FRIEDRICH NAUMANN FOUNDATION For Freedom.
South Caucasus

HYBRID THREATS AND RESILIENCE

Safeguarding Democratic Values in a Connected World

Tinatin Khidasheli

ANALYSIS

Imprint

Publisher
Friedrich-Naumann-Foundation for Freedom South Caucasus
4. T. Choveldize Street, 0108
Tbilisi, Georgia

/freiheit.org/South-Caucasus
/FNFSC

Authors
Tinatin Khidasheli

Editor
Iago Tsitaishvili

Contact
Phone: +995 32 225 05 94,
+995 32 225 04 16
Email: iago.tsitaishvili@freiheit.org

Date
November 2024

Notes on using this publication
This publication is an information offer of the Friedrich Naumann Foundation for Freedom.
It is available free of charge and not intended for sale. It may not be used by parties or election workers for the purpose of election advertising during election campaigns (federal, state or local government elections, or European Parliament elections).

The views, opinions, and conclusions expressed in this policy paper are those of the author alone and do not necessarily reflect the official views or positions of the Friedrich Naumann Foundation for Freedom South Caucasus, the paper represents the author's independent analysis and insights, which may not coincide with the Foundation's perspectives on every issue discussed.

Based on the principles of liberalism, the Friedrich Naumann Foundation for Freedom offers civic education in Germany and more than 60 countries worldwide. In the South Caucasus region, we closely work with partners from civic society, academia, media, and politics. Together, we promote Democracy and fight against disinformation and hybrid warfare. We stand for Human Rights and Rule of Law. We encourage innovative solutions based on the principles of the Social Market Economy. And we foster dialogue by creating a network among Liberals in the South Caucasus.

Scanning the QR code provided in this publication will direct you to the Friedrich Naumann Foundation South Caucasus Webpage page. This page is not affiliated with the author or publisher of this book, and the content of the page is not endorsed or verified by them. The information on the FNF South Caucasus page is provided as a convenience to our readers who may be interested in additional information related to the Friedrich Naumann Foundation for Freedom South Caucasus.

Abstract

This policy paper delves into the complex realm of hybrid threats—a pressing issue in today's globally connected and technologically sophisticated landscape. Hybrid threats combine traditional and modern warfare techniques, including information warfare, cyber-attacks, and psychological operations, aiming to destabilize opponents before physical conflicts even begin. This analysis emphasizes that traditional military capabilities, like tanks and missiles, continue to play a crucial role. These conventional forces project power and make a vital strategic statement.

The paper will explore the concept of a holistic approach to national security, emphasizing the importance of societal preparedness and resilience. It will illustrate how nations can strengthen their security frameworks by making resilience and deterrence policies imperative to strategic planning. By examining how different strategies harness their societal and governmental capabilities to thwart hybrid threats, the paper aims to offer actionable insights on developing effective deterrence and resilience policies with a special emphasis on the opportunities and challenges of small states.

Keywords:

#Hybridthteats #ConventionalWarfare #resilience

Table of contents

Introduction

Hybrid warfare or hybrid threats are not new. However, their prominence has increased significantly in an era marked by unprecedented connectivity and rapid technological advance. It notably challenges liberal democracies today, worldwide. Hybrid threats, characterized by a blend of conventional and unconventional tactics, include targeted disinformation campaigns, cyber-attacks, and covert influence operations, as well as the instrumentalization of trade and investments or attacks on critical infrastructure, are increasingly potent tools in the hands of state and non-state actors seeking to undermine the foundations of democratic societies. These threats operate below the threshold of armed conflict, making them difficult to discern and attribute, which complicates response efforts. Building resilience against such threats necessitates a whole-of-society approach.

Hybrid threats refer to a diverse and dynamic range of adversarial activities that combine conventional military tactics with unconventional methods to achieve strategic objectives. Those include cyber-attacks, disinformation campaigns, economic coercion, and political subversion. These threats exploit the vulnerabilities of states, organizations, and societies, blurring the lines between war and peace, combatants and non-combatants, and state and non-state actors. The complexity of hybrid threats lies in their ability to operate across multiple domains simultaneously—land, sea, air, space, and cyberspace—creating a multifaceted challenge that is difficult to detect, attribute, and counteract. A proactive and forward-thinking approach, combined with a high level of readiness and a systematic, conceptual vision for effective deterrence, is essential. This holds true for all states, regardless of their size or economic status.

Russia's brutal aggression against Ukraine is a textbook case of hybrid warfare, where Russia has utilized a combination of military forces, cyber-attacks, and information warfare, including the use of "little green men" (unmarked soldiers) and a robust propaganda campaign, to destabilize Ukraine and annex Crimea while preparing a conventional war. This approach is allowing Russia to achieve its geopolitical aims while complicating the international community's response due to the ambiguity of the situation.

1. Understanding hybrid threats

The primary goal of hybrid threats is to weaken or destabilize the targeted entity through a blend of tactics. Here are, though non-exhaustive, examples of forms and patterns used by Russia in its immediate neighbourhood.

As an example, the instrumentalization of migration to destabilize countries or even entire regions by igniting tensions among local populations and challenging the capacity of governments to respond effectively has been exploited extensively by Russia. Other dominant methods targeting the region include:

- Economic Coercion: Using traditional economic measures such as sanctions, trade restrictions, or financial manipulation to exert pressure and influence political decisions. Economic coercion might come in the form of specifically designed credit and loan policies that manipulate states into debt traps or total economic dependency when investments and loans or "economic cooperation" are weaponized1.
- Covert Influence Operations: Secret activities aimed at manipulating political, social, or economic events to achieve strategic objectives without direct confrontation. Those might include elite capture by diverse forms of soft power operations in academia, targeting universities and research centers or media and think tank communities.
- Disinformation Campaigns: Deliberate dissemination of false or misleading information to influence public opinion, to brainwash, to sow discord, and to erode trust in institutions, democratic values, or the rules-based international order.
- Cyber Attacks: Unauthorized and malicious activities targeting information systems, networks, and infrastructures to disrupt, damage, or gain unauthorized access. It often includes attacks on critical infrastructure. The targeting of essential systems and/or services such as energy, transportation, health care, and communication networks causes significant disruption and chaos, or even destruction.
- Military Posturing and Limited Incursions: Deploying military forces or engaging in minor skirmishes to intimidate, provoke, or create confusion without escalating to full-scale war.

