countermeasures and ensuring the resilience of democratic institutions in an era defined by hybrid threats (Juhász, 2024.).

Regional and Global Case Studies. Eastern Europe: The Experiences of Romania, Moldova, and Georgia

In 2024, hybrid warfare in Eastern Europe reached new levels of sophistication, targeting the sovereignty and democratic integrity of nations such as Romania, Moldova and Georgia. These states, positioned at the geopolitical crossroads of Russia and the West, are uniquely vulnerable to destabilization efforts. The hybrid tactics employed include disinformation campaigns, cyberattacks, and the exploitation of economic and political vulnerabilities, all designed to undermine their alignment with Western institutions like the European Union and NATO.

Romania: Disinformation and Electoral Interference

Romania's 2024 presidential election was a stark demonstration of how hybrid warfare can disrupt democratic processes. During the election, far-right candidate Călin Georgescu emerged as a surprise frontrunner in the first round, thanks largely to an extensive disinformation campaign orchestrated by Russian operatives. Moscow leveraged social media platforms such as TikTok, where over 100 influencers were mobilized to amplify pro-Russian and nationalist narratives favorable to Georgescu.

These influencers targeted younger voters with engaging but misleading content, falsely attributing Romania’s economic struggles to EU integration and promoting conspiracy theories about corruption among pro-Western candidates. As a result, public trust in the democratic process was significantly eroded, and social divisions deepened. When Romanian authorities annulled the election results due to the scale of foreign interference, it marked a critical moment in recognizing the vulnerabilities of digital platforms in the democratic sphere (Pop and others, 2024).

Moldova: Persistent Hybrid Threats

Moldova, already grappling with internal divisions, faced intensified hybrid threats in 2024. The pro-European government of President Maia Sandu was targeted by Russian disinformation campaigns aiming to derail the country's European Union accession process. Narratives circulating in Moldova claimed that EU membership would lead to economic decline, higher taxes, and the erosion of national sovereignty. These messages were disseminated through both traditional and social media channels, exploiting existing skepticism toward European integration (Peru-Balan, 2024.).

Energy dependency continued to be a significant vulnerability for Moldova. Russia's state-controlled energy giant Gazprom strategically disrupted gas supplies during critical moments, such as during negotiations between Moldova and the EU on energy diversification. These disruptions were timed to exacerbate political tensions and undermine the credibility of the Sandu administration. The combination of economic

leverage and information warfare demonstrated the multi-pronged approach Russia employs to maintain its influence in Moldova (Youngblood, 2024).

Georgia: Electoral Manipulation and Political Destabilization

Georgia has long been a target of Russian hybrid tactics, and the 2024 parliamentary elections were no exception. The ruling Georgian Dream party, led by billionaire Bidzina Ivanishvili, declared victory with 54% of the vote. However, international observers, including the OSCE and EU representatives, flagged the elections as neither free nor fair. Evidence of Russian interference included extensive disinformation campaigns and financial support to pro-Russian parties and NGOs.

Russian-controlled media actively portrayed opposition groups as agents of Western interests, framing them as threats to Georgian sovereignty and traditional values. At the same time, cyberattacks targeted government websites and independent media outlets, further complicating the electoral process. These hybrid tactics aimed to deepen political polarization, weaken Georgia's democratic institutions, and deter its progress toward EU and NATO membership (Le Monde, 2024).

The cases of Romania, Moldova, and Georgia in 2024 highlight the dynamic and evolving nature of hybrid warfare in Eastern Europe. By exploiting the unique vulnerabilities of each nation, including societal divisions, energy dependency, and democratic processes, hybrid tactics have proven to be a powerful tool for destabilization. Addressing these threats requires a multifaceted approach, including enhanced digital literacy to combat disinformation, energy diversification to reduce economic vulnerabilities, and strengthened international cooperation on cybersecurity and election integrity.

Russia and Western Democracies: Analyzing Russian disinformation strategies

Russia's hybrid warfare strategies have evolved significantly, employing increasingly sophisticated disinformation campaigns and cyberattacks to target Western democracies. These operations are designed to erode trust in democratic institutions, deepen societal divisions, and weaken international alliances.

One prominent example is Russia's interference in the 2016 US. presidential election. Russian operatives exploited social media platforms, creating fake accounts and disseminating polarizing content to manipulate public opinion. By amplifying existing societal tensions, such as racial inequality and immigration debates, these actors capitalized on vulnerabilities within American society to sow discord. The impact of these operations extended beyond the United States. During the 2017 French presidential election, Russian-backed groups utilized similar tactics, including the dissemination of hacked information to undermine Emmanuel Macron's campaign, illustrating the seamless integration of disinformation into Russia's hybrid warfare strategies.

