e-ISSN: 2798-4427

JGSS

Journal of Global Strategic Studies

Vol. 05 No. 02 Desember 2025

MASTER'S PROGRAMS IN INTERNATIONAL RELATIONS
FACULTY OF SOCIAL AND POLITICAL SCIENCE
JENDERAL ACHMAD YANI UNIVERSITY

E-ISSN: 2798-4427
DOI: 10.36859/jgss.v5i2

Journal of Global Strategic Studies
Vol. 05 No. 02
December 2025

CONTENTS

E-ISSN: 2798-4427
DOI: 10.36859/jgss.v5i2

Journal of Global Strategic Studies
Vol. 05 No. 02
December 2025

GLOBAL STRATEGIC STUDIES

E-ISSN: 2798-4427
DOI: 10.36859/jgss.v5i2.3866

Journal of Global Strategic Studies
Vol. 05 No. 02
December 2025

Neither Cold nor Hot: Western States' Defensive Response to the Hybrid Warfare Threat

Ian Roberge & Daven Ng

York University

This article is interested in hybrid warfare and states' defensive policy responses from a Western perspective. Hybrid warfare has become a critical component of contemporary interstate conflicts, deliberately narrowing the gap between conventional military engagements and grey zone operations. It combines military tactics with non-military tools, such as cyber operations, disinformation campaigns, and economic coercion, to weaken adversaries without engaging in conventional warfare. Russia's War in Ukraine illustrates the use of hybrid warfare to achieve imperialist objectives, while similar campaigns have targeted other Western democracies. China's actions in the Indo-Pacific reflect comparable hybrid strategies. While much attention has focused on its offensive use, less is known about how states respond defensively. This paper explores how Australia, New Zealand, the United Kingdom, Canada, the United States, and Finland respond to hybrid threats. It argues that Western policy responses are uneven, with some states better prepared than others. Effective defense requires a clear definition of hybrid warfare, a comprehensive approach, and sustained resources. Based on publicly available policy documents, this comparative case study assesses how national interests are protected, despite research limitations due to the classified nature of hybrid operations.

Keywords: *hybrid warfare, grey-zone, military, civilian, transparency, foreign interference*

Introduction

In the last two decades, we have witnessed a fundamental shift in interstate conflict, moving away from clearly defined military confrontations toward ambiguous engagements between war and peace situated within the grey zone. At the forefront of this transformation lies hybrid warfare, a deliberate and strategic approach employed by states to weaken and undermine their adversaries without providing a clear *casus belli*.

Hybrid warfare achieves this by seamlessly integrating conventional military tactics with non-military tools, such as cyber operations, disinformation campaigns, and economic coercion. This hybrid approach has become a pivotal component of contemporary interstate conflicts, with states worldwide adopting it as a strategic tool. The conceptual foundations of hybrid warfare are traced to Frank Hoffman, whose work synthesized several earlier strands of thinking on modern conflict (Fridman, 2018; Nasu, 2019; Wegge & Wetzling, 2020). Drawing on four earlier works: Thomas Hammes and William Lind's fourth-generation warfare concept, Thomas Huber's Compound Wars, Qiao Liang and Wang Xiangsui's Unrestricted Warfare, and the U.S. National Defense Strategy of 2005, Hoffman (2007) defined hybrid warfare as the combined use of conventional and unconventional strategies and tactics by state or non-state actors to achieve synergistic effects on the battlefield. A key feature of hybrid warfare is its deliberate creation of ambiguity, blurring the lines between war and peace. While the concept has since evolved, particularly following Russia's 2014 invasion of Crimea, Hoffman's framework remains central to ongoing debates about the nature of contemporary conflict and continues to inform how hybrid threats are analyzed (Fridman, 2018). Russia's war in Ukraine serves as a vivid example of how hybrid warfare is being employed to advance imperialist foreign policy objectives. Similar tactics have also been adopted by other state actors, notably China, whose activities in the Indo-Pacific underscore the strategy's expanding global significance. While the offensive use of hybrid warfare is increasingly documented, the understanding of how states' foreign and defense policies have evolved in response remains limited.

In this article, we study Western states' responses to hybrid warfare by comparing their conceptual understanding of hybrid threats, the clarity of their legislative frameworks, and the comprehensiveness of their governmental structures and policies. Our analysis specifically examines how six Western democracies, Canada, Australia, New Zealand, the United Kingdom, the United States, and Finland have responded to the challenges posed by hybrid warfare, focusing on the Five Eyes member states for their shared security interests and Finland for its proximity to Russia. Hybrid warfare represents a multifaceted threat that compels states to develop a comprehensive, targeted and strategic approach (Aoi et al., 2018). We argue that although hybrid warfare is widely acknowledged as a significant security challenge across our case studies, there remain significant variations in their response, with some countries notably better prepared than others.

To develop this argument, the rest of the article is organized in four sections. The first section reviews recent scholarship on hybrid warfare, situating our study within broader debates on the nature of contemporary hybrid warfare. The second section presents the study's methodology and identifies the indicators for the analysis. Third, the results across the six states are presented. Finally, the conclusion draws together our findings with a discussion highlighting key policy gaps, strengths, and opportunities for improvement against the evolving nature of hybrid warfare.