[1] See, Banned in Russia: the Politics of Georgian Wine by Mamuka Tsereteli, at https://www.cacianalyst.org/publications/analytical-articles/item/10801-analytical-articles-caci-analyst-2006-4-19-art-10801.html or *Georgia Stuck in the Russian Economic Trap*, by Giorgi Tskhadaia at https://forbes.ge/en/georgia-stuck-in-the-russian-economic-trap/

Hybrid threats manifest in various forms and can appear differently depending on their context. These threats vary not only by a diverse array of tactics but also by the actors executing these threats. Hybrid and conventional warfare can either be conducted solely by state actors or through a collaboration of state and non-state entities, including terrorist groups, paramilitary organizations, and criminal networks. These actors exploit the openness and interconnectedness of democratic societies, utilizing advanced technologies and global communication networks to enhance their impact. The efficacy of hybrid threats lies in their ability to operate below the threshold of traditional military responses, thereby avoiding direct confrontation and detection. This underscores the necessity for a comprehensive and integrated approach to resilience and defence, ensuring that societies are equipped to address and mitigate the multifaceted nature of hybrid threats.

Hybrid threats challenge traditional security paradigms because they do not fit neatly into existing categories of warfare or conflict. Conventional military strategies and legal frameworks are often ill-suited to address these threats' diffuse and multidimensional nature, necessitating new approaches that emphasize resilience, collaboration across sectors, and the integration of diverse capabilities.

2. Traditional actors

One of the characteristics of hybrid warfare, as already mentioned, is the different roles of states in understanding and handling conflicts. It is widely accepted that some states frequently employ non-state actors2, particularly during the initial stage of preparing and instigating confrontation. The rise of non-state actors and states' strategic use of proxies represent significant developments in contemporary international relations and security dynamics. Non-state actors, encompassing a wide array of entities such as terrorist organizations, insurgent groups, paramilitary forces, and criminal networks, have increasingly become influential players on the global stage.

While these non-state actors operate outside the traditional state-centric framework, they often pursue their own agendas while exploiting the vulnerabilities and opportunities presented by globalization, technological advancements, and transnational networks. The asymmetrical nature of their operations, combined with their ability to adapt and innovate, poses unique challenges to conventional state-based security apparatuses.

States, recognizing the potential benefits of utilizing non-state actors, have increasingly adopted strategies that involve the use of proxies to achieve their geopolitical and strategic objectives. This proxy warfare3 approach enables states to exert influence and pursue interests without direct involvement, thereby reducing the risks of retaliation and maintaining plausible deniability. By employing non-state actors, states can conduct politically sensitive operations or violate international norms by conducting cyberattacks, targeted assassinations, or destabilization efforts, while clouding their direct role in these activities. The complex and clandestine nature of these relationships makes attribution difficult, complicating the international community's ability to hold states accountable for their proxies' actions.

Plausible Deniability best describes the role played by non-state actors for the government and high officials to avoid accountability. It aligns with “covert operations" long used by governments across the globe. The term's roots go back to US President Harry Truman's National Security Council Paper 10/2 of June 18, 1948, which defined covert operations as "all activities which are conducted or sponsored by this Government against hostile foreign states or groups or in support of friendly foreign states or groups but which are so planned and executed that any US Government responsibility for them is not evident to unauthorized persons and that if uncovered the US Government can plausibly disclaim any responsibility for them."

The implications of this trend are profound, as the traditional Westphalian model of state sovereignty and accountability is increasingly challenged. The blurred lines between state and non-state actions undermine the efficacy of the international legal frameworks designed to manage conflict and maintain global security. Furthermore, the use of proxies exacerbates regional instabilities and can escalate conflicts, as non-state actors often operate with a degree of autonomy that can lead to unpredictable and uncontrolled consequences. Addressing these challenges requires a nuanced understanding of the motivations and mechanisms behind state-proxy relationships, as well as enhanced international cooperation and robust strategies to counteract the influence and operations of non-state actors in the global arena.

3. The use of non-state actors by states

It is essential to distinguish between different types of non-state actors. Groups like Hezbollah or ISIS operate with

[2] Parker, N., & Cave, D. (2015). *Non-State Actors in International Relations*. Routledge.

[3] Barzashka, I. (2015). Proxy Warfare and the Future of Conflict. *Strategic Studies Quarterly*, 9(3), 99-123; Mumford, A. (2013). *Proxy Warfare*. Polity.

distinct agendas and structures, often acting independently or with specific ideological motivations. In this paper, focus is put on numerous cases of states utilizing non-state actors for their own purposes. In those cases, the primary aim is to obscure attribution and complicate international accountability. For instance, state-sponsored non-state actors might be involved in cyberattacks, asymmetric warfare, or other covert operations that serve that state's strategic interests while maintaining its plausible deniability.

The deliberate use of such actors by states creates a grey area in international relations and law, as the traditional frameworks for accountability and response are less effective. This strategy not only blurs the lines of responsibility but also undermines the mechanisms designed to uphold international norms and security. As a result, it necessitates more sophisticated and coordinated efforts in intelligence, diplomacy, and cybersecurity to accurately identify and address the true sources of these threats.

3.1 Lazarus Group and North Korea

An example of that is the North Korean hackers used for cybercrime and espionage. The state-sponsored hacking group, the Lazarus Group, has been involved in various cyber operations, including the 2014 Sony Pictures hack and the 2017 WannaCry ransomware attack, which affected hundreds of thousands of computers in over 150 countries, including critical infrastructure like the UK's National Health Service. Other significant targets affected included Spain's Telefónica, Germany's Deutsche Bahn, and FedEx in the United States. A complex process of combined technical analysis, forensic evidence, and intelligence assessments has allowed the attribution of the WannaCry ransomware attack to North Korean hackers, specifically the Lazarus Group.