The United Kingdom has also been a significant target of Russian disinformation. The Brexit referendum in 2016 saw the proliferation of misleading narratives concerning the European Union, particularly around immigration and economic policy. Russian state media outlets such as RT and Sputnik amplified these messages, exemplifying the

coordinated use of traditional and digital media to influence public opinion and destabilize political processes (Menkiszak, 2024).

A key feature of Russia's hybrid approach is its alignment with long-term strategic objectives, such as undermining the unity of NATO and the European Union. By exploiting societal and political vulnerabilities in targeted nations, Russia's disinformation campaigns hinder collective responses to global challenges and weaken the coherence of Western alliances. These developments highlight the necessity of coordinated countermeasures, including intelligence-sharing and joint policy initiatives among affected states, to mitigate the impact of hybrid warfare (Kakachia and others, 2024).

International Examples: Lessons from the 2024 US. Presidential Election

The 2024 US. presidential election offers a compelling case study on the evolution of hybrid warfare. Disinformation campaigns during this election cycle exhibited unprecedented sophistication, incorporating artificial intelligence and machine learning to craft highly convincing fake news and personalized narratives. These operations specifically targeted voter groups with tailored misinformation to suppress voter turnout or manipulate preferences.

A particularly alarming development was the weaponization of deepfake technology. Fabricated videos purporting to show candidates making controversial statements spread widely on social media, undermining public trust in the authenticity of information. In addition, cyberattacks on voter registration systems created administrative confusion and delays, exacerbating public perceptions of electoral vulnerability. Although these cyberattacks did not alter votes, their psychological impact on public confidence in democratic processes was significant.

Social media platforms played a pivotal role in facilitating hybrid operations during the 2024 election. Algorithms designed to maximize user engagement inadvertently amplified divisive content, enabling disinformation campaigns to reach vast audiences. Despite increased efforts by technology companies to detect and remove malicious actors, the overwhelming volume of misleading content highlighted the ongoing challenges of balancing free expression with the need to mitigate harmful influence campaigns.

The lessons from the 2024 election underscore the critical importance of proactive measures to protect electoral integrity. These measures include enhancing public awareness of disinformation tactics, investing in robust cybersecurity infrastructure, and fostering international cooperation to hold both state and non-state actors accountable for hybrid operations. Addressing these challenges at a systemic level is vital, given their implications for the stability of democratic institutions worldwide (Alaverdov and others, 2023).

Strategies for Democratic Resilience. Media literacy and combating disinformation

Democracies face evolving hybrid threats that exploit vulnerabilities across societal, political, and technological domains. To counter these challenges, a multifaceted strategy that emphasizes media literacy, cybersecurity, and the strengthening of civil society is essential (European Parliament, 2024).

Media literacy is a cornerstone of democratic resilience, equipping citizens with the tools to critically evaluate information and resist manipulative disinformation campaigns. These programs teach individuals to recognize credible sources, identify biases, and understand the emotional triggers often exploited in disinformation, such as fear or anger. A significant focus of media literacy initiatives is on election-related disinformation, where false claims about voter fraud or integrity can undermine trust in democratic processes. For example, the European Commission's "Media Literacy for All" project and Finland's integration (European Commission, 2021) of media literacy into school curricula have demonstrated success in building public awareness and resilience to misinformation (European Digital Media Observatory, 2023). To maximize their impact, media literacy programs must be inclusive, addressing the needs of diverse demographics, including those with limited digital skills or access to information. Tailored initiatives ensure broader societal engagement and a more robust defense against disinformation (Kristin and Vogt, 2024).

Enhancing Cybersecurity measures

The protection of electoral systems is vital for maintaining democratic integrity. Modern election infrastructure, including electronic voting platforms and voter databases, is increasingly targeted by cyberattacks. Robust cybersecurity measures, such as end-to-end encryption and multi-factor authentication, are essential for safeguarding these systems. Estonia's e-governance framework is a leading example, demonstrating how advanced security protocols can bolster trust in digital electoral processes (Estonian Centre for International Development, 2024).

Real-time threat detection and response are equally critical. Tools leveraging artificial intelligence and machine learning help identify and mitigate cyber threats before significant harm occurs. During the 2020 US. presidential election, state and federal collaboration successfully prevented major disruptions, showcasing the importance of coordinated efforts.

