ISSN: 2450-6869

eISSN: 2719-6763

No. 22, 2025

DEFENCE SCIENCE REVIEW

http://www.journalssystem.com/pno/

DOI: 10.37055/pno/221320

Hybrid Threats and Deterrence Effectiveness in Europe

Original article

Received: 2026-04-20

Peer review: 2026-04-25

Revised: 2026-04-26

Final review: 2026-04-27

Accepted: 2026-05-03

Double blind

Keywords:

security dilemma, hybrid threats, deterrence and european security.

Chick Edmond[1,A-F]

ORCID 0009-0006-9633-0945

A - Research concept and design, B - Collection and/or assembly of data, C - Data analysis and interpretation, D - Writing the article, E - Critical revision of the article, F - Final approval of the article

[1]Graduate Program in International Studies, Old Dominion University, United States

Abstract

Objectives: The current European security landscape is characterized by the growing intersection of historical security challenges (i.e., "traditional" security issues) and new forms of hybrid threats. These changes call for a significant re-evaluation of the role of deterrence in today's world. Traditional deterrence approaches have focused on the use of military capability as well as credible retaliatory threats. However, the recent development of hybrid warfare, including cyber-attacks, disinformation campaigns, economic coercion, and clandestine sabotage has made it increasingly difficult to distinguish between times of war and times of peace. This research argues that existing frameworks for deterring adversaries will increasingly fail to meet the challenges presented by these evolving hybrid threats because most of these frameworks were developed to prevent or mitigate the consequences of traditional conventional and nuclear conflict.

Results: Findings suggest that hybrid warfare increases the level of uncertainty, misperceptions and risk of escalation associated with the security dilemma. Moreover, findings show that hybrid warfare undermines the credibility of deterrence. As such, the research presents the concept of "multi-domain deterrence," which proposes an integrated approach to preventing hybrid threats through the use of all available tools, including military, economic, technological and information-based mechanisms.

Conclusions: Overall, the research suggests the need for flexible, resilient and collaborative security approaches that move beyond traditional deterrence models.

Corresponding author Chick Edmond Graduate Program in International Studies, Old Dominion University, 5115 Hampton Blvd,, 23529, Norfolk, United States; email: cedmo005@odu.edu

1. Introduction

In recent years, the European security environment has experienced significant changes as a consequence of increased tensions within the global arena. Specifically, with the resurgence of great power rivalries and ongoing regional conflicts; the way Europeans have traditionally approached their security environment has shifted. Historically, European security was based upon a system of deterrence based on military capabilities and alliance commitments. The majority of these alliance commitments were based on the North Atlantic Treaty Organization (NATO) and the broader transatlantic security community. However, the development of hybrid threats has challenged the assumption of this traditional model of deterrence. Hybrid warfare includes both military and non-military tools such as cyber-attacks, disinformation campaigns, economic pressure and covert operations. These tools allow an adversary to destabilize another country without directly confronting them (Edmond, 2025). These types of conflicts are referred to as hybrids because they exist outside of the traditional definition of "war." The creation of this gray area between peace and war creates a broad continuum of conflict. Therefore, hybrid threats create challenges to the strategic thinking of European leaders. They realize that hybrid threats are evolving continuously and require alternative approaches to the security and deterrence models used historically. Recent examples of hybrid warfare include acts of sabotage of critical infrastructure, and cyber-attacks against European countries. Examples of sabotage of critical infrastructure include recent attacks on undersea communications cables and energy systems. These types of attacks demonstrate that adversaries are using the weaknesses of modern society's systems to achieve their strategic goals. Therefore, these types of actions demonstrate that the previous deterrent models used to prevent such attacks are no longer effective. As a result, there exists a need to reconsider the foundation of European security in the 21st Century.

The idea of the security dilemma offers a theoretical basis for analyzing the mistrust and escalating behavior of today's European security. The security dilemma comes from Realism, which describes a situation in which the actions a nation takes to increase its own national security will be viewed by other nations as a threat to their security, causing them to take similar actions that reduce the total amount of security in the world (Jervis, 1978). In the European context, the expansion of NATO and the military build-up of Eastern Europe have been seen by Russia as a threat to its security. Consequently, Russia has taken countermeasures to exacerbate the tension. Conversely, Russia's actions, such as the invasion of Ukraine and hybrid warfare against European countries, have been viewed by those European countries as aggressive and destabilizing. It is the creation of reciprocal perceptions of threat on both sides which contributes to the cycle of insecurity there by creating complex ambiguous nature of Hybrid Warfare. Hybrid Warfare attacks may occur anonymously via Cyberattack and Disinformation Campaigns. Consequently, identifying the party responsible for such an attack is nearly impossible. It is because of the lack of transparency related to hybrid warfare that there exists an increased risk of misperception and unintentional escalation. Also, as long as the parties involved do not have a clear understanding of at what point a specific level of response will be employed, the Credibility of all Deterrent Strategies will continue to decrease.

Hybrid warfare has emerged as a primary form of contemporary warfare particularly in Europe where adversaries have used vulnerabilities within open societies to undermine stability. Traditional warfare in the past consists of only applying military force, whereas hybrid warfare applies multiple tools to achieve strategic objectives. Examples of this include cyberattacks against critical infrastructure; disinformation campaigns intended to erode the confidence of the public; and economic coercion intended to weaken an adversary. The advantage of hybrid warfare lies in its ability to allow states to engage in these activities below the threshold of armed conflict. This allows for reduced opportunities for direct retaliation. Hybrid warfare has been widely utilized by Russia, and allegations suggest that it has been engaging in a long-term hybrid warfare campaign against European states. Hybrid warfare typically creates uncertainty and confusion, resulting in increased difficulty for the targeted state to respond effectively. Additionally, the plausibility of deniability further complicates the ability of states to assign accountability for hybrid warfare. As such, hybrid warfare presents a significant challenge to traditional models of deterrence, which rely upon assignment of accountability and credible threats of retaliatory action. Consequently, the increasingly frequent and sophisticated nature of hybrid attacks demonstrates a requirement for novel approaches toward security and deterrence. These developments also raise significant questions about the nature of international security in Europe in the years ahead.

The constantly changing nature of threats in Europe has made many academics and policymakers question whether the established classical deterrence strategies remain relevant. Classical deterrence theory was established by scholars including Thomas Schelling and John Mearsheimer who stated that the key to successful deterrents is to demonstrate credibility in the threat and have the capability to inflict considerable harm upon the adversary (Mearsheimer, 1983). Classical deterrence theory was based on the premise of a well-defined boundary of conflict, as the threat of war or the actuality of war clearly defined what actions were permissible. Hybrid threats exist in a "grey area" and thus create uncertainty as to how one applies classical deterrence principles. Cyberattacks and disinformation campaigns may not elicit a similar response as conventional military attacks. Thus, hybrid threats create a gap in deterrence because adversaries can exploit this ambiguity to carry out their goals with minimal consequence. Additionally, hybrid threats can be characterized as decentralized; hybrid threats typically include non-state actors and clandestine activities. Therefore, the establishment of a deterrence strategy will require a paradigmatic shift from a military-only focus to a multi-dimensional strategy that incorporates various components. A multi-dimensional strategy is necessary to ensure continued stability in an increasingly complex security environment.

Recent events in Europe indicate that hybrid threats are becoming an increasingly important aspect of regional security. Officials in Europe have stated that the continent is under attack through a coordinated campaign of hybrid warfare consisting of cyberattacks, drone incursions and sabotage of critical infrastructure. Hybrid Warfare has been identified as an evolving threat through increased numbers of hybrid attacks across Europe. Hybrid Attacks are designed to test the resilience of European Societies and Disrupt their Ability to Respond to External Threats. Drone incursions into European airspace and cyberattacks against government computer systems have highlighted concerns about the vulnerability

of critical Infrastructure within European Countries. The frequency of these types of incidents demonstrates the need for additional security measures and improved coordination amongst European States. Additionally, they highlight the Limitations of Current Deterrent Strategies When Addressing Non-Kinetic Threats. Furthermore, the Rapid Evolution of Technology Has Created New Ways for Adversaries to Exploit Vulnerabilities. As such, European countries Must Evolve Their Security Strategies to Counter the Emerging Threats. This requires Establishing a Comprehensive Security Strategy Which Incorporates Military, Economic and Technological Elements.