Cybersecurity researchers identified significant similarities between the WannaCry code and other malware previously attributed to the Lazarus Group. These similarities included specific lines of code, algorithms, and unique characteristics that were consistent with known North Korean hacking operations (Kaspersky Lab, 2017). In addition, the infrastructure used in the WannaCry attack, such as command and control servers, overlapped with the infrastructure used in past attacks by the Lazarus Group. This overlap provided strong evidence linking the ransomware to North Korean actors (US-CERT, 2017).

On the other hand, national intelligence agencies were significantly involved in investigating and assessing the WannaCry ransomware attack, including those from the United States and the United Kingdom. These agencies possess access to classified information and advanced intelligence-gathering capabilities, providing additional context and evidence that linked the attack to North Korean state-sponsored actors (Office of the Director of National Intelligence, 2018; National Cyber Security Centre, 2018). The collaboration between these intelligence entities and cybersecurity experts played a crucial role in the comprehensive analysis and attribution of the attack. Despite this overwhelming evidence, North Korea has labelled the US accusation a "grave political provocation" with "ulterior motives" and never taken the blame nor punished anyone. "This move is a grave political provocation by the US aimed at inducing the international society into a confrontation against the DPRK by tarnishing the image of the dignified country and demonizing it," DW quoted a spokesperson for the DPRK.

3.2 Little Green Men and the Russian Federation

The use of non-state actors by Russia in the Ukraine war, particularly since the annexation of Crimea in 2014, provides a model case of hybrid warfare strategy. These non-state actors include paramilitary groups and private military companies, such as the Wagner Group, that have been involved in a range of actions, from direct combat to training and advising separatist forces and local militias. It has played a crucial role in the destabilization of the region. The Wagner Group has been described as an attempt at plausible deniability of Kremlin-backed interventions not only in Ukraine but in Syria and in various African countries as well.

Another important component are local separatist groups, organized in both military and non-military units. The latter serve as a powerful arm of disinformation and propaganda machinery. In Eastern Ukraine, particularly in the Donetsk and Luhansk regions, Russia has supported and sometimes directly organized local militias and separatist groups. These groups have been armed, trained, and sometimes led by Russian operatives. They receive substantial support from Russia, blurring the lines between local insurgencies and state-backed operations.

Finally, one of the most notable non-state actors in the Russian aggression against Ukraine was the appearance of the so-called "little green men" during the annexation of Crimea in 2014. These were unmarked soldiers in green uniforms, later identified as Russian Special Forces, who played a key role in taking over key installations and infrastructure in Crimea without direct attribution to the Russian state.

3.3 Separatist wars in Georgia and the Russian Federation

Russia's involvement with non-state actors and local separatist groups in Georgia set a prominent example well before the start of the brutal war against Ukraine. It showed its broader strategy of using hybrid warfare to undermine the principles of state sovereignty and territorial integrity, to influence regional politics, and to assert its geopolitical interests. This strategy has been particularly evident in the Abkhazia and South Ossetia regions. The support for separatist movements in Georgia illustrates Russia's use of non-state actors to achieve its

strategic objectives without resorting to full-scale conventional warfare. This approach allowed Russia to maintain a degree of plausible deniability and to exert influence over its neighbours while avoiding the direct political and military costs associated with outright annexation or prolonged military occupation. This took place in the early nineties of the last century when the concept of hybrid warfare was neither clearly defined nor comprehended.

Unfortunately, regardless of all the tools and strategies deployed against Georgia, they did not provide sufficient grounds for the international community to understand to what extent the Russian Federation was ready to establish itself on the territories it claimed as its own.

All the precedents were set. In both Abkhazia and South Ossetia, local militias and paramilitary groups have played critical roles in maintaining control over these regions. These forces, often composed of ethnic Abkhazians, Ossetians, and volunteers from the North Caucasus, were commanded and trained by regular Russian army instructors. Russia has supplied and fed all separatist groups, paramilitaries, and militias with military equipment, training, and financial resources. This support has included the provision of arms and military advisors, which has bolstered the separatists' capabilities to resist Georgian control. During the war in the early 1990s and the brief war in 2008, Russian military involvement was the only cause for the separatists' successes against Georgian forces.4

4. The Subversive Influence of Hybrid Threats on Democratic Societies

Hybrid threats are multifaceted and sophisticated. They serve different goals depending on the circumstances and actors. Regardless of the specific goals, one common dominator is to aim at the erosion of public trust towards democratically elected governments, democratic institutions, and the rule-based order. They target the foundational values that sustain democracies, such as freedom of speech and the integrity of electoral processes. Hybrid threats are designed to exploit the inherent vulnerabilities of democratic societies, undermining the values and principles that maintain these systems.

4.1 Erosion of Public Trust in Institutions and Political Integrity

In the heart of a bustling democratic nation, trust and confidence in the government are the cornerstones of society. Citizens engage in lively debates, media outlets thrive on freedom of speech, and elections are celebrated as the pinnacle of democratic expression. However, unseen forces are at work, seeking to undermine these very foundations.

4.2 Disinformation Campaigns

Several methods used by adversaries and disinformation campaigns are, by far, the most sophisticated and effective at creating confusion and scepticism among the public. This erosion of trust in government, media, and other institutions destabilizes the democratic process. As an example, one can recall the case of the 2016 US presidential elections, where the extensive use of social media by Russian state-sponsored actors to amplify divisive content has been documented extensively, notably in reports by the Senate Intelligence Committee on Russian interference in the 2016 US elections.

Imagine a country where the truth is no longer clear, where every piece of news is questioned, and doubt creeps into the minds of even the most informed citizens. This is the new reality for any nation under siege by disinformation campaigns. In the 2016 US presidential election, shadowy figures from Russia's Internet Research Agency (IRA) crafted a web of false narratives. These operatives spread fake news and divisive content across social media platforms, targeting voters with precision. Their goal was simple: to sow discord among the populace by eroding trust in the electoral process. As the election drew closer, their disinformation reached a fever pitch. Social media feeds were flooded with sensational headlines, each designed to play on fears and prejudices. The result was a fractured society, with citizens doubting the integrity of their institutions and the legitimacy of the electoral process. Trust in the media and the government began to waver, and the once unshakable faith in democracy started to crumble.