International cooperation further strengthens cybersecurity. Initiatives like the NATO Cooperative Cyber Defence Centre of Excellence facilitate information sharing and joint responses, enhancing collective defense. However, continuous investment and innovation are required to address the rapidly evolving nature of cyber threats.

Strengthening civil society and promoting transparency

A vibrant civil society plays a pivotal role in countering hybrid threats by promoting transparency, accountability, and civic engagement. Civil society organizations (CSOs), such as the Digital Forensic Research Lab, specialize in identifying and debunking disinformation, reducing its impact on public opinion. These efforts are particularly critical during elections, where exposing false claims can prevent them from influencing voter behavior. Transparency initiatives further bolster democratic resilience. Practices like publishing detailed election results and granting access to public records build trust in institutions and provide citizens with accurate information to counter disinformation. Countries like Canada and Sweden have effectively implemented such measures, reinforcing public confidence in governance.

CSOs also enhance resilience through civic education and public participation. Campaigns encouraging voting and community engagement empower citizens to actively defend democracy. For example, grassroots movements in Ukraine have successfully mobilized support for democratic reforms, illustrating civil society's potential to drive positive change even in adverse conditions. An enabling environment is essential for civil society initiatives to thrive. Governments must ensure that CSOs have adequate legal and financial resources, while international support can provide additional expertise and funding. By recognizing and supporting the role of civil society, democracies can build robust defenses against hybrid threats.

Building democratic resilience against hybrid warfare requires a comprehensive strategy addressing disinformation, cybersecurity, and civic engagement. Media literacy initiatives foster critical thinking, cybersecurity measures protect electoral integrity, and civil society strengthens transparency and accountability. While challenges remain, these strategies provide a roadmap for creating resilient democratic institutions capable of withstanding the complexities of modern hybrid threats (Center for Civilians in Conflict, 2024).

Summary and recommendations

Hybrid warfare presents an evolving threat to democratic elections, blending conventional strategies with unconventional tools such as cyberattacks, disinformation campaigns, and economic coercion. These tactics are designed to exploit systemic vulnerabilities, disrupt political stability, and erode trust in democratic processes. The most concerning feature of hybrid warfare is its adaptability, enabling adversaries to target specific weaknesses within different societies. This multidimensional challenge underscores the need for robust and coordinated responses.

The impact of hybrid warfare on democratic elections is profound. Disinformation campaigns manipulate public opinion by spreading false narratives, often intensifying societal divisions. These campaigns not only influence voter behavior but also erode trust in electoral institutions, as evidenced by the 2016 US. presidential election, where foreign actors amplified divisive content on social media. Similarly, cyberattacks on electoral infrastructure, such as voter databases, create chaos and foster doubts about election integrity, further undermining public confidence. Compounding this challenge is the difficulty of attributing responsibility, as hybrid operations often blur the lines between state and non-state actors, complicating accountability and response strategies (Association of the United States Army, 2021).

Addressing these threats requires a multifaceted approach:

- **Strengthening International Cooperation**

Hybrid threats are inherently transnational, making international collaboration essential. Organizations such as NATO and the European Union have established frameworks to address hybrid threats, including specialized task forces for monitoring and countering disinformation and cyberattacks. For instance, the European Centre of Excellence for Countering Hybrid Threats and the NATO Cooperative Cyber Defence Centre of Excellence have provided valuable platforms for sharing resources and

expertise. Democracies should enhance these efforts by developing multilateral agreements with clear protocols for intelligence sharing, joint investigations, and coordinated sanctions against perpetrators. Such measures can strengthen collective resilience and deter aggressors.

- **Developing Media Literacy Programs**

Media literacy initiatives are crucial for empowering citizens to recognize and counter disinformation. These programs foster critical thinking and provide tools to evaluate the credibility of information. Countries like Finland have successfully integrated media literacy into school curricula, equipping students to navigate online content critically. Public awareness campaigns and partnerships with technology companies further amplify the impact of these initiatives. For example, social media platforms have introduced features to flag disputed content, helping users identify misinformation. To remain effective, media literacy programs must evolve alongside emerging threats, such as deepfake technology and AI-driven disinformation.