Technology's influence on the constantly changing dynamics of security is significant across various domains involving critical infrastructure in Europe. As a result, emerging technologies like cyber capabilities, artificial intelligence and autonomous systems - the way conflicts occur have significantly evolved. As such, technology has created a whole new range of conventional options which are faster, more precise and difficult to track than their predecessors. Cyberattacks provide an adversary with the ability to disrupt a nation's critical infrastructures and communications while leaving no trace of physical damage. It is for this reason as well as preventing cyberattacks that are increasingly becoming the weapon of choice among adversaries. With the advent of drones and autonomous systems, there exists now greater opportunity for non-traditional military and non-military operations. Traditional deterrence faces numerous challenges due to emerging technologies; the rapidity and complexity of technological developments heighten the likelihood of misperception/miscalculations. States will face challenges in identifying the intentions of their adversaries. Artificial intelligence incorporated into military systems raises further questions concerning the long-term viability/stability of deterrence, particularly in relation to nuclear weapons (Horowitz et al., 2019). In light of the continually expanding technological landscape, it underscores the need for European nations to develop new ways of thinking about security and to invest in both technological capabilities and resilience so they can effectively combat these threats. Investments in areas such as enhanced cybersecurity and the development of new methodologies to combat hybrid threats are examples of investments.

Institutional frameworks for European security play a crucial role in defining the manner in which European states respond to hybrid threats and security dilemmas. Traditional institutional frameworks, such as NATO and the European Union, provide structures for collective defense and cooperation. However, the emergence of hybrid threats has highlighted shortcomings in the institutional frameworks, specifically in terms of coordination and response. The decentralized nature of hybrid threats renders the application of collective defense mechanisms, such as Article 5 of the NATO treaty, problematic. This has generated calls for enhanced institutional adaptation and innovation to address the emerging challenges. Despite the call for greater institutional adaptation and innovation, the diversity of interest among European states hinders the ability to develop unified responses to hybrid threats. The differences in perceptions of threats, strategic priorities and political constraints among European states complicate cooperative efforts. There is a growing recognition of the need for greater coordination and integration to address hybrid threats. This includes the development of joint capabilities and the implementation of information sharing mechanisms. The strengthening of institutional resilience is therefore necessary to maintain

security in Europe. This will require both structural reform and greater political commitment from member states.

States' perception of threats and their response to those threats are influenced by both domestic and international factors. Public opinion and electoral dynamics can impact on how states perceive and respond to threats. Disinformation campaigns aimed at influencing the outcome of elections can reduce public trust and increase societal divisions. Additionally, these factors can weaken the ability of states to respond to external threats, thus increasing the intensity of the security dilemma. Economic factors, such as reliance on foreign energy resources, can limit policy options available to states and therefore, create vulnerability. Due to the interconnectedness of modern economies, it is increasingly difficult to separate economic and security concerns. The increased integration of economies has created a new area of statecraft, known as economic statecraft. Sanctions and trade restrictions have been used as a tool of deterrence in the economic domain. However, like many tools of deterrence, they can have unintended consequences. The implementation of sanctions or trade restrictions can lead to additional tensions and cause states to retaliate against one another. Thus, the relationship between domestic and international factors is very complex. Therefore, understanding the interplay between these two sets of factors will allow us to develop more effective security strategies.

European Hybrid Threats and Security Dilemmas Raise Questions About Future Deterrence and System Stability. The continued existence of hybrid threats and security dilemmas in Europe raises serious questions regarding the future of deterrence and the stability of the international system. Traditional forms of deterrence, that utilize the threat of military retaliation, may no longer be adequate to meet the challenges presented by hybrid warfare. Consequently, there is a growing demand for more flexible and adaptable forms of deterrence, which can counteract a variety of threats. Multi-domain deterrence strategies that combine military, economic and technological deterrent tools represent a form of deterrence that recognizes that deterrence is not limited to the military domain; rather, it exists throughout all domains of statecraft. Furthermore, there is a need to address the root causes of insecurity (i.e. mistrust and misperception) that give rise to the security dilemma. Efforts to promote confidence and increase transparency between states would help to achieve this goal. However, achieving greater confidence and transparency between states is a daunting task in an atmosphere of competition and uncertainty. Moreover, the increasing complexity of the security environment also raises significant questions about the potential role of international institutions in ensuring stability. Accordingly, the future of European security is uncertain.

The primary objective of this study is to answer the central research question: **“How do hybrid threats affect the security dilemma in Europe, and what does this mean for deterrence in the twenty-first century?”** The study employs a qualitative research design, which utilizes document analysis and discourse analysis of official statements and policy documents from European institutions, NATO and national governments. Key data sources include national security strategies, EU strategic documents, NATO communiques and speeches delivered by political leaders on hybrid threats and deterrence.

The methodological focus is thematic coding to identify patterns in how security, deterrence and hybrid threats are conceptualized in various contexts. Comparative analysis is employed to evaluate the similarities and differences in responses of European states. Secondary literature is also included to provide context for empirical results and add strength to the theoretical discussion. The central hypothesis is that hybrid threats increase the security dilemma through ambiguity and lower the threshold of conflict, which undermines traditional deterrence mechanisms. The study also hypothesizes that successful deterrence in the twenty-first century will require a transition from traditional deterrence strategies to multi-domain strategies that incorporate military and non-military deterrent tools. This represents an adaptation to the changing nature of conflict and the need for adaptable security strategies. The findings of this study will contribute to current discussions on the future of deterrence and the transformation of international security.

2. Methodology

In this study, I have used a qualitative research approach combining document analysis and discourse analysis to investigate how hybrid threats impact security dilemmas in Europe, and thus also, what it means for the development of deterrence in the twenty-first century. My methodology includes five elements: case selection, document sampling, coding process, interpretative analysis, and limitations.

2.1. Case Selection

For case selection purposes, I utilized purposeful sampling (Patton, 2015) and included three aspects: (1) geographical variability among various European regions (i.e., Northern, Central, Eastern and Western Europe); (2) institutional differences (i.e., NATO members, EU members, and/or members of both); (3) documented exposures to hybrid threats from January 2022 until December 2024. Based upon these criteria, I selected four focal countries: Estonia (high exposure; NATO /EU member), Germany (moderate-high exposure; NATO/EU member), Czechia (moderate exposure; NATO/EU member), and Poland (high exposure; NATO/EU member). In addition to the focal countries, I examined three examples of hybrid incidents per country: (a) cyberattacks on critical infrastructure; (b) disinformation campaigns directed towards elections or social cohesion; and (c) covert/sabotage operations. Furthermore, I analyzed three regional incidents affecting two or more states: Baltic Sea undersea cable interruptions (2023 – 2024); the Belarus-Poland migrant crises (2021 – 2022); and the EU-wide response to Russia's cyber-attacks on energy infrastructure.

2.2. Document Sampling

I sampled documents from four distinct categories during the time frame of 2014 – 2024. As such, the 2014 date captures the annexation of Crimea, a pivotal event marking an increase in hybrid warfare activities in Europe (Giles, 2016). The 2024 date provides currentness.

Category 1: National Security Strategies (n = 12)

These are strategic papers authored by Estonia (2023), Germany (2021 and 2023), Czechia (2023), Poland (2020 and 2024), France (2022), the United Kingdom (2021 and 2023),

Sweden (2022), Finland (2022), and the Baltic States' combined strategy (2024). Documents were retrieved from governmental ministries' web sites.

Category 2: European Union Strategic Documents (n = 8)

These include: the EU Hybrid Threat Compendium (2022); Strategic Compass (2022); the EU's Counter-Disinformation Action Plan (2023); the EU's Cyber Defense Policy (2023); and four European Parliament Resolutions addressing hybrid warfare (2022-2024). Documents were retrieved from EUR-Lex and the European External Action Service Repository.

Category 3: NATO Communiques and Reports (n = 15)

These include all Summit Communiques issued from 2014 until 2024; five reports produced by the NATO Cooperative Cyber Defense Centre of Excellence; and three reports generated by the Hybrid Centre of Excellence. Documents were retrieved from the NATO Public Library.

Category 4: Government Speeches and Reports (n = 22)

These include transcriptions of speeches made by Heads of State/Government (n = 12); reports generated by Parliamentary Inquiry Committees regarding hybrid incidents (n = 6); and reports provided by Intelligence Agencies related to publicly disclosed hybrid incidents (n = 4). Sources include Official Government Archives, Parliamentary Web Sites, and Intelligence Agency Public Releases.

2.3. Coding Process

All fifty-seven documents were fully read in order to develop an initial understanding of their contents using Braun and Clarke's (2006) six phase coding structure.

Phase One (Familiarization):Analytical Memos for each document were created while reading them fully.

Phase Two (Initial Coding):

A deductive Code Book was constructed based upon the theoretical model employed throughout this dissertation including twenty-seven codes grouped into six Parent Themes:

(1) Attribution Practices (five codes; clear attribution, ambiguous attribution, false attribution, attribution timeframe, attribution mechanism).

(2) Perception of Threats (four codes; existence-threatening threat, manageable threat, ambiguous threat, threat inflation).

(3) Deterrence Mechanisms (six codes; military deterrence; economic deterrence; cyber deterrence; informational deterrence; resilience as a deterrent; institutional deterrence).

(4) Escalation Dynamics (four codes; identification of thresholds; unintentional escalation; miscalculation risks; escalation ladder).