On Hybrid Warfare

The concept of hybrid warfare is now broadly recognized, though it remains hotly debated. Frank Hoffman (2007) is acknowledged as the first scholar to have conceptualized the term (Fridman, 2018; Nasu, 2019; Wegge & Wetzling, 2020). Hoffman (2007) defined hybrid warfare as the deliberate combination of conventional and unconventional strategies and tactics by state or non-state actors to create ambiguity and achieve synergistic effects on the battlefield. His framework remains important for understanding the evolving nature of hybrid threats, particularly the interplay between military, technological, and political tools (Fridman, 2018; Wegge & Wetzling, 2020). While Hoffman (2007) drew on cases such as the 2006 Lebanon War to illustrate hybrid tactics, where Hezbollah combined conventional and unconventional operations with advanced technologies to challenge the Israeli Defense Force, the concept has evolved considerably, particularly in response to state-level applications. Russia's actions in Crimea in 2014 are usually understood as the first successful state-level application of hybrid warfare, combining covert military operations, cyberattacks, economic coercion, espionage, and sophisticated disinformation campaigns (Aoi et al., 2018; Bowers, 2018; Ito, 2022; Jackson, 2019). These tactics created operational ambiguity and plausible deniability, complicating responses and countermeasures (Briggs & Matejova, 2023; Stănescu, 2023). Thompson (2022) notably characterizes Russia's strategy as forcing states into accepting a new geopolitical reality through carefully managed perceptions and strategic ambiguity.

Despite consensus on Crimea's importance, scholarly debates persist about precisely defining hybrid warfare. NATO's definition emphasizes a combination of military and non-military methods employed covertly or overtly by state and non-state actors (Bowers, 2018; Carment & Belo, 2018; NATO, 2024). This description resonates strongly with Russia's operations in Crimea. However, some academics argue for definitions that require significant conventional military engagement alongside

unconventional strategies, referencing earlier conflicts like Hezbollah's tactics during the 2006 Lebanon War (Lanoszka, 2016). Conversely, contemporary analyses increasingly emphasize the strategic dominance of non-military elements. Scholars like Thompson (2022) suggest a deliberate preference by states such as Russia and China to achieve political objectives without overt military escalation, highlighting hybrid warfare's inherent flexibility and context-dependent nature (Aoi et al., 2018; Bowers, 2018).

Technological advancements have also significantly reshaped contemporary hybrid warfare, with cyber operations and influence campaigns becoming central to its strategy. Scholars emphasize how digital platforms amplify hybrid warfare's decentralized and non-linear characteristics, enabling state actors to exploit societal vulnerabilities and undermine political cohesion without triggering conventional military responses (Fridman, 2018; Paterson, 2020; Stănescu, 2023). Russia's strategic success in Crimea emphasized the need for enhancing state preparedness, advocating comprehensive policies that integrate traditional military preparedness with robust cybersecurity, economic resilience, and strategic communication capabilities (Rausta & Monaghan, 2021; Wegge & Wetzling, 2020).

Contemporary conceptualizations emphasize hybrid warfare's strategic position within legal and operational grey zones, focusing on the manipulation of perceptions and misinformation campaigns that avoid crossing established thresholds of war (Boucher, 2018; Briggs & Matejova, 2023). Briggs and Matejova (2023) specifically align this approach with the Russian concepts of *maskirovka* and *gibridnaya voyna*, underscoring the strategic manipulation integral to these tactics. Nasu (2019) elaborates that hybrid warfare occupies a space between diplomatic measures and outright military confrontation, utilizing centralized state resources and strategic planning to destabilize opponents internally through legal, informational, and economic methods (Burkle et al., 2022; Carment & Belo, 2018; Granholm et al., 2022). Democratic states face unique vulnerabilities in countering hybrid warfare, particularly due to constitutional protections of free speech and decentralized bureaucratic decision-making, which adversaries effectively exploit through disinformation and influence operations (Ito, 2022; Paterson & Hanley, 2020). Economic strategies also constitute a core component of hybrid warfare, as states leverage financial and infrastructural tools to achieve strategic objectives while avoiding direct military confrontation. For example, China's Belt and Road Initiative and strategic 5G deployments exemplify efforts to expand influence and set international standards advantageous to its strategic objectives (Chung, 2021; Ito, 2022). Likewise, Russia's manipulation of energy supplies demonstrates economic

resources' strategic weaponization to exert political pressure on European states (Aoi et al., 2018; Briggs & Matejova, 2023). In both cases, these economic measures exemplify the hybrid warfare strategy of combining conventional and unconventional tactics to create ambiguity, influence perceptions, and advance state interests without triggering open conflict.

Additionally, regional scholarly perspectives shape differing understandings of and perceived threats posed by hybrid warfare. Western literature primarily explores Russian hybrid threats against Europe and North America, highlighting cyber interference, economic pressure, and targeted disinformation campaigns such as those seen during the 2016 U.S. election and the UK's Brexit (Burkle et al., 2022; Janicatova & Mlejnkova, 2021; Paterson & Hanley, 2020). Conversely, Asia-Pacific literature emphasizes China's hybrid operations characterized by maritime disputes, strategic naval expansions, and the deployment of maritime militias disguised as civilian entities to blur the lines of international response capabilities (Aoi & Heng, 2021; Chung, 2021; Ito, 2022; Ong, 2018). North Korea represents a unique regional actor employing asymmetric hybrid methods, including cyberattacks and state-sponsored criminal activities, to compensate for its conventional military disadvantages (Bowers, 2018). Despite its adoption, the concept of hybrid warfare faces criticism regarding its definitional vagueness, and potential overgeneralization. Critics highlight that hybrid tactics such as psychological operations and irregular warfare have historical precedents. Nevertheless, contemporary digital platforms and operational integration distinguish current hybrid practices significantly, marking a clear evolution from historical forms of warfare (Briggs & Matejova, 2023; Jackson, 2019; Murray & Mansoor, 2012).