- **Promoting Transparency and Civic Engagement**

Transparency and active civic participation are essential for building resilience against hybrid threats. Open government practices, such as publishing election results and ensuring decision-making transparency, foster trust and reduce the effectiveness of disinformation campaigns. Civil society organizations (CSOs) play a pivotal role by acting as watchdogs and exposing false narratives. Initiatives like the Digital Forensic Research Lab exemplify how CSOs can debunk disinformation and raise public awareness. Encouraging public engagement through civic education campaigns and grassroots movements further strengthens democratic resilience. Governments must support these efforts by creating an enabling environment for CSOs, including legal protections and financial resources.

Hybrid warfare poses a significant challenge to democratic elections, but a combination of international collaboration, media literacy, and transparency can mitigate its impact. By investing in these strategies, democracies can protect the integrity of their institutions and maintain public trust. Proactive and adaptable responses will be critical in safeguarding democratic governance against the evolving landscape of hybrid threats.

Conclusion

Hybrid warfare poses a significant and multifaceted threat to the stability and integrity of democratic systems worldwide. By blending traditional military strategies with unconventional methods such as disinformation campaigns, cyberattacks, and economic coercion, adversaries exploit the inherent vulnerabilities of open and interconnected societies. These tactics not only destabilize political institutions but also erode public trust, deepen societal divisions, and undermine democratic governance.

Addressing these challenges requires a comprehensive and adaptive response. Strategies must include strengthening international cooperation to enhance collective resilience, implementing robust cybersecurity measures to safeguard electoral integrity, and fostering media literacy programs to empower citizens against disinformation. Additionally, promoting transparency and civic engagement is essential for reinforcing public trust and accountability within democratic institutions.

As hybrid warfare continues to evolve, democracies must remain vigilant and proactive. Through coordinated efforts at the national and international levels, it is possible to mitigate the risks posed by these threats and ensure the resilience of democratic systems against an increasingly complex and adaptable adversarial landscape.

BIBLIOGRAPHY

Pomerantsev, Peter, and Internet Archive. 2014. Nothing Is True and Everything Is Possible: The Surreal Heart of the New Russia. Internet Archive. New York: PublicAffairs. https://archive.org/details/nothingistrueeve0000pome.

NATO StratCom COE. 2017. "Hybrid Threats: A Strategic Communications Perspective." https://stratcomcoe.org/pdfjs/?file=/publications/download/Strategic-Communications-Hybrid-Threats-Toolkit.pdf?zoom=page-fit.

Waltzman, Rand. 2017. "The Weaponization of Information: The Need for Cognitive Security." Www.rand.org. April. https://www.rand.org/pubs/testimonies/CT473.html.

Giles, K. 2016. "Handbook of Russian Information Warfare." https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/resources/docs/NDC%20fm_9.pdf.

Mumford, Andrew, and Pascal Carlucci. 2022. "Hybrid Warfare: The Continuation of Ambiguity by Other Means." European Journal of International Security 8 (2): 1–15. https://doi.org/10.1017/eis.2022.19.

Total Military Insight. 2024. "Civic Engagement in Hybrid Warfare: Strengthening Community Resilience." The Insurance Universe. July 28, 2024. https://totalmilitaryinsight.com/civic-engagement-in-hybrid-warfare/.

Cheng, Qi, Conor Cunningham, Fabian Gacayan, Anni Gu, Alex Hall, Olivia Lee, Ashley Sawyer, Safy Sayoud, Vriti Wadhwa, and Jion Yi. 2018. "Hacking Democracy: Cybersecurity and Global Election Interference." Washington.edu. https://digital.lib.washington.edu/researchworks/items/7ecba2a2-d894-4893-9546-8005dcbb0f18.

Atkinson, Carol. 2018. "Hybrid Warfare and Societal Resilience: Implications for Democratic Governance." Information & Security: An International Journal 39 (1): 63–76. https://doi.org/10.11610/isij.3906.

Colibasanu, Antonia. 2024. "Romania's Electoral Crisis: A Blueprint for Defending Democracy." Policycommons.net. December 11, 2024. https://policycommons.net/artifacts/17909292/romanias-electoral-crisis/18805277/.

Postma, Marie Šafář. 2024. AI at the Battlefield of Human Mind.

Bennett, W Lance, and Steven Livingston. 2021. The Disinformation Age: Politics, Technology, and Disruptive Communication in the United States. New York, Ny: Cambridge University Press.

Lawson, Sean T, and Robert W Gehl. 2024. "Masspersonal Social Engineering and the Evolution of the Influence Industry." Routledge EBooks, August, 83–96. https://doi.org/10.4324/9781003256878-7.