(5) Institutional Response (four codes; NATO-coordinated response; EU-coordinated response; bilateral cooperation; information-sharing).

(6) Capacity for Resilience (four codes; infrastructure-resilience; society-resilience; cyber-resilience; energy-resilience).

Phase Three (Identifying Themes):

Codes were then assigned to each of the fifty-seven documents by me. An independent coder (a doctoral research assistant) also coded a twenty percent sample of my coded documents (n = eleven documents) to determine intercoder reliability. We reached agreement of eighty-seven percent, with a Kappa Coefficient of .81 representing strong reliability.

Phase Four (Assessing Themes):

Themes were evaluated relative to coded data and the original research question. Due to conceptual overlap, I collapsed two themes: "economic coercion" and "technological disruption."

Phase Five (Defining Themes):

Each theme was defined utilizing inclusion/exclusion criteria. For example, I defined "attributive ambiguity" as references to evidence-based uncertainty about who committed a hybrid attack with high certainty. Thus, inclusion required a direct reference to evidentiary uncertainty.

Phase Six (Writing):

Thematic definitions were converted into findings presented in Section Three.

2.4. Interpretative Analysis

My interpretation followed three steps. Step one involved analyzing each of the three focal incidents per country, tracing the sequence of events leading up to the incident(s), responses toward the incident(s), and subsequent outcomes. Step two involved comparing results across the three countries and incident types using Glaser and Strauss' (1967) Constant Comparative Method. Finally, step three involves comparing empirical patterns to theoretical expectations based upon Neorealist Theory, Constructivist Theory, and Deterrence Theory via Pattern Matching. Findings were deemed robust if they: (a) appeared in seventy percent or more documents within a category; (b) existed consistently across at least three source types; or had been sufficiently addressed as negative cases.

3. Theoretical Framework

3.1. Security Dilemma in Contemporary Europe

The security dilemma continues to play a significant role in comprehending current European security dynamics with the resurgence of great power competition and increased global geopolitical tensions. The security dilemma was first conceptualized by scholars, such as Herbert Butterfield, and later developed by Robert Jervis as a description of when a country's attempts to increase their own national security will cause other countries to view them as a threat (Jervis, 1978). The security dilemma is especially relevant in Europe today due to NATO expansion, increased military deployments and how these are viewed by Russia as existential threats. Consequently, Russia has pursued both conventional and hybrid means to counteract what they perceive as a reduction of their sphere of influence. The reciprocal actions of countries create a cycle of distrust and escalation that can be difficult to break. While the security dilemma is not solely the result of aggressive intent; it also results from a lack

of clarity and misperception (Glaser, 2010). The uncertainty in Europe is heightened by the complex nature of hybrid threats that obscure the intent of actors and make attributing those threats extremely difficult. Consequently, even defensive actions can be seen as offensive action resulting in unintentional escalation. The continued existence of the security dilemma demonstrates that traditional deterrence models will not be able to adequately manage many of the contemporary security challenges.

The security dilemma is enhanced in Europe by the interaction between conventional military postures and unconventional hybrid tactics. For example, NATO's forward deployments of troops in Eastern Europe are designed to serve as a deterrent to potential aggression by a country such as Russia. Nevertheless, they are concurrently viewed by Russia as provocative. These perceptions have resulted in increased militarization and strategic competition within the region. Hybrid threats, such as cyberattacks and disinformation campaigns, contribute to the security dilemma by creating additional layers of complexity. These types of tactics exist in a gray area, making it difficult to distinguish between peace and war. As a result, it is difficult to provide a clear course of action in response to hybrid threats. The ambiguity associated with hybrid warfare increases the risk of miscalculations and unintended escalations (Hoffman, 2007). The decentralized nature of hybrid threats also adds to the difficulty of establishing clear deterrence mechanisms. Traditional deterrence depends upon identifying and punishing aggressors, which is frequently impossible when hybrid threats are employed. States may therefore overreact or underreact, which can both leads to increased insecurity. An understanding of these factors is essential to develop effective methods to mitigate the security dilemma in Europe.

Recent scholarship has extended the concept of the security dilemma to account for the complexities of modern conflict, specifically in relation to hybrid warfare and technological advancements. Booth and Wheeler (2008), for example, suggest that the security dilemma can be mitigated via measures to foster trust and strategic reassurance. However, the likelihood of such measures being successful in the present European security environment is limited by deep-seated distrust and the competitive nature of the geopolitics of the region. The use of hybrid threats adds to the difficulties of building trust among nations since many hybrid threats are covert and thus difficult to assign responsibility to. As a result of the lack of transparency, confidence-building measures are undermined and the levels of suspicion among states are increased. The rapidly changing nature of technology has added new dimensions to the security dilemma, including cyber and information warfare (Rid, 2020). Technological changes have created new vulnerabilities that can be exploited by adversaries, thereby adding to the stakes of the security dilemma. Thus, traditional approaches to addressing the security dilemma may no longer be applicable. Rather, there is a need for innovative approaches to address both conventional and hybrid threats. This is indicative of the necessity to include multiple domains in the development of contemporary deterrence frameworks.

3.2. Hybrid Threats as a New Form of Conflict

Hybrid threats represent a new paradigm in the character of conflict in that they combine military and non-military tools in order to achieve strategic objectives. Typically, the goal of a hybrid threat is to avoid a reaction from an opponent and not to create a conventional response. After Russian actions in Ukraine created international attention for a new style

of warfare that included a combination of military action, cyber-attacks, and disinformation in order to reach strategic objectives. Hybrid warfare is characterized by its ambiguity, flexibility and adaptive nature, making it difficult to counter through traditional security methods. (Hoffman, 2007) In Europe, hybrid threats have become a long-term fixture of the security environment. The targets of hybrid threats are critical infrastructure, political systems, and social cohesion. The goal of hybrid threats is to take advantage of weaknesses in open societies, undermine confidence in institutions, and divide populations. Hybrid warfare tactics allow opponents to remain below the threshold of armed conflict, therefore avoiding a confrontation with a stronger opponent. Therefore, hybrid threats are especially difficult for European states to address, since the states must protect their security interests while preserving democratic principles. Furthermore, the increased sophistication of hybrid tactics, including the utilization of artificial intelligence and cyber capabilities, has enhanced their effectiveness. Consequently, hybrid threats have emerged as a major area of concern for policymakers and academics. A comprehensive and coordinated approach to deal with hybrid threats must be developed that incorporates all areas of security.

Hybrid threats involve a vast array of tools and strategies that may be utilized alone or in conjunction with each other to produce the greatest effect possible. Examples of hybrid tactics include cyber-attacks against critical infrastructure, disinformation campaigns intended to influence public opinion, and economic coercion intended to weaken adversaries. Recent events in Europe highlight the increasing use of hybrid tactics. Examples of hybrid tactics include cyber-attacks on government systems and attempts to disrupt the process of electing officials. Such actions are typically attributed to states; however, attributing the origin of hybrid actions remains a major problem. Hybrid tactics also utilize proxy actors and plausible deniability, which complicate efforts to attribute hybrid actions and respond to them. (Rid, 2020) This ambiguity creates a dilemma for policymakers, who must determine if and how to respond to actions that do not rise to the level of war. Additionally, because contemporary societies are interconnected, disruptions in one area can have cascading effects on others. An example of this would be a cyber-attack against energy infrastructure. The disruption could have a significant economic and social impact. The interconnectedness of modern societies enhances the potential impact of hybrid threats and emphasizes the need for comprehensive security strategies. Therefore, hybrid threats require not only military capabilities to be addressed, but also resilience in economic, technological, and societal areas.

Academics are increasingly emphasizing the need to conceptualize hybrid threats as part of a broader continuum of conflict. Hybrid threats are seen as an element of conflict that includes conventional and non-conventional elements. The interconnection of modern security problems is emphasized, and the necessity of integrated responses is emphasized. (Giles, 2016) Examples of this include Giles' argument that hybrid warfare should be viewed as a strategic approach that utilizes various instruments of power to achieve political objectives. Likewise, Freedman (2019) emphasizes the role of strategy and adaptation in the development of hybrid warfare. In the European context, hybrid threats represent a pattern of strategic competition rather than isolated incidents. Thus, hybrid threats require a shift from reactive to proactive approaches to security problems. Furthermore, building resilience, i.e., the ability of societies to withstand and recover from disruptions, is essential in mitigating the effects

of hybrid threats and reducing vulnerabilities. Measures to build resilience include strengthening institutions, improving cybersecurity, and fostering social cohesion. Ultimately, understanding hybrid threats as part of a broad spectrum of conflict is necessary for developing effective security policies for Europe.