The ongoing Russo-Ukrainian conflict underscores significant shifts in hybrid warfare practices and illuminate important gaps in the scholarly literature. One such prominent gap is the limited comparative analysis of how democratic states develop policies to counter hybrid threats effectively. This comparative perspective is essential to understanding policy strengths and weaknesses among targeted nations. Addressing this deficiency, this study comparatively analyzes hybrid warfare responses by Canada, Australia, New Zealand, the United Kingdom, the United States, and Finland, providing insights into diverse national policy approaches and identifying best practices of countering hybrid warfare activities. Ultimately, this analysis aims to bridge notable gaps in academic understanding and policy formulation, enhancing the collective preparedness of democratic states confronting hybrid warfare threats.

Research Method

This study employs a qualitative, multiple-case study design, with each state serving as the unit of analysis (Yin, 2018). This methodology is suitable for examining the complex challenges posed by hybrid warfare, where the boundaries between the issue and its broader political and institutional context are often blurred (Ibid.). A cross-case synthesis approach is applied to this analysis, which allows for comparison between states while also highlighting the key differences in their policies countering hybrid warfare (Ibid.). Through this comparative framework, this study aims to discern recurring patterns and divergences in national policy, underscoring both common strategies and country-specific approaches. To achieve this, this research draws on evidence primarily in the form of official government documentation such as national government policies, legislative documents, and institutional mandates and statements. To evaluate state responses to hybrid warfare, this study applies six standardized features that ground the fluid concept of hybrid warfare policy into clear and observable indicators, thereby allowing systematic evidence gathering and comparative analysis.

The first indicator assesses whether a state explicitly defines hybrid threats in its strategic documents, which is essential for guiding coherent policy action. The second examines whether legislative instruments have been enacted or updated to address hybrid threats, including cybercrime, disinformation, and foreign interference. The third looks at institutional responsibility by identifying which agencies or interdepartmental bodies are tasked with leading and coordinating hybrid warfare responses. The fourth reviews the existence and scope of national strategies or policy frameworks specifically aimed at countering hybrid threats. The fifth considers whether states acknowledge or develop offensive capabilities, such as active cyber operations, as part of their national security posture. The sixth and final indicator evaluates transparency and public communication, particularly the extent to which governments disclose hybrid threats and responses to build public resilience. Together, these indicators provide an original analytic framework built on established methodology, adapted to comparing hybrid warfare readiness across jurisdictions. Following the collection and analysis of official government documents, legislative texts, and departmental statements, several key themes emerge in how the selected states conceptualize and address hybrid warfare.

Government Policies and Results

Across Canada, Australia, New Zealand, the United Kingdom, the United States, and Finland, hybrid warfare is broadly understood as a multifaceted threat that

integrates both conventional and unconventional military and non-military tactics. Definitions vary but consistently recognize the roles of both state and non-state actors, with countries such as Russia, China, and Iran frequently identified as primary sources of hybrid threats. Legislative responses predominantly target cyber threats, disinformation, and foreign interference; however, the scope, depth, and specificity of these measures differ notably among states. Institutionally, countries demonstrate diverse strategic emphases, ranging from civilian-led approaches to reliance on military and intelligence agencies. Differences also exist in interdepartmental coordination and transparency, reflecting national priorities, political systems, and threat perceptions. The table below outlines key findings as categorized by the six standardized indicators.

E-ISSN: 2798-4427
DOI: 10.36859/jgss.v5i2.3866

	Finland	United States	United Kingdom	New Zealand	Australia	Canada
Indicator 1 How does the country define hybrid warfare, or a synonymous concept?	Defines hybrid threats as systematic state-led strategies combining multiple methods (Ministry of the Interior, 2025). State actors: Russia and China (Finnish Security and Intelligence Service, 2024; 2025a).	Hybrid warfare defined as integrated gray-zone activities alongside conventional military actions. (National Intelligence Council, 2024). State actors: Russia, China, Iran, and North Korea (U.S. Department of Homeland Security, 2023; National Intelligence Council, 2024b, 7).	Hybrid warfare defined as multiple synchronized instruments targeting vulnerabilities, notably emphasizing cognitive operations (Multinational Capability Development Campaign, 2019, 13). State actors: China and Russia (Ministry of Defence, 2023).	Hybrid threats defined as combined military, covert, and overt non-military actions (National Cyber Security Centre, 2022, 23). State actors: China and Russia (Department of the Prime Minister and Cabinet, 2023).	Hybrid warfare defined as blending conventional, cyber, and irregular tactics. (The Senate, 2023, 3). State Actors: China, Russia, and Iran (*Ibid.*).	Hybrid warfare defined as coordinated diplomatic, informational, cyber, military, and economic tactics (Department of National Defence, 2017, 53). State actors: China, India, Russia, North Korea (Canadian Centre for Cyber Security, 2024).
Indicator 2 How does the country address the issue of hybrid warfare and its related operations in their legislation?	*Border Guard Act* and *Cyber Resilience Act* (Ministry of Justice, 2018; Ministry of the Interior, 2025d; National Cyber Security Centre Finland, 2025; European Commission, 2025).	*FARA*, *Gray Zone Defense Act*, and related bills (U.S. Department of Justice, 2024; United States Congress, 2023; 2019; 2022; 2024a; 2024b).	*National Security Act 2023* (UK Legislature, 2024).	*Crimes Act 1961* (Ministry of Justice, 2025)	*Autonomous Sanctions Act*, *Criminal Code*, and *Espionage and Foreign Interference Act* (The Senate, 2023)	*An Act respecting countering foreign interference*, and *Foreign Influence Transparency Act* (Public Safety Canada, 2024b; 2024j; Department of Justice Canada, 2025).
Indicator 3 Which government agencies and departments are primarily responsible for addressing hybrid warfare?	Ministry of Defence Ministry for Foreign Affairs Ministry of Education and Culture Ministry of the Interior	Department of Defense U.S. Department of Justice Department of Homeland Security.	Ministry of Defence Secretary of State for the Home Department Secretary of State for Foreign, Commonwealth and Development Affairs	Ministry of Defence Government Communications Security Bureau Department of the Prime Minister and Cabinet Ministry for Ethnic Communities Ministry of Justice	Department of Defence Department of Home Affairs Attorney General' s Department*	Department of National Defence Public Safety Canada