Disinformation campaigns attack a fundamental pillar of democracy: freedom of speech. Adversaries exploit the free flow of information, the very principle of liberal democracies and open societies, to infiltrate, influence, and destabilize from within. In the shadows, state and non-state actors work tirelessly to control the narrative. For example, in various countries, Russian state-owned media and affiliated outlets spread their narratives, discrediting independent journalism and promoting their agendas. This

[4] See *The War For Abkhazia: 25 Years Later,* by Amos Chapple at https://www.rferl.org/a/twenty-five-years-on-from-the-start-of-the-abkhaz-war/28690617.html or, *Point Of No Return: 30 Years On, Survivors Remember The War In Abkhazia* at https://www.rferl.org/a/georgia-abkhazia-war-survivor-memories/32620722.html

manipulation extends beyond traditional media to the digital sphere, where troll farms and botnets harass and intimidate journalists, activists, and ordinary citizens who dare to speak out. Their success is celebrated once the public starts to doubt every bit of information, when lines are blurred, and even the idea of honest journalism is lost. That, coupled with the massive pressure of constant harassment in social media, taints the once vibrant public discourse with fear. The threat of online harassment and provocations silences voices that once spoke freely. This chilling effect is very tangible, and the freedom to express dissenting opinions is under siege. The very essence of democracy, built on the exchange of ideas and open debate, is at risk.

4.3 Cyber Attacks

Beyond the realm of disinformation, another threat looms in the digital ether. The critical infrastructure of democratic countries, from power grids to public services, is constantly threatened by cyber-attacks. In 2015, Ukraine faced this chilling reality when a cyber-attack attributed to Russian hackers plunged parts of the country into darkness. Power grids failed, homes were without electricity, and the vulnerability of essential services was laid bare.

In this interconnected world, the cyber domain became a battlefield where adversaries could strike without warning. The attackers do not need to cross borders with armies; they simply need to exploit weaknesses in the nation's digital defenses. Each successful breach might erode public confidence in the government's ability to protect its citizens, shaking the very foundations of society. Conventional forces might get involved eventually, as needed. Still, war starts long before actual army intervention, specifically undermining trust in the elected government and its ability to protect, making response more difficult.

4.4 Election Interference

Targeting election infrastructure is not exclusive to US elections. Russia used this tactic on multiple occasions, from the Balkans to Ukraine, Georgia, etc. In 2020, the European Union highlighted the threat of foreign interference in its electoral processes, citing numerous instances of cyber-attacks and disinformation campaigns originating from state actors like Russia and China.5 The Kremlin understands elections as the best time to disturb and manipulate. Long before the start of the election cycle, massive disinformation campaigns are being prepared. Covert influence operations seek to manipulate electoral outcomes. These efforts can include spreading false information about candidates, covert funding of certain political groups6, or even hacking voter databases.

4.5 Economic Coercion

Economic Coercion and political manipulation highlight hybrid threats' most complex and insidious nature. Coercion is another tool used intensively to erode public trust in democratic institutions, and it can be just as powerful as the military. To combat these threats, nations must build resilience, strengthening their economic independence and political integrity. Understanding, recognizing, and addressing the nuances of economic coercion is essential for democratic societies to better protect themselves from the unseen forces that seek to compromise their sovereignty and values.

In a world where nations are interconnected by trade and finance, the power to influence extends beyond the battlefield and into the realms of economics and politics. Often behind closed doors, politicians struggle with the moral implications of their "pragmatic" decisions dictated by business and economic interests. Economic coercion created a chasm between principles and pragmatism, leading to compromises that chipped away at political integrity. What began as a stand for democratic values was now a complex balancing act, with economic survival hanging in the balance.

The typical scenario of a more "pragmatic approach" involves urging the government to mend ties and restore trade even with adversaries. Lobbyists, public figures, or influencers usually arrive first with calls for "normalization" as soon as economic pressure escalates and leaders in democratic nations face increasing calls to reconsider their political stances. Influenced by economic interests, the media echoes these sentiments, delicately shifting public opinion.

Numerous such instances occurred in Georgia before the

---

5 Cyber-enabled foreign interference in elections and referendums, by Sarah O'Connor, Fergus Hanson, Emilia Currey & Tracy Beattie, at ASPI_ICPC https://www.aspi.org.au/report/cyber-enabled-foreign-interference-elections-and-referendums See also, *Report on foreign interference in all democratic processes in the European Union, including disinformation* by Special Committee on foreign interference in all democratic processes in the European Union, including disinformation (INGE 2). Rapporteur: Sandra Kalniete at https://www.europarl.europa.eu/doceo/document/A-9-2023-0187_EN.html

6 See materials about Russian covert funding of Georgian Dream Party in 2024 parliamentary elections in Georgia. *Russian Ties of Georgian Dream Donors: Market Dependency and State-Favored Financial Benefits* by Civic IDEA at https://civicidea.ge/en/russian-ties-of-georgian-dream-donors-market-dependency-and-state-favored-financial-benefits/8877/ and *Russian Businesses of Georgian Dream Donors* by Civic IDEA at https://civicidea.ge/en/russian-businesses-of-georgian-dream-donors-part-ii/9105/

2008 war. In 2006, after the Georgian government arrested four Russian army officers on charges of spying. Later, on the same day, they were handed over to Russia with the OSCE's facilitation7. Almost immediately, the repercussions began. The Russian Federation, feeling insulted, imposed severe trade restrictions on Georgia's key exports, with a total ban on exports8 from Georgia. Immediately, "traditional" trade saw a sharp decline in activity, and the economy started to feel the strain. Russia, particularly its Chief Sanitary Inspector Gennady Onishenko,9 was effectively manipulating Georgia's political decisions without firing a single shot.