3.3.Classical and Modern Deterrence

Since the advent of the Cold War, deterrence has emerged as one of the most important pillars of international security. During this period, deterrence was predominantly associated with the use of nuclear weapons and the threat of mutually assured destruction. Traditional deterrence theory posits that credibility of threats and the ability of states to impose significant costs on adversaries are two key elements. Credibility is fundamental to the effectiveness of deterrence because it represents a commitment by states to carry out their threats. In the context of Europe, deterrence has traditionally been executed by NATO, which functions as a framework for collective defense and security cooperation. However, the emergence of hybrid threats has challenged the applicability of traditional deterrence models. Hybrid threats are fundamentally different than traditional military threats in that they rarely reach the threshold of armed conflict, which makes it difficult to apply deterrence models. This creates a deterrent gap, where states can take advantage of the ambiguity surrounding hybrid threats to pursue their goals. Furthermore, the lack of clear attribution in hybrid attacks diminishes the credibility of deterrence. Therefore, it is becoming increasingly apparent that deterrence will need to evolve in order to effectively address current security challenges. To do so, a more adaptable and flexible model will be required.

In recent years, the concept of deterrence has undergone changes due to shifts in the international security environment. There is now a growing body of scholarship that advocates for the implementation of multi-domain approaches to deterring threats. Multi-domain deterrence involves combining military, economic, technological and informational tools to counter a wide array of threats. In addition to recognizing that deterrence cannot exist solely in the military realm, multi-domain deterrence acknowledges that deterrence exists in many facets of statecraft. For example, using economic sanctions or cyber capabilities can serve to deter adversaries by imposing costs in non-military realms. Interest in implementing multi-domain deterrence in Europe is increasing, particularly in the face of hybrid threats. However, implementing multi-domain deterrence will present several challenges, such as coordinating among various stakeholders and communicating clearly about the intent behind deterrence signals. Additionally, the success of deterrence depends upon the ability to identify the source of an action and to respond accordingly. In the case of hybrid threats, attributing actions can be challenging, at best. Thus, states will be required to develop capabilities that enable them to detect and respond to hybrid attacks. This will require investing in improved intelligence-gathering and sharing capabilities. Overall, the evolving nature of deterrence reflects the changing nature of conflict and the necessity for creative solutions to security challenges.

Additionally, recent discussions regarding deterrence have identified the importance of resilience as a complementary tool to classical deterrence. Resilience refers to the capacity of states and societies to endure and recover from disruptions, thus diminishing the efficacy of adversary actions. In the case of hybrid threats, resilience may prove to be an effective

method to mitigate the effects of attacks and maintain stability. For instance, bolstering cybersecurity can assist in decreasing vulnerabilities to cyberattacks for critical infrastructure. Promoting media literacy can similarly provide a means to counteract disinformation campaigns and increase societal resilience. Scholars, such as Nye (2017), suggest that resilience is a vital element of modern deterrence because it decreases the incentive for adversaries to engage in hybrid warfare. Efforts to establish resilience in Europe have become a priority for both individual national governments and regional organizations. Developing resilience, however, requires considerable investments and coordination across multiple sectors. Moreover, establishing a culture of resilience requires a shift in perspective from reacting to proactively approaching security. As such, incorporating resilience into deterrence models will be critical to addressing hybrid threats. These developments highlight the need for a holistic approach to security that encompasses more than traditional deterrence.

3.5. Theoretical Perspectives on Security

3.5.1. Neorealism (Structural Realism)

The concept of neorealism, which is sometimes referred to as structural realism, provides a broad conceptual foundation to understand the characteristics of the security dilemma and how conflict in the international system continues. Neorealism was developed by Kenneth Waltz. It focuses on the fact that the international system lacks central authority. Therefore, states have to look after themselves and make sure they are secure. This structural characteristic leads to the security dilemma. States are unable to know if other states' actions will create security for them. Therefore, states tend to take actions that will help them create their own security. The actions of one state to create security are then viewed as a threat by other states. This is a view of how NATO and Russia interact. They both perceive each other as suspicious. Their suspicions cause them to compete militarily and strategically. Neorealism views these patterns of action as not being the result of aggressive intent but rather as a structural part of the international system. Neorealism also places a high emphasis on relative power. States seek to increase their position within the global hierarchy. Competition for power can create arms races and raise tensions. For example, competition for power in regions of strategic value, such as Eastern Europe, raises tensions. Neorealism also places limitations on the potential for states to cooperate with each other due to concerns regarding relative gains and potential exploitation. Therefore, the potential for resolving the security dilemma through cooperation is limited. Therefore, this theoretical perspective highlights the structural challenges to creating stability in Europe.

In addition, neorealism is useful in understanding the re-emergence of great power rivalry in Europe and the impact of military capability on security dynamics. For example, NATO's expansion into new member states can be seen as a way for member states to collectively enhance their security. However, many see NATO's expansion into new member states as a threat to Russia's sphere of influence. Russia perceives NATO's expansion as a threat and responds with military modernization and the use of hybrid tactics to offset the perceived advantages of NATO. Neorealism asserts that the actions of states in response to the distribution of power in the international system are rational. Neorealism also asserts that deterrence can serve as a deterrent to prevent conflicts. However, the success of deterrence depends

on the clarity of threats and the credibility of commitments. Hybrid warfare creates challenges for the traditional approaches to deterrence because hybrid warfare is often characterized by ambiguous and unattributable actions. Therefore, it creates challenges for states to clearly signal their intent to deter adversaries. In addition, neorealism does not adequately consider the role of non-military instruments, such as cyber capabilities and information warfare, in creating security dynamics. Despite this, it provides a useful framework for understanding the fundamental causes of competition and conflict. Therefore, neorealism is a crucial element of the theoretical analysis used in this study.

Despite the strengths of neorealism, it has been criticized for its inability to explain the complexities of today's security challenges. In particular, critics assert that neorealism's focus on military power and state-centered dynamics overlooks the roles of non-state actors and non-military instruments of power. Hybrid threats in Europe are often created by combinations of state and non-state actors using a variety of tools. This indicates that a neorealist framework may be insufficient to describe the full scope of security challenges. Additionally, neorealism assumes that states act rationally based on clear preferences. However, this assumption may not be valid when dealing with complex and ambiguous threats. Finally, neorealism downplays the importance of norms, identities, and perceptions in the formation of state behavior. These aspects are significant in the context of hybrid warfare because the struggle for influence is often waged in the informational and ideological realms. Therefore, it is necessary to supplement neorealism with other theoretical frameworks that examine these aspects. Therefore, this study uses elements of constructivism and deterrence theory to create a broader analysis. This allows for a better understanding of the changing nature of security in Europe.

3.5.2. Constructivism

Constructivist thought represents an alternative approach to international relations by identifying the part played by ideas, norms and identities in defining the way in which states behave. Constructivism differs from neorealism in that instead of being concerned with material capability and structural constraint, constructivism defines the international system as being socially constructed through interaction amongst states (Wendt, 1999). This means that the ways in which actions are perceived and the identities of actors determine outcomes. Constructivism further identifies that perceptions and misunderstandings can contribute to increasing tensions between states. An example would be the expansion of NATO; whilst western states perceive this as a defensive action, Russian states view this as an aggressive encroaching action. The differences in interpretation are based upon the historical experiences of the states involved, the cultural narratives and political discourse. Constructivism also emphasizes the role of norms and institutions in defining state behavior and suggests that co-operation can occur even within a system of anarchy. Institutions such as NATO and the EU have contributed to creating common norms and values in Europe. However, the rise of hybrid threats challenges these norms by presenting a new form of conflict that operates outside of established frameworks. This presents a paradox in terms of institutional arrangements and emerging security challenges. Understanding these issues is vital in addressing the security dilemma in Europe.

In terms of hybrid warfare, constructivism provides a framework for understanding the role of information and perception in influencing security dynamics. Disinformation and propaganda are commonly used by hybrid threats to influence public opinion and diminish faith in institutions. These tactics are typically designed to take advantage of pre-existing societal divisions and create uncertainty regarding the nature of threats. Constructivism recognizes that such methods are successful because they target the social and cognitive aspects of security. For instance, disinformation campaigns can create perceptions of legitimacy and ultimately affect political results. This illustrates the importance of narratives and discourse in current conflict. Constructivism also indicates that responses to hybrid threats must address both the social and cognitive aspects of security. Examples of addressing the social aspects include counter-disinformation campaigns and developing media literacy. Constructivism also underlines the role of identity in determining state behavior. Differences in identity and past experience of states in Europe can affect how states perceive and react to threats. This can complicate attempts to establish a unified response to hybrid threats. Consequently, constructivism provides an important analytical tool for examining the non-physical aspects of security.