E-ISSN: 2798-4427
DOI: 10.36859/jgss.v5i2.3866

	Finland	United States	United Kingdom	New Zealand	Australia	Canada
Indicator 4 How do these government agencies and departments counter hybrid warfare and its related operations in their policies?	The Finnish Defence Forces prepare for hybrid threats, while the ministries of Foreign Affairs, Education and Culture, and Interior collaborate on cybersecurity, media literacy, and counterintelligence (Ministry of Defence, 2024; Ministry for Foreign Affairs, 2025a; 2025b; Ministry of the Interior, 2025; SUPO, 2024). Civil agencies cooperate, but no civil–military coordination noted.	DoD handles hybrid warfare worldwide, including cyber and information ops (U.S. Special Operations Command, 2023; U.S. Army Cyber Command, 2025). Civilian agencies (DoJ, DHS, FBI, CISA) investigate foreign interference and strengthen infrastructure (U.S. Department of Justice, 2019; 2021; 2023; U.S. Department of Homeland Security, 2021; 2023). Civil–military cooperation noted (NSA, 2022).	The British Armed Forces monitor grey-zone developments; the National Cyber Force counters cyber and hybrid threats (Ministry of Defence, 2023; National Cyber Force, 2025). Civil agencies (Home Office, MI5, GCHQ, MI6) target foreign influence, espionage, and disinformation (Home Office, 2024a; MI5, 2025; National Cyber Security Centre, 2023; 2024), but no civil–military cooperation is evident.	The NZDF trains special operations to handle hybrid warfare and information warfare (NZDF, 2017; 2023). Civilian agencies, GCSB's National Cyber Security Centre, NZSIS, and the Ministry for Ethnic Communities, tackle cyber threats and foreign interference, with cooperation among them (Ministry for Ethnic Communities, 2024; NZ Security Intelligence Service, 2025), but no civil–military collaboration noted.	The ADF counters grey-zone threats with enhanced capabilities (Ministry of Defence, 2020; Australian Army, 2025), and the Australian Signals Directorate handles signals intelligence and cyber operations (Australian Signals Directorate, 2022; 2025). Civil agencies (e.g., Home Affairs, AFP, ASIO's CFI Taskforce) tackle foreign interference, but no civil–military collaboration noted (Attorney General's Department, 2024).	DND counters hybrid threats through the CAF, CANSOFCOM, and CSE (Department of National Defence, 2017; Canadian Armed Forces, 2025; CANSOFCOM, 2020; CSE, 2023). Public Safety's CSIS and RCMP investigate foreign interference (National Security and Intelligence Committee of Parliamentarians, 2024a). Civil–military cooperation noted (Canadian Armed Forces, 2025).
Indicator 5 How does the government engage in hybrid warfare?	Finland does not have a publicly declared hybrid warfare policy. There is no official documentation confirming government engagement in hybrid warfare operations.	The United States does not frame hybrid warfare as an official policy. However, USSOCOM, cyber command, and psychological operations units routinely engage in activities associated with hybrid warfare.	The United Kingdom does not have a publicly available hybrid warfare policy. Nonetheless, its military may conduct hybrid-related activities through psychological operations units (Ministry of Defence, 2021).	New Zealand has not issued any official documents indicating the existence of a hybrid warfare policy. Public sources do not confirm government-led hybrid operations.	Australia does not officially recognize hybrid warfare as a policy in public documents. However, the Australian Army's Intelligence Corps and the Australian Signals Directorate can conduct offensive cyber and hybrid warfare operations (Australian Army, 2025; Australian Signals Directorate, 2022; 2025).	Canada does not have a publicly declared hybrid warfare policy. However, the Canadian Armed Forces and CANSOFCOM engage in cyber and psychological operations that reflect hybrid warfare activities (Canadian Armed Forces, 2025; Canadian Army, 2025; CANSOFCOM, 2020). Additionally, CSE is authorised to conduct active cyber operations under government direction (CSE, 2023).
Indicator 6 How does the government engage in transparency and accountability relative to hybrid warfare?	Outside of publicly available defence reports, no official communications to the public were found. However, the Finnish Border Guard (2025a), Ministry of the Interior (2025a; 2025c; 2025d), and SUPO (2024) communicate to the public on hybrid warfare and related countermeasures.	Outside of publicly available defence reports, no official communications to the public were found.	Outside of publicly available defence reports, no official communications to the public were found. The government has communicated on initiatives like the Foreign Influence Registration Scheme, and different departments have disclosed some of their activities related to countering hybrid	Outside of publicly available defence reports, no official communications to the public were found. The government has communicated on initiatives like the Foreign Influence Transparency Scheme, and different departments have disclosed some of their activities related to countering hybrid	Outside of publicly available defence reports, no official communications to the public were found. The government has communicated on initiatives like the Foreign Influence Transparency Scheme, and different departments have disclosed some of their activities related to countering hybrid threats.	Outside of publicly available defence reports, no official military communications to the public were found. The government has communicated on initiatives like the Foreign Influence Transparency Scheme, and different departments have disclosed some of their activities related to countering hybrid

The results reveal a notable divergence in how Western democracies confront the growing challenge of hybrid warfare. Responses range from fragmented, siloed efforts to integrated national strategies that weave together civil, military, and legislative dimensions. At one end of this spectrum is Canada, which clearly identifies hybrid warfare as a complex combination of diplomatic, informational, cyber, military, and economic tactics (Department of National Defence, 2017). Yet despite this recognition, Canada's approach remains fragmented and lacks overall strategic cohesion. The Canadian Armed Forces and Communications Security Establishment focus on cyber and disinformation threats, while Public Safety Canada and its agencies address foreign interference through instruments like the Foreign Influence Transparency and Accountability Act. Each agency tends to operate independently, with seemingly limited coordination among them (Public Safety Canada, 2024f, 2024j; Communications Security Establishment, 2023).