Initially, the developments were catastrophic for the Georgian wine industry, which had been exporting up to 90 percent of its products to Russia since Soviet times. The ban expanded to the mineral waters Borjomi and Nabeglavi as well as other agricultural products, which most traditionally went to the Russian markets. Local businesses, dependent on exports, began to struggle. Jobs were lost, and the political climate grew tense as citizens demanded action. The government faced a difficult choice: to stand firm on its principles or to capitulate to the economic pressure.

Although the embargo's consequences were disastrous initially, with strong determination and proper policies, Georgia soon diversified its exports. Russian sanctions even helped to raise Georgian wine production and some other exports to higher standards compatible with European and North American market criteria.

In addition to economic measures, financial manipulation, through specially devised investment, loans, and credit policies, has become another tool. As such, state investments may be selectively directed to politically favourable factions within the democratic nation, subtly influencing the political landscape. The infusion of funds creates dependencies, and it only takes a short time before certain political groups find themselves aligned with the interests of the coercive state. As an example, one can recall Russia using targeted energy investments to gain political allies in Eastern Europe and the Balkans. For instance, Russia has extended loans and favourable gas pricing to countries with pro-Russian political leaders, creating economic dependencies. In Hungary, Prime Minister Viktor Orbán's government has maintained a close relationship with Moscow, partly due to a major Russian-backed loan to finance the Paks nuclear power plant expansion. This financial relationship has sometimes aligned Hungarian policies more closely with Russian interests despite Hungary being an EU member.10

The adversary's calculation is simple: policy decisions must begin reflecting the new realities dictated by the markets' mounting pressure on politics and elections. External economic influences taint the democratic process. The erosion of democratic norms is neither immediate nor overt but a slow, creeping process that gradually compromises the political integrity of the political class if not confronted by a firm deterrence policy.

4.6 Migration Crisis and Social Division

Every day, malign actors exploit social divisions in different parts of the world. Hybrid threats are used not only to target institutions but to tear apart the social fabric of a nation itself. Active exploitation from foreign interferences and disinformation campaigns prepares grounds for the rise of the populist right, and this is where populism or the extreme right takes over. The European migration crisis serves as an example, where disinformation campaigns stoked fears and xenophobia across Europe. Inflammatory content fuelled nationalist sentiments and deepened political polarization. Research from the European Policy Centre indicates that these efforts aim to stoke fear, deepen social divides, and support populist agendas11. During the 2015 European migration crisis, disinformation actors linked migration to threats against health, wealth, and national identity, manipulating existing insecurities to fuel nationalist sentiments across Europe. False narratives claimed that migrants were responsible for crime, disease, or economic strain, resonating deeply with polarized audiences. According to EPC, disinformation stories are frequently "laundered" across borders, with fake stories about migration re-emerging in various European media ecosystems, such as Germany, Italy, and Spain. These stories spread through traditional channels and private messaging apps, evading fact-checking efforts and

---

7 See Georgia: Ulterior Motives Seen Behind Escalation Of Spy Row, by RFE/RL at https://www.rferl.org/a/1071743.html for reoccurring story see https://www.rferl.org/a/Georgia_Says_13_Alleged_Russian_Spies_Arrested/2211508.html

8 See *Russia Cuts Off Georgian Water and Wine* at https://iwpr.net/global-voices/russia-cuts-georgian-water-and-wine

9 See *First wine, now Russia bans Georgia's water*, at https://www.theguardian.com/world/2006/may/06/russia.nickpatonwalsh See also, https://www.messenger.com.ge/issues/3677_july_22_2016/3677_edit.html for reoccurring story see https://www.rferl.org/a/russia-bans-georgian-drinks/25130472.html

10 See *Hungary's Russian-built nuclear plant powered by politics in Brussels at https://www.politico.eu/article/hungarys-russian-built-nuclear-plant-powered-by-politics-in-brussels/ or Putin and Orban solidify Russian-Hungarian ties amid international pressures at https://www.lemonde.fr/en/european-union/article/2023/10/17/putin-and-orban-solidify-russian-hungarian-ties-amid-international-pressures_6182314_156.html*

11 See, ISSUE Paper: *Fear and lying in the EU: Fighting disinformation on migration with alternative narratives, by Alberto-Horst Neidhardt , Paul Butcher at https://www.epc.eu/content/PDF/2020/Disinformation_on_Migration.pdf*

strengthening extremist positions and mistrust in public institutions.

The tactics used in hybrid warfare evolve rapidly, often outpacing a defender's ability to develop effective countermeasures. This dynamic environment makes it challenging to keep up with an adversary's latest methods and technologies. For example, a cyber-attack might coincide with a disinformation campaign and a physical attack on infrastructure. This overlap of tactics can also obscure the origins and intentions of the threat.

4.7 China's Subtle Influence

China, a nation adept at using economic levers to achieve its geopolitical aims, provides numerous examples. Whenever countries have dared to oppose its policies, whether it was over territorial disputes or human rights issues, China has responded with trade restrictions or even pulling investments. The message was clear: opposing China came with significant economic costs.

Lithuania's decision to host a Taiwanese delegation in 2021, despite explicit warnings from China, triggered significant economic coercion from Beijing. China viewed the "Taiwan Representative Office" opening as a violation of its One China principle and responded by imposing trade restrictions on Lithuania. These included blocking exports, particularly of Lithuanian products like lasers, and pressuring companies, like Continental, which imported parts from Lithuania .12 The Lithuanian government's decision to open the Taiwanese office reflected its broader foreign policy shift towards supporting democratic values and human rights. Lithuania also condemned China's actions in Xinjiang and banned Chinese companies like Huawei from its 5G network13.

The economic squeeze was palpable, and soon, officials found themselves in heated debates, weighing the economic fallout against their diplomatic stance. Consequently, some Lithuanian officials acknowledged the cost, with some suggesting that the decision to host Taiwan was a mistake. However, despite the economic coercion, Lithuania did not reverse its stance. The country continued its approach, with some officials noting that they were determined not to give in to what they saw as Beijing's undiplomatic tactics.