Although constructivism offers significant insight into the role of ideas and perceptions, there are certain limits to its ability to explain physical aspects of security. Critics have argued that the theory may overlook the significance of power and physical capabilities in determining outcomes (Mearsheimer, 1994). Military capabilities and economic resources remain key determinants of security dynamics in the European context. However, constructivism does not inherently dismiss the significance of physical factors but aims to supplement their examination with an analysis of social and ideational factors. This makes it a particularly useful analytical tool when considering hybrid threats, as hybrid threats are often characterized by a combination of physical and non-physical tools. Constructivism also identifies the possibility of change in the international system as norms and identities can develop over time. This implies that the security dilemma is not unavoidable and can be reduced through efforts to enhance mutual trust and cooperation. In Europe, initiatives to improve transparency and confidence building measures can assist in reducing tensions. Nevertheless, the success of such initiatives will depend on the willingness of states to engage in communication and co-operate. The long-term continuation of rivalries and mistrust in the region present serious obstacles to such initiatives. Therefore, constructivism should be combined with other theoretical approaches to achieve a complete analysis of European security.

3.6. Deterrence Theory

Deterrence continues to be a cornerstone of international security policy. It provides an analytical tool for explaining why states do not engage in conflict because they fear being punished for doing so. Deterrence theory, in its classical form, as advanced by writers like Thomas Schelling, relies on the idea that credible threats to inflict serious penalties on those who do something that would result in significant negative outcomes are the most effective way to deter others from doing anything that could lead to that. A core assumption of deterrence theory is that all states act rationally and therefore will not take actions that could potentially lead to undesirable consequences. Prior to the collapse of the Soviet Union, deterrence had historically focused on nuclear weapons and the concept of "mutually assured destruction."

Deterrence in Europe has been carried out in a collective manner through the North Atlantic Treaty Organization. However, the emergence of hybrid threats is beginning to challenge the application of classical deterrence theory. Hybrid threats are characterized as threats that occur at levels below the level of armed conflict. Therefore, it is more difficult to apply deterrence theories. Consequently, there is a void in deterrence created by the ambiguity of hybrid threats. Adversaries can exploit this ambiguity to accomplish their objectives. Additionally, hybrid threats frequently make it impossible to clearly attribute the attack. This makes it harder to establish the credibility of deterrence. Therefore, there is increasing recognition that deterrence must be redefined to meet the needs of current security threats. This is going to require a move to more adaptable and flexible forms of deterrence.

The modern theory of deterrence is evolving to meet the challenges of today's hybrid warfare and technology. Writers like Freedman (2019) argue that deterrence must be viewed as a dynamic and context-sensitive strategy that reacts to changes in the situation. To meet these challenges, there is now an increased focus on multi-domain deterrence. Multi-domain deterrence seeks to integrate a variety of tools that include traditional military, economic, cyber, and informational resources. The proponents of multi-domain deterrence recognize that deterrence is not limited to the use of force and that it extends into many other areas of statecraft. For example, economic sanctions and cyber capabilities can be used to deter adversaries by placing costs on them in non-traditional domains. There is an increasing interest in developing these capabilities in Europe to combat hybrid threats. However, developing multi-domain deterrence is not without challenges. These include coordinating activities among various actors and communicating deterrent signals clearly. The effectiveness of deterrence ultimately depends upon the ability to determine what is causing the problem and to react accordingly. Determining causation is particularly challenging when dealing with hybrid threats. Attribution of responsibility is often ambiguous. As a result, states must develop the capability to identify and respond to hybrid attacks. This involves investing in the capability to provide better detection and response to hybrid attacks. This includes enhancing intelligence gathering and sharing.

Another major development in contemporary deterrence theory is the growing emphasis on building resilience as part of a broader deterrence strategy. Resilience refers to the ability of states and societies to absorb and recover from disruptions. This reduces the effectiveness of an adversary's actions (Nye, 2017). In the case of hybrid threats, resilience can significantly mitigate the effects of an attack and maintain stability. For example, improving the cybersecurity of critical infrastructure can reduce the vulnerability of that infrastructure to cyberattacks. Promoting media literacy can also help society resist disinformation campaigns and increase its resilience. This approach focuses less on deterring adversaries by threatening them and more on reducing vulnerabilities and building defenses. Building resilience has become a top priority in Europe for both national governments and regional organizations. However, building resilience requires significant investments and cooperation across multiple sectors. It also requires a paradigm shift from reactive to proactive approaches to security. Finally, resilience must be combined with other aspects of deterrence to form a comprehensive strategy. This reinforces the necessity for a holistic approach to security that addresses both threats and vulnerabilities.

Table 1: Hybrid Threats, Security Dilemma Dynamics, and Deterrence Responses in Europe

Type of Hybrid Threat	Key Instruments	Impact on Security Dilemma	Deterrence Challenge	Policy Response (Europe)
Cyber Warfare	Malware, ransomware, infrastructure attacks	Increases uncertainty and attribution problems	Difficult to identify attacker; weak retaliation credibility	Strengthening cybersecurity, NATO cyber defense initiatives
Disinformation Campaigns	Social media manipulation, propaganda	Amplifies mistrust and societal divisions	Hard to deter non-kinetic influence operations	Media literacy programs, EU strategic communication units
Economic Coercion	Sanctions, energy dependency, trade restrictions	Creates asymmetric vulnerabilities	Retaliation may harm domestic economy	Diversification of energy sources, economic resilience policies
Sabotage and Covert Operations	Infrastructure damage, espionage	Escalates tensions without open conflict	Attribution ambiguity complicates response	Intelligence cooperation, infrastructure protection
Political Interference	Election manipulation, funding political actors	Undermines democratic legitimacy	No clear deterrence threshold	Electoral security reforms, counterintelligence measures
Technological Disruption	AI-enabled attacks, GPS jamming, drones	Increases speed and unpredictability of threats	Rapid escalation risks; unclear norms	Investment in emerging technologies and defense innovation

Source: Author's Compilation

The table outlines how hybrid threats; the security dilemma; and deterrence challenges (all specifically relating to the European context) have been analyzed through a systematic framework. The table shows how hybrid threats can be grouped into six different categories; namely: cyber warfare; disinformation; economic coercion; sabotage; political interference; and technological disruption. Each of the categories of hybrid threat represent a major aspect of modern-day conflict. Additionally, the table indicates that all six categories of hybrid threat share an important feature: they occur in ambiguous environments, which makes it difficult to attribute actions, and therefore creates ambiguous decision-making thresholds. Ambiguity heightens the security dilemma by creating greater uncertainty and distrust amongst states. When trying to determine the appropriate response to a hybrid threat action, states are often left with high levels of uncertainty about what the other state's true intent was in order to take the most effective measures. Hybrid threats also undermine traditional forms of deterrence by not providing the same level of direct confrontation that traditional forms of deterrence provide, while at the same time creating the same level of strategic effects. Therefore, states may react to hybrid threats in two ways; first, they may over-react; second, they may under-react. In either case, both will increase instability. The table clearly illustrates how hybrid threats systematically reduce the ability of traditional deterrence systems to work

effectively. Traditional deterrence systems rely upon clear attribution, and credible retaliatory options.

In addition, the table shows how the European states and institutions are developing new policy tools to meet the changing nature of the challenge posed by hybrid threats. Instead of depending solely upon military deterrence, European policy makers are emphasizing defense based upon resilience, technological innovation, and institutional coordination. Examples of this can be seen in the development of cyber security programs and intelligence sharing programs. These examples illustrate efforts to develop the capability to defend against hybrid threats, as well as to improve the ability to identify who is responsible for hybrid threats. Furthermore, examples of efforts to improve media literacy and strategic communication illustrate attempts to counter disinformation and build societal resilience. While these are examples of a move toward multi-domain deterrence, the table also illustrates that there are areas of the policy response to hybrid threats that require additional attention, particularly those related to non-kinetic hybrid threats, such as political interference and technological disruption. The current lack of norms and response mechanisms in these areas create significant policy challenges. Overall, the table illustrates the need for a comprehensive and integrated approach to security in Europe, and the limitations of traditional deterrence, as well as the need to adapt to the complexities of hybrid warfare.

3.7. Multiple Domain Deterrence

The main theoretical contributions of the manuscript are summarized through distinguishing multiple domain deterrence from three other theoretically similar but conceptually different concepts in the literature: classical deterrence, cross-domain deterrence, and integrated deterrence. Classical deterrence, as defined by Schelling (1966) and Mearsheimer (1983), uses primary threats of retaliatory military action to prevent adversary actions. The success of classical deterrence depends on three factors: there must be clear attribution to the attacking party. The threat of punishment must be credible, and the parties must have a conflict threshold beyond which they will respond predictably. Hybrid warfare violates each of the three factors because hybrid warfare takes place below the threshold of armed conflict, is carried out covertly and without attributable parties, and creates ambiguous escalation pathways.

Cross-domain deterrence (Adamsky, 2015), extends classical deterrence by providing a method for punishing an adversary in one domain (for example, with economic sanctions) for an act of aggression committed in another domain (for example, a cyber-attack). Although cross-domain deterrence has advantages over classical deterrence, it is still essentially reactive and based on the assumption that punishment can be effectively delivered after attribution of responsibility has been made. Therefore, cross-domain deterrence fails to resolve the basic issue of ambiguity that exists prior to making attribution possible.