New Zealand reflects a similar pattern of compartmentalized action. While it defines hybrid threats as the confluence of military and non-military tools, it relies heavily on specialized bodies such as the Government Communications Security Bureau's National Cyber Security Centre and the Ministry of Justice (National Cyber Security Centre, 2022; Ministry of Justice, 2025). Cooperation exists, but efforts lack cohesion and coordination across institutions (Department of the Prime Minister and Cabinet, 2023). Australia takes a modest step forward, explicitly defining hybrid warfare as a blend of conventional and irregular tactics. It has invested in enhancing both military capabilities and interagency mechanisms, with organizations like the Australian Signals Directorate and the Australian Defence Force assuming prominent roles (Department of Defence, 2024; Australian Signals Directorate, 2022). However, the absence of a centralized national doctrine weakens the overall coherence of its response, as responsibilities remain distributed among multiple civilian bodies (Justice and Community Safety Directorate, 2024).

The United Kingdom also demonstrates strong institutional capabilities, particularly through its intelligence and cybersecurity agencies, including MI5 and the National Cyber Force. Hybrid warfare is understood as the orchestration of multiple instruments against societal vulnerabilities (Ministry of Defence, 2023). Yet, in the absence of a unified doctrine, its approach remains somewhat opaque to the public and fragmented across departments (Home Office, 2024a; UK Legislature, 2024).

Further along the spectrum, the United States demonstrates a more mature response framework. Hybrid threats are addressed in legislation such as the Gray Zone Defense Assessment Act, providing a legislative anchor for a more holistic approach (United States Congress, 2023). While some decentralization persists, key institutions, including the Department of Defense, Department of Justice, and Department of Homeland Security, coordinate efforts to confront hybrid threats with significant operational capacity and legal authority (Cybersecurity & Infrastructure Security Agency, 2025a; U.S. Department of Homeland Security, 2023).

At the far end stands Finland, whose national posture towards hybrid threats is the most cohesive and transparent of the states surveyed. Hybrid threats are not only well-defined, as systematic, state-led strategies, but are also addressed through a deeply integrated model involving military readiness, cross-ministerial cooperation, and well-established legislative scaffolding, including the Border Guard Act and Cyber Resilience Act (Finnish Security and Intelligence Service, 2024; Ministry of Defence, 2024; National Cyber Security Centre Finland, 2025). Finland further distinguishes itself through its clear public communication and education initiatives, enhancing societal resilience through openness and preparedness. Ultimately, these results depict states' preparedness from loosely connected institutional responses to more complete and integrated strategies. While all six countries recognize the gravity of hybrid threats, their readiness varies considerably, shaped by political will, legal frameworks, and the degree of coordination between civil and military sectors.

Discussion

This section discusses the key findings from the comparative case studies, illustrating how varied state responses to hybrid warfare support the article's thesis. Despite a shared recognition of hybrid warfare as a security issue, differences in policy and legislation, and institutional structures, as noted in the results section, have led to varying levels of preparedness. This analysis builds upon the research's six indicators: conceptual definitions, legislative responses, institutional roles, identified threat actors, offensive strategies, and transparency.

Understandings of Hybrid Warfare and Related Concepts

The six countries examined each define hybrid warfare differently, although all recognize it as a coordinated blend of military and non-military tactics below the

threshold of conventional war, aimed at achieving political objectives. To start, Australia stands out as the only country to explicitly frame hybrid warfare as a military strategy. The Australian Defence Force has identified it as a critical threat, prompting investment in military capabilities. However, this military-centric view contrasts with historical examples like Russia's 2014 invasion of Crimea, where non-military tools played a central role (Rausta & Monaghan, 2021; Thompson, 2022; Wegge & Wetzling, 2020). Scholars caution that hybrid warfare should not be confined to military or civilian domains, as such binaries may hinder comprehensive responses (Wegge & Wetzling, 2020). This highlights how states diverge in their framing of hybrid warfare, which affects their broader policy decisions in countering hybrid activities.

Conceptual differences directly shape how each state builds policy, legislation, and institutional structures to counter hybrid threats. Australia's militarized framing raises questions about whether it enhances or limits its response capacity. By contrast, the United Kingdom reflects a broader shift toward emphasizing non-military elements, particularly cyber and information operations, in its use of the term, though its internal definitions remain inconsistent (Janicatova & Mlejnkova, 2021). In addition, Australia is also alone in recognizing lawfare as part of hybrid warfare, aligning with Burkle et al. (2022) and Carment and Belo (2018), who note lawfare's use to disrupt internal governance through legitimate legal mechanisms. However, specific policy responses remain unclear. In turn, the absence of this recognition in other countries may suggest a gap that limits their ability to anticipate legal manipulation. In this respect, incorporating lawfare into national strategies could strengthen democratic resilience, and its absence can be understood as evidence of uneven preparedness among states' readiness to counter hybrid warfare.