5. Globalization as a Catalyst for the Amplification of Hybrid Threats

Hybrid threats represent a significant concern today due to their ability to exploit the vulnerabilities of interconnected, open societies using a combination of conventional and unconventional tactics. Technology and connectivity have significantly amplified the scope and impact of hybrid threats. The ability to disseminate disinformation widely, conduct sophisticated cyber-attacks, exploit global interdependencies, and coordinate operations in real time are key factors that make hybrid threats particularly challenging in the modern era.

Their ambiguity, complexity, and potential for widespread disruption demand a comprehensive, whole-of-society response to build resilience and protect democratic values. Significant concerns regarding a contemporary security landscape are based on several factors:

Technological advancement and the proliferation of digital technologies and the internet have created new avenues for successful hybrid warfare. Cyber-attacks, disinformation campaigns, and covert influence operations can be executed with greater speed and reach, targeting vast audiences and critical infrastructures with relative ease. Advancements in artificial intelligence, machine learning, and other emerging technologies are enhancing the capabilities of actors engaging in hybrid warfare. These technologies enable more sophisticated and targeted attacks, increasing potential disruption and damage. For instance, the common use of drones and artificial intelligence in hybrid warfare adds a completely new dimension and increases these threats' effectiveness. Drones can be used for surveillance, targeted strikes, or as platforms for cyber-attacks, while AI can enhance the effectiveness of disinformation campaigns through sophisticated targeting and content generation.

Hybrid threats often target civilian sectors, blurring the lines between civilian and military domains. Attacks on critical infrastructure, such as power grids, communication networks, and healthcare systems, can

---

12 See *How China is Punishing One Small European Nation over Taiwan*, at The Economist, https://www.economist.com/search?q=%22How+China+is+Punishing+One+Small+European+Nation+over+Taiwan%22 or *An Analysis of China's nomic Coercion against Lithuania,* by Konstantinas Andrijauskas, at https://www.cfr.org/sites/default/files/pdf/Andrijauskas_An%20Analysis%20of%20China's%20Economic%20Coercion%20Against%20Lithuania_0.pdf see also https://www.fpri.org/article/2023/07/lithuanias-bet-on-taiwan-and-what-it-means-for-europe/

13 See, https://www.datacenterdynamics.com/en/news/european-union-considers-mandatory-ban-on-huawei-in-5g-networks-report/

have devastating impacts on civilian populations, creating chaos and eroding societal resilience.

Increased connectivity is fertile ground, particularly for instrumentalizing trade, economies, and investments. The interconnected nature of the global economy and international relations means that the impact of hybrid threats can have far-reaching consequences beyond the immediate target. Disruptions in one region can have cascading effects on global markets, supply chains, and geopolitical stability. An example was the 2017 NotPetya cyber-attack, attributed to Russian actors, which targeted Ukrainian companies but quickly spread globally, affecting major corporations like Maersk and FedEx and causing billions of dollars in damage.14

Traditional security paradigms and defence mechanisms are eroding. Conventional military strategies and doctrines are often ill-suited to address these threats' multifaceted and diffuse nature, necessitating new approaches and greater collaboration across sectors. Additionally, technological advancements have outpaced theoretical and legal frameworks, highlighting a significant gap that must be addressed.

6. Recommendations and Conclusion

To effectively combat hybrid threats, it is essential to recognize that this process involves three critical stages: recognition (acknowledging), mapping, and addressing. Each of these stages is integral to building a robust and adaptive resilience framework capable of countering the complex and dynamic nature of hybrid threats. By progressing methodically through these stages, policymakers and stakeholders can better safeguard democratic values and maintain the integrity of their societies in the face of evolving challenges.

The first and foundational step in building successful resilience is acknowledging these threats' complexity and pervasive nature. This stage involves a deep and systematic understanding of the environment in which hybrid threats operate. It requires identifying the vulnerabilities within a society's political, economic, and social fabric and technological systems that adversaries might exploit. Recognition is not just about awareness but also about appreciating the interdependencies and the potential cascading effects that hybrid threats can have across various sectors. By recognizing the full scope of these threats, policymakers and stakeholders can better anticipate the ways in which hybrid tactics might manifest and disrupt democratic processes.

Once the complexity and potential vulnerabilities are recognized, the next crucial stage is **mapping.** This involves a detailed analysis and documentation of the specific pathways through which hybrid threats could penetrate and affect society. Mapping includes identifying key actors, both state and non-state, who may be involved in deploying hybrid tactics and understanding their motivations, capabilities, and strategies. It also requires a thorough assessment of these actors' resources and methods, such as cyber tools, disinformation campaigns, economic pressure, or proxy forces. Effective mapping provides a strategic overview that helps in visualizing how different elements of hybrid threats are interconnected and where they might converge to create significant impacts. This stage is critical for developing targeted and proactive measures to mitigate risks.

The final stage in combating hybrid threats is **addressing** the identified challenges through a coordinated and comprehensive approach. This stage involves implementing practical measures to strengthen resilience and counteract the specific vulnerabilities and threats that have been recognized and mapped. Addressing hybrid threats requires a multifaceted strategy that may include enhancing cybersecurity, improving information integrity, building public awareness, and fostering international cooperation. It also involves developing and enforcing legal and regulatory frameworks that adapt to hybrid threats' evolving nature. Moreover, addressing these threats demands a whole-of-society approach, engaging not just government agencies but also private sector entities, civil society organizations, and the general public.

Best practices might include:

Applying societal preparedness measures. This involves strengthening community networks and fostering a culture of resilience to withstand and recover from hybrid attacks. It also involves initiatives to promote social cohesion and trust in institutions. For effective action, it is essential to educate citizens about hybrid threats and emergency readiness through diverse civil defence training programs that are run systematically and cohesively as part of formal education curricula. Public awareness campaigns and training programs can empower individuals to recognize and respond to threats effectively.