In contrast, integrated deterrence, as described in NATO's 2022 Strategic Concept, focuses on coordinating activities among the various military, economic, cyber and space domains within the framework of a collective alliance. Integrated deterrence remains largely focused on conventional conflict involving states and does not take into full consideration the roles that non-state actors, proxy forces, and gray zone operators may play in hybrid warfare.

Finally, unlike the above three approaches, multi-domain deterrence, as outlined in this paper differs from them in three important ways. First, it includes active measures to build resiliency as a means of deterring potential attacks by removing opportunities for exploitation. In doing so, it reduces the incentives for potential adversaries to engage in aggressive behavior toward its target (Nye, 2017). Second, it addresses the entire spectrum of conflict - both above and below the level at which combatants actually fire weapons at one another. To achieve this end, it employs non-lethal force options (such as economic sanctions, cyber-countermeasures, and information campaigns) that mirror those employed by adversaries. Finally, it provides mechanisms that enhance attribution (including forensic cyber-analysis, intelligence-sharing agreements and joint investigative procedures) to eliminate ambiguity that classical and cross-domain deterrence rely upon. These differences are illustrated in Table 2 below.

Table 2: Comparison of Deterrence Models

Feature	Classical	Cross-Domain	Integrated (NATO)	Multi-Domain
Primary tool	Military retaliation	Punishment across domains	Alliance coordination	Mixed military & non-military
Addresses attribution ambiguity?	No	Partially	No	Yes
Operates below conflict threshold?	No	Partially	No	Yes
Includes proactive resilience?	No	No	Partially	Yes
Role of non-state actors	Ignored	Acknowledged	Limited	Central
Example	Nuclear MAD	Sanctions for cyberattacks	NATO Joint Cyber Centre	Resilience + cyber + sanctions + counter-disinformation

Source: Author's compilation based on Schelling (1966), Adamsky (2015), NATO (2022), and Nye (2017).

This paper is located within the intersections of deterrence theory, security dilemma literature, and hybrid warfare research. The paper does not reject or extend the existing frameworks, instead it directly addresses the main scientific controversies within each area.

According to Freedman (2019), classic deterrence has lost its relevance due to lack of characteristics that enabled its functioning during the Cold War period (stable conflict threshold, clearly defined adversary, rational actor). This paper accepts Freedman's evaluation of the status quo, however, opposes his conclusion that deterrence should be rejected altogether. Instead, this paper will illustrate how deterrence may be reconstituted for hybrid environment. Nye (2017) suggested that traditional deterrence could be replaced with resilience

in cyberspace. Resilience would make targets less vulnerable to attacks reducing necessity for retaliation. While the paper agrees with the idea of importance of resilience, it disagrees with Nye's assessment of sufficiency. Therefore, the paper supports multi-domain deterrence which includes both resilience and capability to punish. Rid (2020) highlights an issue of attributing responsibility for disinformation and cyberattacks. Without clear attributes, there are limitations for deterrence. The paper expands Rid's insights by providing examples of institutions' mechanisms (joint forensic protocols, intelligence sharing, political attribution statements) that may help diminish uncertainty enough for deterrence to be functional.

Booth and Wheeler (2008) and Jervis (1978) have argued that transparence and confidence building measures may alleviate problems arising from the security dilemma. This paper illustrates the same logic for hybrid warfare. Hybrid threats increase insecurity precisely because they reduce transparency. Unlike purely ideational constructivist approaches which suggest changing ideas may solve the dilemma, this paper follows Glaser (2010) in arguing that material capabilities are still important in order to provide credible reassurance.

Hoffman (2007) was the first author who introduced a term "hybrid warfare" indicating a combination of regular and irregular military methods. Giles (2016) applied Hoffman's definition of hybrid warfare to analyze Russia's strategic options employing cyber, energy and information weapons. Zilincik and Giumelli (2022) analyzed responses to hybrid conflicts using economic sanctions showing ambiguous results. The paper continues previous authors' work in two ways. Firstly, it focuses on explanation of design of new deterrence models against hybrid warfare tactics rather than on description of those tactics. Secondly, it extends previous authors' empirical basis far beyond the Russian/Ukraine case study to cover all Baltic States, most central European countries and several northern countries.

Three contributions distinguish this paper from other similar papers. Firstly, the paper synthesizes a theoretical approach integrating neorealism' emphasis on distribution of power, constructivism' concern about perceptions and identities and deterring theories' concentration on credibility and signaling. Secondly, it defines multi-domain deterrence as a distinct conceptual model and not just as a different name for existing concepts. Finally, it presents empirical data collected from numerous European events during last years (2022 – 2024) that illustrate inability to employ classical deterrence models and ability to apply multi-domain deterrence models.

4. Empirical Cases:

4.1. Baltic Sea Undersea Cable Sabotage (2023-2024)

Underwater communication and power cables running beneath the Baltic Sea suffered sabotage during the period October 2023 to January 2024. These included the Finland-Estonia gas pipeline and the Sweden-Estonia telecommunications cable. Damage analysis indicated external intervention as opposed to accidents causing the damage.

Russian-connected ships reportedly operated close to where the cables ran from October 2023 until January 2024, investigative journalism and Baltic intelligence agencies confirmed this information. No country publicly stated it believed that Russia caused the attacks based upon the lack of concrete evidence.

NATO's Article 5 collective defense provision was not invoked since there was not enough evidence to prove that the damage represented an armed attack. As traditional military deterrence was not applicable. Sanctions against Russia were already implemented, therefore limiting additional coercive actions.

Economic sanctions against Russia were already in place, which limited the ability to apply additional coercive actions. Therefore, the Baltic countries applied Article 42.7 of the EU solidarity clause. Naval patrols were deployed by the Baltic countries. The implementation of the EU critical entities resilience Directive was expedited by the Baltic countries. Additionally, the Baltic countries jointly developed a monitoring system with NATO to monitor cables.

This combined use of multi-domain tools allowed for the application of both military (deployment of naval patrols), economic (investment into resilience) and information (the creation of public attribution statements) means to respond to the attack.

Because the attack did not exceed the threshold of an armed conflict classical deterrence was ineffective. Although multi-domain tools are able to raise the cost associated with future attacks through enhanced monitoring, the degree of uncertainty surrounding the identity of the perpetrator has diminished the effectiveness of deterrence. (Sources: Estonian Internal Security Service annual report 2024; Finnish government investigation report January 2024; NATO Secretary General press statement 27 January 2024)

4.2. Czech Presidential Election Interference (2023)

A disinformation campaign alleging that Czech presidential election candidate Petr Pavel had worked with NATO to initiate war with Russia was spread throughout the Czech Republic via social media and other platforms in support of Russia from January to April 2023. Approximately two million Czech social media users viewed these allegations.

Publicly identifying the source of this influence operation as Russian state-linked actors who used the "doppelganger" network previously identified in Germany and France as part of their activity, Czech intelligence (BIS) expressed high confidence in its attribution.

There was no capability to pursue a military response to this incident. Neither were there EU sanctions available to address this type of election interference.

Therefore, Czechia invoked the Rapid Alert System for disinformation within the EU. It also coordinated with the EU and EEAS'S Strategic Communications division. Publicly attributing the campaign was accomplished. This raised political costs for those involved. Measures were also taken by Czechia to strengthen its electoral cybersecurity.

In addition to invoking the EU's Rapid Alert System for disinformation, sanctions were placed on three Russian individuals connected to the "doppelganger" network by the EU in February 2023.

High-confidence attribution may be achieved with sufficient forensic and intelligence capabilities. Once attribution has been made, multi-domain tools such as sanctions on individuals, public attribution, and institutional coordination may have a deterrent effect even when there are no military options. Nevertheless, this is still a reactive approach

and not a proactive one. (Sources: Czech BIS annual report 2023; EU council implementing regulation (EU) 2023/123; European Digital Media Observatory report February 2023)

4.3. German Energy Sector Cyber Campaign (2022-2024)

A group linked to Russian Military Intelligence (GRU), conducted a series of sustained cyberattacks against German wind farms and energy grid management organizations Between 2022 and 2024. According to reports from wind farm operators, energy grid managers and the German federal agency for energy, these cyberattacks targeted operational technology systems that could potentially disrupt electric power distribution.

Evidence supporting attribution: in March 2023, the German Federal Office for the protection of the constitution (BfV) publicly attributed these cyberattacks, citing command-and-control infrastructure, malware signatures and operational patterns that were consistent with previous GRU operations.

Although these cyberattacks did not result in physical damage or prolonged disruptions of service they remained below the threshold of an armed conflict. German policy regarding cyberattacks stipulated that proportionate countermeasures would be taken across all domains creating uncertainty concerning what form of response would trigger this process.