Furthermore, the distinction between foreign interference and foreign influence, made only by Australia and New Zealand, represents another point of conceptual divergence. The two Pacific countries define interference as malicious and influence as potentially benign if transparent. Other states use the terms interchangeably, which blurs the lines between legitimate diplomacy and covert manipulation. In practice, adopting this distinction may help states craft more targeted responses. All six countries differentiate between disinformation (intentional falsehoods) and misinformation (unintentional inaccuracies). Furthermore, Canada, the United Kingdom, and the United States further recognize malinformation, the weaponized use of truthful information to mislead. Therefore, this layered approach signals an evolving approach to information threats and highlights the need for nuanced, adaptable policies. Ultimately,

states that have not yet incorporated these distinctions could improve their hybrid threat responses by refining their definitions and frameworks accordingly.

The State Actors Responsible for Hybrid Warfare

All six countries identified Russia and China as the primary state actors behind hybrid warfare, consistent with existing literature. Russia's record includes economic and information warfare (Briggs & Matejova, 2018; Janicatova & Mlejnkova, 2021), while China combines diplomacy and information tactics in its strategy (Chung, 2021; Ito, 2022; Ong, 2018). Iran and North Korea were also noted by several states, though not universally. North Korea, for example, uses hybrid tactics to pursue foreign policy objectives against stronger powers (Bowers, 2018). Canada uniquely identified India as a hybrid threat actor, likely in response to recent allegations of Indian interference domestically (Canadian Centre for Cyber Security, 2024). These variations reflect how national security priorities and geopolitical contexts influence each state's threat assessments. While there is consensus on major adversaries, differing views on secondary actors suggest that hybrid warfare responses are highly context-dependent, and even when states agree on the threat actors, their policy responses are shaped by the unique threats they respectively face. Additionally, all six states also acknowledged the threat posed by non-state actors, reinforcing the need for broad and adaptable hybrid warfare policies. This recognition naturally leads into a closer analysis of how states balance offensive and defensive strategies when addressing hybrid warfare.

Variations in the Development of Legislation

Carment and Belo (2018) suggest that democracies often respond slowly to new threats due to decentralized decision-making and constitutional constraints. Yet, all six countries have recently introduced or are planning legislation to counter hybrid warfare, to varying levels of success. So far, the United States and Finland have passed legislation explicitly addressing hybrid threats. In 2023, the U.S. enacted a law assessing national counter-hybrid capacities, calling for stronger domestic capabilities and greater allied cooperation. Finland's legislation expands border guard powers, its only military-linked agency in this context, to address hybrid scenarios (Digital and Population Data Services Agency, 2025), reflecting its heightened security concerns due to its proximity to Russia. This approach offers a model worth examining by Australia and New Zealand, both of which have experienced Chinese naval incursions near their maritime boundaries

(Department of Defence, 2025). Australia and the United Kingdom have enacted foreign influence transparency registries to curb covert foreign interference; Canada has legislation to this effect, though it has yet to put in place a registry. The United States' Foreign Agents Registration Act of 1938 serves a similar role. These initiatives reflect a growing recognition of hybrid warfare's non-military dimensions. Legislating a polymorphous threat, however, remains challenging. In the United States, the challenge of getting legislation through Congress is evident; three other bills addressing hybrid threats have stalled in the Senate for over a year, while another failed in the House. These legislative efforts primarily target foreign interference, raising concerns about potential misuse given the ambiguity of hybrid warfare (Briggs & Matejova, 2023), especially in politically polarized environments like the U.S. post-2016. While many states still lack dedicated hybrid warfare legislation, the increasing use of hybrid warfare language in policy documents and related legislative developments signal growing institutional adaptation. As such, these legislative variations reveal differing levels of national preparedness and highlight opportunities for more cohesive and effective responses.

How Governments Have Addressed Hybrid Warfare

Across all six countries, hybrid warfare is primarily addressed through civilian, non-military institutions responsible for public safety, defense, and national security. These agencies focus on specific elements, such as cyber threats, disinformation, and foreign interference, rather than hybrid warfare as a unified concept. Carment and Belo (2018) emphasize the importance of integrating responses within civil-military frameworks, especially as hybrid threats often target civilian domains. Despite their involvement, public details of these policies remain limited, with insights derived from policy documents and official statements. Coordination typically occurs through reporting lines to higher national security or defense authorities, reflecting a wide-ranging, though compartmentalized approach. While most countries run public awareness campaigns to combat disinformation, Finland stands out by embedding hybrid threat education into its curriculum, a proactive move shaped by its proximity to Russia (Stănescu, 2023). Similar long-term societal strategies could benefit other states. Ito (2022) notes how China's hybrid tactics include leveraging small businesses to exert influence, prompting some countries to develop awareness programs for vulnerable sectors. As underscored by these examples, civilian institutions are on the frontline of hybrid threat responses and often operate in parallel to military efforts to combat hybrid warfare.

As for countries' military response, defense documents across all six states recognize hybrid warfare as a strategic concern, but public articulation of military roles remains limited. In Canada, New Zealand, and the United States, special operations units reportedly handle hybrid threats, though specific policies remain classified. All states also participate in NATO-led initiatives like the Multinational Capability Development Campaign (2019), though the influence of such collaborations on national policy is unclear. Public documentation on civil-military cooperation is sparse. Canada and the U.S. indicate some coordination in cyber defense, though concrete evidence is lacking. The likely classified nature of such partnerships makes comprehensive analysis difficult. In practice, civilian agencies handle the components of hybrid warfare, while militaries take a more holistic view, identifying hybrid warfare as an overarching threat in national defense strategies.