Civil-military cooperation is a vital element of defence. This is why it is of utmost importance to have society prepared

---

14 See *The Untold Story of NotPetya, the Most Devastating Cyberattack in History: Crippled ports. Paralyzed corporations. Frozen government agencies. How a single piece of code crashed the world* by Andy Greenberg at https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ or Case Documents of Notpetya Cuber Attack, at https://www.sipa.columbia.edu/sites/default/files/2022-11/NotPetya%20Final.pdf

and educated about various ways and tools used by adversaries utilizing hybrid threats. Effective collaboration between the military, law enforcement, intelligence, formal education institutions, and civil society is crucial for a coordinated response to hybrid threats and the establishment of clear frameworks for cooperation. As extreme as it might sound, in frontline countries under higher risks, it is highly recommended that joint exercises between military and civilians be conducted to improve coordination and response to hybrid threats. This enhances overall security.

Investing in advanced cybersecurity measures, including threat detection, incident response capabilities, and robust educational and training programs, is another essential step to protect critical infrastructure and information systems from cyber-attacks. Comprehensive incident response plans must be developed and regularly updated to quickly address and mitigate the impact of cyber-attacks. Success is only guaranteed if all these measures are implemented by fostering collaboration between government agencies and private sector companies to share threat intelligence and best practices.

To protect critical infrastructure, the initial steps are to conduct regular risk assessments to identify vulnerabilities and establish strong redundant systems and backup protocols to ensure the continuity of essential services during attacks. This can only be achieved with solid public-private partnerships, as most of the critical infrastructure is privately managed and owned.

Last but not least, information integrity and effective disinformation countermeasures are required. Information warfare is an entirely separate, well-developed concept used around the world by malign powers. It is used to disorient societies, break trust, and interfere with the fundamental value systems societies built in liberal democracies. Thus, it is an absolute must to implement robust media literacy programs, including formal educational programs, to help the public identify and critically assess disinformation. Governments must encourage and even support independent fact-checking organizations to verify information and debunk false narratives on a regular basis.

Public civil-military cooperation and partnership are particularly important because a modern military has a ratio of approximately 1:10 of the "frontline soldier armed to the teeth to rearguard and support units," also widely known as the "tooth-to-tail ratio."15 It is a widely discussed figure in military literature. It means that about eight or nine people in support units are responsible for the success of one soldier on the frontline. Thus a large majority of those in the armed forces serve the protection of their homeland from a workplace instead of with weapons in hand, that is logistics, medical support, communications, maintenance, etc. Given the shifting realities and the different, developed, and technologically advanced nature of warfare today, more than ever before, strong societal preparedness is the key to success.

Finally, international cooperation in sharing intelligence and best practices is vital to addressing the transnational nature of hybrid threats. Strengthening alliances and collective defence agreements ensures a unified front against adversaries.

As the shadows of hybrid threats loom larger, the urgency to address them becomes clear. To maintain the integrity and functioning of democratic systems, it is crucial that political leaders, along with international allies, recognize and address these threats. Efforts need to be ramped up to enhance cybersecurity measures, educate the public on media literacy, and protect critical infrastructure.

Numerous efforts have been put in place in multiple EU or neighbourhood states; public awareness campaigns have been launched, informing citizens about the nature of hybrid threats and how to discern fact from fiction. A joint military and civilian exercises are being conducted to improve coordination and response to these multifaceted threats. International cooperation is strengthened, with nations sharing intelligence and best practices to present a united front against these sophisticated adversaries.

Fighting hybrid threats is essentially the fight for democracy. It is an ongoing battle, a continuous struggle to protect the values that underpin democracy. This paper serves as a stark reminder of the vulnerabilities that exist in our interconnected world. It highlights the importance of vigilance, resilience, and collective action in safeguarding the principles of freedom, trust, and integrity that define democratic societies.

About the Author

The author, Tinatin Khidasheli, is the Chairwoman of the Georgian think tank Civic IDEA. Formerly liberal politician, MP, and Minister of Defence of Georgia.

[15] See The 'Tooth-to-Tail' Ratio and Modern Army Logistics, by James M Berry, at https://dalecentersouthernmiss.wordpress.com/2021/11/03/the-tooth-to-tail-ratio-and-modern-army-logistics/ or The Long War Series, vol. Occasional Paper 23 *The Other End of the Spear: The Tooth-to-Tail Ratio (T3R) in Modern Military Operations* (PDF by McGrath, John J. at https://www.armyupress.army.mil/Portals/7/combat-studies-institute/csi-books/mcgrath_op23.pdf