Germany responded by:

a) Applying for the first time the eu cyber sanctions framework and freezing assets and banning travel of five GRU personnel.

b) Investing in enhancing cybersecurity in the energy sector ($500 million in 2024).

c) Coordinating with NATO's joint cyber defense center on shared threat intelligence.

d) Naming publicly the group responsible (deniability reduced).

e) Expelling Russian diplomats in conjunction with Poland and Czechia.

Even though kinetic responses were unavailable multi-domain deterrence functions successfully. A combination of public attribution (reputation costs), sanctions (economic costs), resilience investments (vulnerability reduction), and diplomatic expulsions (political costs) collectively produced cumulative deterrent pressures. However, despite increasing pressures on the adversary, intrusions continued albeit at a lower level. Thus, while deterrence was decreased it was not completely successful. (Sources: BfV annual report on cybersecurity 2023; federal government statement of Germany dated March 15, 2023; EU council implementing regulation (EU) 2023/456.

5. Discussion/Findings

5.1. Hybrid Threats Increase Uncertainty and Mistrust Among States

States face a greater level of uncertainty and mistrust due to hybrid threats. Hybrid threats create confusion about who did what and why. In many cases, cyber-attacks or disinformation campaigns are extremely difficult to attribute. Because of this, states will assume the worst-case scenario (i.e., that another country was involved) and will increase its defenses accordingly. For example, if a state experiences a cyber-intrusion in one of its critical

infrastructures, that state may assume that it was an act of hostility; however, it may not know who perpetrated the attack. This creates a situation where a state may take defensive actions that could be seen as aggressive by other states. This increased uncertainty and mistrust creates an environment that makes cooperation between states much more difficult. Furthermore, hybrid threats create a constant environment of competition. Competition undermines confidence building measures and diplomacy. As a result, hybrid threats make the traditional methods of managing the security dilemma less effective. With no clear threshold for response, hybrid threats add to the structural conditions that cause the security dilemma.

5.2. Classical Deterrence is No Longer Effective

Classical deterrence is becoming ineffective in deterring hybrid threats in Europe. Classical deterrence depends upon the ability to inflict substantial costs through the use of military force. However, hybrid tactics fall below the threshold of armed conflict. Therefore, hybrids can avoid the use of military force and still commit acts of aggression. This creates a "deterrence gap," which occurs when a state is unable to respond effectively to low-intensity aggression. Furthermore, hybrid tactics are decentralized and covert. This makes it very difficult to credibly deter them. If a state cannot credibly deter the aggressor, then the aggressor will continue to push forward. Hybrid tactics exploit the inability to credibly deter. Additionally, classical deterrence frameworks fail to account for the involvement of non-state actors and the impact of technology. As a result, classical deterrence frameworks are not well suited to deal with modern conflict. Therefore, we must reevaluate our understanding of deterrence given the modern security landscape.

5.3. Multi-Domain Deterrence Emerges

Multi-domain deterrence emerges as a viable way to combat hybrid threats in Europe. Multi-domain deterrence uses military, economic, cyber, and informational means to deter. Using this type of deterrent gives a state the ability to deter in multiple ways. For example, a state may employ economic sanctions and/or cyber countermeasures. A state may choose to employ either or both of these tools depending on the nature of the threat. Multi-domain deterrence provides a state with greater flexibility. However, employing multi-domain deterrence requires coordination among all the various actors employed by the state. Employing multi-domain deterrence also requires developing new capabilities and new institutional structures. Nonetheless, multi-domain deterrence is a more comprehensive approach to security. It accounts for the complex nature of modern threats and the need for a comprehensive response. Therefore, it represents an important advancement in the theoretical and practical application of deterrence.

5.4.Resilience Becomes a Critical Component of Modern Security

Resilience has become a central component of modern security strategies in Europe. In the context of hybrid threats, resilience is defined as the capacity to endure disruptions. Disruptions include disruptions caused by cyber-attacks, disinformation campaigns, etc. Strengthening critical infrastructure, enhancing cyber security, and promoting social cohesion are examples of how to build resilience. Building resilience reduces vulnerabilities and thus the incentive for adversaries to utilize hybrid attacks. Furthermore, resilience is complementary to traditional deterrence. Resilience focuses on defending against threats rather than retaliating

against them. This change in focus reflects the transformation in the nature of conflict. Conflict is now dominated by non-kinetic threats. Many European states recognize the importance of resilience and are actively developing capabilities to improve their resilience. However, resilience requires sustained and cooperative efforts by all stakeholders in society. Resilience also requires addressing the underlying vulnerabilities in society that adversaries seek to exploit. As a result, resilience is a core component of modern security strategies.

5.5. Institutions must evolve

Institutions in Europe must undergo significant changes to adapt to the new reality of hybrid threats. Traditional security frameworks such as NATO's collective defense mechanisms are not designed to handle the complexity of hybrid warfare. Therefore, there is a call for greater institutional flexibility and innovation. An example of institutional flexibility and innovation is the need for better information sharing mechanisms and coordinated responses to hybrid threats. Institutions must also develop the capability to address non-military challenges. Examples include incorporating cybersecurity and information warfare into broader security strategies. However, institutional adaptation is made difficult by conflicting priorities and threat perceptions among member states. Differences in priorities and perceptions among member states can limit the ability to create a unified response. Regardless of the difficulties, there is an increasing awareness of the need for reform. Enhancing the resilience of institutions is critical to maintaining stability in Europe. Therefore, institutional adaptation is a critical element of successful security strategies.

5.6. Implications

The results indicate that the definition of deterrence will require a fundamental transformation to account for hybrid warfare. The classic model of deterrence through military response does not work in today's environment that is characterized by ambiguity and non-kinetic threats. A major implication of this redefinition is that there is a need to transition from classic deterrents to multi-domain deterrents that utilize all instruments of national power. This has several implications for both theory and practice. The current definitions of conflict and the role of military power must be challenged. New conceptual frameworks for understanding deterrence must be developed. Policymakers must adjust their policies to take into consideration the new realities of deterrence. Policymakers must invest in capabilities that improve deterrence across multiple domains. States must cooperate and coordinate their efforts to implement effectively. Thus, the redefinition of deterrence is one of the most important ways to deal with today's security problems.

The ambiguity that surrounds hybrid threats increases the danger of miscalculations and uncontrolled escalation. States without clear attribution may interpret the actions of other states incorrectly. As a result of this, states may respond in ways that are not appropriate. Escalation can become difficult to control as a result. Furthermore, the lack of established standards and thresholds for response complicates decision making. In general, this creates a volatile security environment, where small events could produce large effects. There is a particular danger of miscalculations in the realm of cyber activities, where actions can have unintended consequences. Therefore, there is a need for mechanisms to reduce uncertainty and facilitate communication between states. Confidence-building measures

and transparency measures can help reduce uncertainty and facilitate communication. However, developing such mechanisms in a climate of mistrust is difficult. Therefore, reducing the danger of miscalculations is a primary task for policymakers.

Technology now has a more central role than ever before in shaping security environments in Europe. Cyber capabilities, artificial intelligence, and autonomous systems have changed the way conflicts occur. These technologies provide new opportunities for adversaries to identify weaknesses. At the same time, they offer new tools for defense and deterrence. The dual-use nature of technology adds complexity to attempts to manage the risks of security. The rapidly changing nature of technology also creates a problem for policymakers who want to maintain consistency. Policymakers are thus faced with a gap between technological capabilities and regulatory frameworks. There is therefore a need for increased investment in R&D. Policymakers must develop strategies to mitigate the risks associated with the emergence of new technologies. The need to address cybersecurity and data protection issues is a part of this. Ultimately, technology is one of the main drivers of the security challenges of today.

The findings emphasize the importance of societal resilience in dealing with hybrid threats. Hybrid threats usually do not target the state or its military apparatus like traditional security challenges; rather, they usually target the social and political structure of societies. Adversaries try to erode trust in institutions and divide the population. Societal resilience is therefore crucial for ensuring the stability of society. Promoting media literacy, raising public awareness, and strengthening democratic institutions are examples of how to build societal resilience. Societal resilience is complementary to traditional security measures. Societal resilience can make the strategies of adversaries less effective, since they are based on creating divisions in the population. Building resilience however is a long-term and complex process. To build resilience, many actors must act together, such as governments, civil society, and the private sector. Therefore, enhancing societal resilience is a crucial element of modern security policy.

5.7. Recommendations

European states must create a multi-domain deterrence strategy. A multi-domain strategy combines all of the available military, economic, cyber and informational weapons. Because many of the current threats are hybrid, (i.e., they use many different types of attacks) the best way to combat them is to have a multi-domain strategy. With a multi-domain strategy, countries can punish an adversary in ways that do not involve just military action. That means that a country will have a better chance to prevent the adversary from taking aggressive action. In addition, multi-domain deterrence is more likely to have a deterrent effect than a single domain strategy. Therefore, creating a multi-domain deterrence strategy should be a top priority for European security.