Overall, governments have taken steps to address hybrid warfare's key components, but most policies are recent, and their effectiveness remains uncertain. The rise of foreign-supported fringe groups in the U.S. (Department of the Treasury, 2024) and the strategic use of social media by adversaries (Stănescu, 2023; Ito, 2022; Richey, 2018) reveal the societal risks posed by hybrid tactics. Russia and China, for instance, exploit internal divisions, using political systems against themselves (Chung, 2021; Stănescu, 2023), often through covert, non-military actions that offer plausible deniability (Briggs & Matejova, 2023; Rausta & Monaghan, 2021; Thompson, 2022; Wegge & Wetzling, 2020). This ambiguity complicates attribution and limits response options, often forcing target states into reactive positions (Bowers, 2018; Thompson, 2022). While national strategies are evolving, they tend to address symptoms, like cyberattacks and disinformation, rather than the strategic objectives driving hybrid threats. Without clearer definitions and proactive planning, states risk remaining vulnerable to the blurred, adaptive tactics that define hybrid warfare. This suggests that future efforts will need to focus not only on improving institutional coordination but also on addressing the underlying strategies that underpin hybrid warfare.

Conducting Hybrid Warfare

Publicly available documents suggest that none of the six countries officially engage in hybrid warfare. However, both military and civilian agencies responsible for defending against hybrid threats, particularly cyber and intelligence bodies, are also equipped to conduct offensive operations if authorized. While the literature rarely addresses Western states as hybrid warfare actors, Carment and Belo (2018) argue that

interventions and aid programs may constitute hybrid tactics. Similarly, Ito (2022) views China's Belt and Road Initiative (BRI) as a strategic form of hybrid engagement. Though beyond the scope of this paper, programs like Canada's Official Development Assistance and USAID might be interpreted similarly, though others may classify these efforts as soft power. This reflects broader critiques that hybrid warfare is not a novel concept, but rather a continuation of longstanding geopolitical practices (Murray & Mansoor, 2012; Lanoszka, 2016). Western and Asia-Pacific literature tends to frame Russia and China as primary adversaries, often overlooking how these states understand or operationalize hybrid warfare themselves. This omission creates a significant analytical gap, limiting insight into adversarial motivations, doctrines, and counterstrategies. A Western-centric focus risks presenting a one-sided view that does not fully capture the strategic logic or perspectives of China and Russia. Ultimately, recognizing this imbalance makes it imperative to consider adversarial perspectives more directly when evaluating Western strategies.

Additionally, this gap is especially relevant to this paper's comparative analysis of how Five Eyes countries and Finland respond to hybrid threats. Without engaging with the perspectives of China and Russia, it is difficult to assess the full effectiveness of Western responses. Broader, more inclusive frameworks are needed to understand hybrid warfare dynamics from all sides. The fluidity of the concept further complicates this task. As global adoption of the term increases, its meaning becomes more ambiguous. For instance, Western actions during the Ukraine war, such as freezing assets of Russian oligarchs, may qualify as hybrid tactics (UK Parliament, 2025), though interpretations vary depending on geopolitical perspective. China and Russia would not view themselves as adversaries in the same way Western actors do. With this in mind, to fully understand the modern hybrid threat landscape, it is essential to move beyond a binary framework and consider how all parties engage with and define hybrid warfare.

Communications, Transparency, and Accountability

Transparency and public communication are central to understanding how Australia, Canada, Finland, the UK, the U.S., and New Zealand approach hybrid warfare. While none of these states have openly disclosed comprehensive hybrid warfare strategies, they address related components, such as cyber threats, disinformation, and foreign interference, through compartmentalized policies. Finland is a notable exception, openly discussing hybrid threats through the Ministry of the Interior and the Border Guard, reflecting a more integrated and transparent approach. This example shows the

contrast in communication and transparency among the states. Indeed, this hesitancy toward transparency may stem from the covert nature of hybrid warfare; disclosing strategies could potentially aid adversaries in circumventing them. However, Richey (2018) counters this view, arguing that transparency in non-military domains, particularly information warfare and cyber operations, can strengthen societal resilience. Drawing from the EU's response to Russian hybrid threats, Richey emphasizes that strategic communication helps prepare institutions and the public to recognize and resist hybrid tactics. These perspectives suggest that while there is a need for secrecy, deliberate transparency can enhance overall preparedness and societal robustness against hybrid threats. Thus, the issue is not whether to communicate publicly, but how to do so without compromising national security. A strategic communication framework can inform and empower citizens without revealing operational vulnerabilities. Finland's example shows how direct engagement with the public can build resilience and foster a proactive security posture. Ultimately, other states would benefit from incorporating similar approaches, reinforcing the broader thesis that adaptive, transparent, and comprehensive strategies are essential for effectively countering hybrid warfare.

Final Thought

This paper has examined how Canada, Australia, New Zealand, the UK, the U.S., and Finland have responded to the evolving threat of hybrid warfare. While all six states recognize hybrid warfare as a blend of conventional and non-traditional tactics, including cyber operations, disinformation, and foreign interference, their responses vary considerably. Canada and New Zealand exhibit fragmented, reactive approaches, while Finland has adopted a comprehensive, transparent strategy that brings together civilian and military preparedness. These contrasts demonstrate the importance of understanding how policies are coordinated and implemented across different institutional frameworks. Additionally, these findings underscore a central insight: preparedness depends not only on recognizing the threat but on how clearly and cohesively states embed hybrid warfare responses across their institutional frameworks.

Looking ahead, stronger coordination between researchers and policymakers will be essential in refining national strategies and building holistic and effective approaches. International collaboration, especially through NATO and allied frameworks, remains uneven and warrants further exploration to strengthen collective responses. In the case of Asia, and particularly with respect to China, future research should address persistent

challenges around data access, strategic transparency, and conceptual differences. Understanding how hybrid threats are defined, deployed, and countered in non-Western contexts will be critical for building informed, adaptive policy responses. Future lines of inquiry should prioritize measuring the effectiveness of hybrid warfare strategies, assessing international coordination efforts, and clarifying the concept's application across different geopolitical environments. These steps are essential in supporting the development of more resilient and coherent responses to hybrid threats as they continue to evolve.