Bibliography

1. Barzashka, I. (2015). Proxy Warfare and the Future of Conflict. *Strategic Studies Quarterly*, 9(3), 99-123.
2. Clunan, A. L., & Trinkunas, H. A. (Eds.). (2010). *Ungoverned Spaces: Alternatives to State Authority in an Era of Softened Sovereignty*. Stanford University Press.
3. Cockayne, J. (2016). *Hidden Power: The Strategic Logic of Organized Crime*. Oxford University Press.
4. Kaldor, M. (2013). *New and Old Wars: Organized Violence in a Global Era*. Stanford University Press.
5. Mumford, A. (2013). *Proxy Warfare*. Polity.
6. Parker, N., & Cave, D. (2015). *Non-State Actors in International Relations*. Routledge.
7. Weiss, T. G. (2013). *Global Governance: Why? What? Whither?*. Polity.
8. Office of the Director of National Intelligence. (2018). "Worldwide Threat Assessment of the US Intelligence Community." Retrieved from ODNI.
9. National Cyber Security Centre. (2018). "Advisory: North Korean Malicious Cyber Activity." Retrieved from NCSC.
10. Symantec. (2017). "Lazarus, WannaCry and the Blind Spot in Banking Cyber Security." Retrieved from Symantec Official Blog.
11. Kaspersky Lab. (2017). "WannaCry Ransomware Used in Wide-scale Attack." Retrieved from Kaspersky Lab Securelist.
12. US-CERT. (2017). "North Korean Malicious Cyber Activity." Retrieved from US-CERT.
13. NHS Digital. (2017). "WannaCry Cyber Attack and the NHS." Retrieved from NHS Digital.
14. CrowdStrike. (2017). "2017 Global Threat Report: Insights on the Cyber Threat Landscape." Retrieved from CrowdStrike.
15. Buchanan, E. (2016). The Role of Private Military Companies in the Ukraine Conflict. *Journal of Strategic Studies, 39*(7), 854-878.
16. Galeotti, M. (2014). Hybrid War or Gibridnaya Voina? Getting Russia's Non-Linear Military Challenge Right. *Jane's Intelligence Review*.
17. Rid, T. (2020). *Active Measures: The Secret History of Disinformation and Political Warfare*. Farrar, Straus and Giroux.
18. Sakwa, R. (2015). *Frontline Ukraine: Crisis in the Borderlands*. I.B. Tauris.
19. Cohen, A., & Hamilton, R. E. (2011). *The Russian Military and the Georgia War: Lessons and Implications*. Strategic Studies Institute.
20. Cornell, S. E. (2002). *Autonomy and Conflict: Ethnoterritoriality and Separatism in the South Caucasus – Cases in Georgia*. Uppsala University.
21. Fawn, R. (2008). *Georgia: Revolution and War*. Routledge.
22. Gegeshidze, A. (2009). Russia's Economic Influence in Abkhazia and South Ossetia. *Georgian Foundation for Strategic and International Studies, Policy Paper*.
23. Toal, G. (2017). *Near Abroad: Putin, the West, and the Contest over Ukraine and the Caucasus*. Oxford University Press
24. International Institute for Strategic Studies. (2020). "China's Use of Coercive Economic Measures."
25. Australian Strategic Policy Institute. (2020). "The China 'Threat': Responses from the Indo-Pacific Region."
26. European Commission. (2018). "Joint Communication to the European Parliament and the Council: Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats."
27. RAND Corporation. (2019). "A Framework for Resilience: Key Elements and International Good Practices."
28. Rid, T. (2020). "Active Measures: The Secret History of Disinformation and Political Warfare." Farrar, Straus and Giroux.
29. U.S. Senate Select Committee on Intelligence. (2019). "Russian Active Measures Campaigns and Interference in the 2016 U.S. Election."
30. House of Commons Digital, Culture, Media and Sport Committee. (2018). "Disinformation and 'fake news': Interim Report."
31. National Defense Strategy Commission. (2018). "Providing for the Common Defense: The Assessments and Recommendations of the National Defense Strategy Commission."
32. European Union External Action Service. (2020). "EEAS Special Report Update: Short Assessment of Narratives and Disinformation Around the COVID-19 Pandemic."
33. DFRLab. (2019). "The Weaponization of Migration."
34. NATO Strategic Communications Centre of Excellence. (2018). "Hybrid Threats: A Strategic Communications Perspective."
35. Department of Homeland Security. (2020). "Cybersecurity and Infrastructure Security Agency (CISA) Annual Report."
36. Sanger, D. E. (2017). "The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age." Crown.
37. International Institute for Strategic Studies. (2020). "China's Use of Coercive Economic Measures."

38. Australian Strategic Policy Institute. (2020). "The China 'Threat': Responses from the Indo-Pacific Region."
39. Freedom House. (2020). "Freedom and the Media 2020: A Downward Spiral."
40. Reporters Without Borders. (2020). "World Press Freedom Index."
41. DiResta, R., et al. (2019). "The Tactics & Tropes of the Internet Research Agency." Graphika and Oxford Internet Institute.
42. U.S. Senate Select Committee on Intelligence. (2019). "Russian Active Measures Campaigns and Interference in the 2016 U.S. Election."
43. Greenberg, A. (2018). "The Untold Story of NotPetya, the Most Devastating Cyberattack in History." Wired.
44. Perlroth, N. (2021). "This Is How They Tell Me the World Ends: The Cyberweapons Arms Race." Bloomsbury Publishing.
45. Lewis, J. A., & Cavanaugh, E. (2016). "The Role of Offensive Cyber Operations in NATO's Collective Defence." Center for Strategic and International Studies (CSIS).
46. Scharre, P. (2018). "Army of None: Autonomous Weapons and the Future of War." W. W. Norton & Company.
47. Cadwalladr, C., & Graham-Harrison, E. (2018). "Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach." The Guardian.
48. European Commission. (2018). "Joint Communication to the European Parliament and the Council: Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats."
49. NATO Strategic Communications Centre of Excellence. (2018). "Countering Hybrid Threats: A Critical Review of the EU's Approach."
50. Center for Cyber and Homeland Security at The George Washington University. (2017). "The Future of Cybersecurity: Emerging Threats and Risk Management."
51. National Infrastructure Advisory Council. (2017). "Surviving a Catastrophic Power Outage: How to Strengthen the Capabilities of the Nation."
52. RAND Corporation. (2019). "A Framework for Resilience: Key Elements and International Good Practices."
53. U.S. Senate Select Committee on Intelligence. (2019). "Russian Active Measures Campaigns and Interference in the 2016 U.S. Election."
54. Rid, T. (2020). "Active Measures: The Secret History of Disinformation and Political Warfare." Farrar, Straus and Giroux.
55. European Commission. (2018). "Joint Communication to the European Parliament and the Council: Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats."
56. NATO Strategic Communications Centre of Excellence. (2018). "Countering Hybrid Threats: A Critical Review of the EU's Approach."
57. The Guardian. (2018). "How Russia's Troll Army Hit America."
58. U.S. Senate Select Committee on Intelligence. (2019). "Russian Active Measures Campaigns and Interference in the 2016 U.S. Election."
59. Rid, T. (2020). "Active Measures: The Secret History of Disinformation and Political Warfare." Farrar, Straus and Giroux.
60. Greenberg, A. (2018). "The Untold Story of NotPetya, the Most Devastating Cyberattack in History." Wired.
61. The Guardian. (2018). "How Russia's Troll Army Hit America."
62. NATO Strategic Communications Centre of Excellence. (2018). "Countering Hybrid Threats: A Critical Review of the EU's Approach."
63. European Commission. (2018). "Joint Communication to the European Parliament and the Council: Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats."
64. RAND Corporation. (2019). "A Framework for Resilience: Key Elements and International Good Practices."

freiheit.org