Whyte, Christopher. 2020. "Cyber Conflict or Democracy 'Hacked'? How Cyber Operations Enhance Information Warfare." Journal of Cybersecurity 6 (1). https://doi.org/10.1093/cybsec/tyaa013.

Ivančík, Radoslav. 2023. "On Disinformation and Propaganda in the Context of the Spread of Hybrid Threats." Vojenské Reflexie 18 (3): 38–58. https://doi.org/10.52651/vr.a.2023.3.38-58.

Lemmon, Julia. 2024. "The Weaponization of Fiction and Truth: Disinformation as Hybrid Warfare and Its Strategic Use in the United States 2024 Election." https://doi.org/10.37458/nstf.25.2.5.

Juhász, K. 2024. “European Union Defensive Democracy’s Responses to Disinformation.” Journal of Contemporary European Studies, 32(4), 1075–1094. https://doi.org/10.1080/14782804.2024.2317275.

Pop, Valentina, Marton Dunai, and Polina Ivanova. 2024. “How Russia-Backed Influencers Meddled in Romania’s Vote.” Financial Times. December 9, 2024. https://www.ft.com/content/4b00e7ec-2c79-4313-b012-4f09f436f3ed.

Peru-Balan, Aurelia. 2024. “Propaganda Narratives and Disinformation: The Information Resilience of the Republic of Moldova.” Consolidarea Rezilienței Sociale Prin Valorificarea Capitalului Uman În Contextul Aderării Republicii Moldova Și Ucrainei La Uniunea Europeană. Conferința Internațională: Științifico-Practică, November, 245–55. https://doi.org/10.59295/crs2024.23.

Youngblood, Steven, and James Rupert. 2024. “Review of Russia’s Disinformation Targets Moldova’s Ties with Europe.” The United States Institute of Peace. https://www.usip.org/publications/2024/07/russias-disinformation-targets-moldovas-ties-europe

Monde, Le. 2024. “The European Union’s Georgian Trap.” Le Monde.fr. October 28, 2024. https://www.lemonde.fr/en/opinion/article/2024/10/28/the-european-union-s-georgian-trap_6730794_23.html.

Menkiszak, Marek. 2024. “Winning the War with Russia Is Still Possible. The West’s Counter-Strategy Towards Moscow.” Ceeol.com. OSW Ośrodek Studiów Wschodnich im. Marka Karpia. https://www.ceeol.com/search/gray-literature-detail?id=1283220.

Kakachia, Kornely, and Shota Kakabadze. 2024. “Beyond Cyber and Disinformation: Russian Hybrid Warfare Tactics in Georgia,” January, 129–52. https://doi.org/10.5040/9781350335257.ch-007.

Alaverdov, Emilia, Sopo Chkopoia, and Zurabi Tchabashvili. 2023. “Cyberterrorism and Its Impact on Contemporary Conflicts and Society.” Advances in Human and Social Aspects of Technology Book Series, June, 170–92. https://doi.org/10.4018/978-1-6684-5760-3.ch008.

European Parliament. 2024. “Resilience of Democracy and European Elections against New Challenges.” Policy Department for Citizens’ Rights and Constitutional Affairs Directorate-General for Internal Policies. https://www.iris.sssup.it/bitstream/11382/566535/1/IPOL_STU%282024%29761471_EN.pdf.

European Commission. n.d. Review of Media Literacy. https://digital-strategy.ec.europa.eu/en/policies/media-literacy.

European Digital Media Observatory. n.d. Review of Finland. https://edmo.eu/resources/repositories/mapping-the-media-literacy-sector/finland/.

Lord, Kristin, and Katya Vogt. 2021. “Strengthen Media Literacy to Win the Fight Against Misinformation (SSIR).” Ssir.org. March 18, 2021. https://ssir.org/articles/entry/strengthen_media_literacy_to_win_the_fight_against_misinformation.

Estonian Centre for International Development. n.d. Review of Cybersecurity and E-Governance. https://estdev.ee/en/fields/cybersecurity-and-e-governance.

Center for Civilians in Conflict. n.d. “Entering the Grey-Zone: Hybrid Warfare and the Protection of Civilians in Ukraine.” https://civiliansinconflict.org/publications/policy/entering-the-grey-zone/.

Association of the United States Army. 2021. “Civil Affairs and Civil-Military Cooperation: A Hybrid Solution to Defeat Hybrid Threats.” https://www.ausa.org/publications/civil-affairs-and-civil-military-cooperation-hybrid-solution-defeat-hybrid-threats.