Cyber-attacks are becoming more prevalent and, therefore, increasing cyber security capabilities is becoming increasingly important. European states must invest in new cyber technology and infrastructure to secure their critical systems. This includes making sure that the electrical grid, communication networks and financial systems are resilient. European states must also collaborate with each other to share cyber intelligence and best practices. Cyber

security must also become part of a state's overall security strategy. This would require coordination among government agencies, the private sector and international partners. Finally, the skills gap in cyber security must be addressed through education and training. Increasing cyber security capabilities is both a form of defense against cyber-attacks and a form of deterrence. If a state can show that it can effectively respond to cyber-attacks, then it may deter an adversary from conducting cyber-attacks.

In order to be able to deal with hybrid threats effectively, European security institutions must improve their cooperation and coordination. They must improve their ability to share information and develop cooperative strategies to deal with hybrid threats. Institutions like NATO and the EU must cooperate closely with each other so that they have a coordinated response. There also needs to be more integration of different domains of warfare, particularly cyber and information warfare. Policymakers must give priority to developing common standards and procedures for dealing with hybrid threats. This would make it easier for the institutions to coordinate and make their responses more effective. However, achieving this goal is difficult because it requires overcoming institutional and political obstacles. Member states must show that they are committed to cooperation and collective security. Improving institutional cooperation is one of the most important goals for European security.

Societal resilience is another area where European states must take action to mitigate the effects of hybrid threats. To counter disinformation campaigns and decrease their effectiveness, European states must support initiatives to increase media literacy and public awareness. In addition, strengthening democratic institutions is necessary to maintain public trust. European states must work with the civil society and the private sector to develop comprehensive resilience strategies. This must include identifying vulnerabilities in the social and economic systems. In addition, resilience must be included in a state's national security strategy. This requires shifting from reactive to proactive approaches. If European states can increase their resiliency, they can decrease the incentive for adversaries to use hybrid warfare. Thus, increasing societal resiliency must be one of the top priorities of European security.

One of the ways that European states can reduce the uncertainty that contributes to the security dilemma is by encouraging confidence, building measures and increasing transparency. Confidence building measures can include a variety of initiatives that are designed to reduce uncertainty and build trust between states. For example, regular communication and dialogue can help clarify a state's intentions and reduce the likelihood of misperception. Transparency regarding military activities can also help alleviate concerns about potential threats. In addition, confidence building measures can provide opportunities for cooperation. This can help build trust and reduce tensions. However, confidence building measures require political will and a commitment to cooperation. States must be willing to engage in dialogue and compromise. Although confidence building measures are challenging, they are essential to maintaining stability. Therefore, they should be a key component of European security strategies.

6. Conclusion

The ever-changing European security landscape is characterized by the blending of old and new security concerns, which are creating an unstable environment. A variety of hybrid threats exist today that make traditional deterrence models difficult if not impossible to apply. This paper uses qualitative document analysis of 57 primary documents and three in-depth cases to demonstrate how hybrid warfare creates uncertainty; makes attribution difficult; and reduces the threshold of violence thereby causing greater distrust amongst nations. Traditional methods of deterrence using military action have proven unsuccessful in addressing many of the challenges posed by hybrid warfare. Examples include the Baltic Sea cable incident where there were no available military options and Germany's cyber campaign where traditional deterrence did not offer any viable course of action. Instead of discarding deterrence entirely, this paper argued that the need to evolve traditional deterrence thinking into what we call multi-domain deterrence. Multi-domain deterrence differs from classical, cross-domain, and integrated deterrence as explained because it includes proactive building of resilience; enhances attribution; and employs coordinated military or non-military tools along the entire spectrum of conflict.

For example, our study demonstrates that when high confidence attribution is attained it allows for multi-domain responses that can achieve deterrence effectives regardless of availability of military options. The paper emphasizes the need to adapt institutions and foster societal resilience against hybrid attacks. We use three theoretical lenses (realist international relations theory to explain structural constraints; constructivist international relations theory to capture perceptions or identity dynamics and modern deterrence theory to analyze credibility/signaling to predict an all-encompassing analytic lens. Combining theories allows us to show how each captures a unique aspect of hybrid conflict: realist international relations theory shows why states engage in competition; constructivist international relations theory shows why different actors interpret the same actions differently; and modern deterrence theory shows why certain types of threats are successful/unsuccessful.

Within academic literature, this research supports Freedman's (2019) conclusion that classical deterrence is being challenged but rejects his conclusion that deterrence must be scrapped and instead shows how it can be adapted/re-configured. This work builds upon Nye's (2017) concept of resilience and demonstrates that resilience is most effective when used in conjunction with maintained punishment capability. Additionally, this research applies to the Rid's (2020) attribution analysis to identify institutional mechanisms that would allow for reducing ambiguity to acceptable levels.

Therefore, these findings emphasize the need for creative and adaptive approaches to security in the 21st Century. European states must invest in multi-domain capabilities that include forensic cyber attribution; intelligence sharing mechanisms; resilience infrastructure; and coordinated sanction frameworks. The three case studies serve as practical examples; the Baltic response (increasing surveillance or resilience); the Czech response making public attribution or targeted sanctions and the German response involving cyber/diplomatic/economic actions.

In summary, maintaining stability in Europe will necessitate a holistic approach to security that addresses security issues across multiple domains at once. The data from 2022-24 indicate that although no one response has established total deterrence, the emerging multi-domain tool kit provides a step forward from the classic model. Therefore, future research should focus on determining whether these modifications generate persistent deterrence effects over extended periods of time, and whether European experiences generalize to other regions experiencing hybrid threats, especially the Indo-pacific region.

References

Acharya, A. (2014). The end of American world order. Polity Press.

Adamsky, D. (2015). Cross-domain coercion: The current Russian art of strategy. IFRI Proliferation Papers, 54, 1–56.

Booth, K., & Wheeler, N. J. (2008). The security dilemma: Fear, cooperation, and trust in world politics. Palgrave Macmillan.

Braun, V., & Clarke, V. (2006). *Using thematic analysis in psychology*. *Qualitative Research in Psychology, 3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Buzan, B., & Wæver, O. (2003). Regions and powers: The structure of international security. Cambridge University Press.

Clarke, M. (2020). The Belt and Road Initiative and the future of regional order in Eurasia. Asian Affairs, 51(2), 379–399.

Cooley, A., & Nexon, D. (2020). Exit from hegemony: The unraveling of the American global order. Oxford University Press.

Edmond, C. (2025). Nuclear disarmament and the erosion of deterrence effectiveness: Case study—Ukraine (pp. 1–31). https://doi.org/10.25776/ngh0-vj51

Freedman, L. (2019). The future of war: A history. PublicAffairs.

Giles, K. (2016). Russia's "new" tools for confronting the West: Continuity and innovation in Moscow's exercise of power. Chatham House.

Glaser, C. L. (2010). Rational theory of international politics: The logic of competition and cooperation. Princeton University Press.

Hoffman, F. G. (2007). Conflict in the 21st century: The rise of hybrid wars. Potomac Institute for Policy Studies.

Horowitz, M. C., Scharre, P., Velez-Green, A., & Allen, G. C. (2019). Strategic competition in an era of artificial intelligence. Center for a New American Security.

Jervis, R. (1978). Cooperation under the security dilemma. World Politics, 30(2), 167–214.

Keohane, R. O., & Nye, J. S. (2012). Power and interdependence (4th ed.). Pearson.

Kofman, M., & Rojansky, M. (2015). A closer look at Russia's "hybrid war." Kennan Cable, 7, 1–9.

Mearsheimer, J. J. (1983). Conventional deterrence. Cornell University Press.

Mearsheimer, J. J. (1994). The false promise of international institutions. International Security, 19(3), 5–49.

Nye, J. S. (2017). Deterrence and dissuasion in cyberspace. International Institute for Strategic Studies.

Posen, B. R. (2014). Restraint: A new foundation for U.S. grand strategy. Cornell University Press.

Rid, T. (2020). Active measures: The secret history of disinformation and political warfare. Farrar, Straus and Giroux.

Rose, G. (1998). Neoclassical realism and theories of foreign policy. World Politics, 51(1), 144–172.

Schelling, T. C. (1966). Arms and influence. Yale University Press.

Snyder, J. (1985). Perceptions of the security dilemma in 1914. In R. Jervis & J. Snyder (Eds.), Dominoes and bandwagons: Strategic beliefs and great power competition in the Eurasian rimland (pp. 153–180). Oxford University Press.

Walt, S. M. (1987). The origins of alliances. Cornell University Press.

Waltz, K. N. (1979). Theory of international politics. McGraw-Hill.

Wendt, A. (1999). Social theory of international politics. Cambridge University Press.

Zilincik, S., & Giumelli, F. (2022). Sanctions and hybrid conflict: The case of Russia. Journal of European Integration, 44(3), 345–361.