References

Aoi, C., M. Futamura, and A. Patalano. 2018. "Introduction: Hybrid Warfare in Asia—Its Meaning and Shape." Pacific Review 31(6): 693–713. https://doi.org/10.1080/09512748.2018.1513548.

Aoi, C. and Y.-H. Heng. 2021. "Regional Communicative Dynamics and International Relations in the Asia-Pacific." Asian Perspective 45(3): 479–501. https://doi.org/10.1353/apr.2021.0032.

Attorney-General's Department. 2024. Foreign Influence Transparency Scheme. Canberra, AU: Attorney-General's Department. Accessed 8 January 2025 at https://www.ag.gov.au/integrity/foreign-influence-transparency-scheme.

Australian Army. 2025. Australian Intelligence Corps. Canberra, AU: Australian Army. Accessed 14 January 2025 at https://www.army.gov.au/about-us/army-corps/australian-intelligence-corps.

Australian Federal Police. 2023. Espionage and Foreign Interference. Canberra, AU: Australian Federal Police. Accessed 1 December 2024 at https://www.afp.gov.au/crimes/espionage-and-foreign-interference.

Australian Federal Police. 2025. Foreign Interference in the Community. Canberra, AU: Australian Federal Police. Accessed 9 January 2025 at https://www.afp.gov.au/sites/default/files/PDF/Factsheet-ForeignInterferenceintheCommunity.pdf.

Australian Security Intelligence Organisation. 2024. Director-General's Annual Threat Assessment 2024. Canberra, AU: Australian Security Intelligence Organisation. Accessed 11 January 2025 at https://www.asio.gov.au/director-generals-annual-threat-assessment-2024.

Australian Signals Directorate. 2022. Australian Signals Directorate 2022–23 Annual Report. Canberra, AU: Australian Signals Directorate. Accessed 15 December 2024 at https://www.transparency.gov.au/publications/defence/australian-signals-directorate/australian-signals-directorate-2022-23-annual-report.

Australian Signals Directorate. 2025. Offensive Cyber. Canberra, AU: Australian Signals Directorate. Accessed 10 January 2025 at https://www.asd.gov.au/about/what-we-do/offensive-cyber#:~:text=The%20Australian%20Signals%20Directorate%20(ASD,authorisation%20of%20the%20Australian%20Government.

Boucher, J.-C. 2018. Hybrid Warfare and Civil-Military Relations. Calgary: Canadian Global Affairs Institute. ISBN: 1988493765.

Bowers, I. 2018. "The Use and Utility of Hybrid Warfare on the Korean Peninsula." Pacific Review 31(6): 762–786. https://doi.org/10.1080/09512748.2018.1513547.

Briggs, C. M. and M. Matejova. 2023. "Hybrid Warfare in Ukraine and Its Impact on Climate Politics." Mezinárodní Vztahy 58(2): 149–165. https://doi.org/10.32422/cjir.745.

Burkle, F. M., K. Goniewicz, and A. Khorram-Manesh. 2022. "Bastardizing Peacekeeping and the Birth of Hybrid Warfare." Prehospital and Disaster Medicine 37(2): 147–149. https://doi.org/10.1017/S1049023X22000425.

Canadian Armed Forces. 2025. Cyber Operator. Ottawa, ON: Canadian Armed Forces. Accessed 17 January 2025 at https://forces.ca/en/career/cyber-operator/.

Canadian Army. 2025. Psychological Operations. Ottawa, ON: Canadian Army. Accessed 4 January 2025 at https://www.canada.ca/en/army/corporate/5-canadian-division/5-canadian-division-influence-activities/psychological-operations.html.

Canadian Centre for Cyber Security. 2022. An Introduction to the Cyber Threat Environment. Ottawa, ON: Canadian Centre for Cyber Security. Accessed 12 December 2024 at https://www.cyber.gc.ca/en/guidance/introduction-cyber-threat-environment.

Canadian Centre for Cyber Security. 2024. National Cyber Threat Assessment 2025–2026. Ottawa, ON: Canadian Centre for Cyber Security. Accessed 6 January 2025 at https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2025-2026.

Carment, D. and D. Belo. 2018. War's Future: The Risks and Rewards of Grey Zone Conflict and Hybrid Warfare. Calgary: Canadian Global Affairs Institute. ISBN: 9781773970431.

Chung, Y. 2021. "Hybrid Challenges in the PRC's Novel Public Opinion Warfare." Pacific Focus 36(3): 405–426. https://doi.org/10.1111/pafo.12194.

Communications Security Intelligence Service. 2021. Foreign Interference: Threats to Canada's Democratic Process. Ottawa, ON: Communications Security Intelligence Service. Accessed 14 December 2024 at

https://www.canada.ca/en/security-intelligence-service/corporate/publications/foreign-interference-threat-to-canadas-democratic-process.html#toc2

Communications Security Establishment. 2023. Cyber Operations. Ottawa, ON: Communications Security Establishment. Accessed 15 December 2024 at https://www.cse-cst.gc.ca/en/mission/cyber-operations.

Cybersecurity & Infrastructure Security Agency. 2025a. Foreign Influence Operations and Disinformation. Washington, D.C.: Cybersecurity & Infrastructure Security Agency. Accessed 15 January 2025 at https://www.cisa.gov/topics/election-security/foreign-influence-operations-and-disinformation.

Cybersecurity & Infrastructure Security Agency. 2025b. Tactics of Disinformation. Washington, D.C.: Cybersecurity & Infrastructure Security Agency. Accessed 5 January 2025 at https://www.cisa.gov/sites/default/files/publications/tactics-of-disinformation_508.pdf.

Department of Defence. 2020. 2020 Defence Strategic Update. Canberra, AU: Department of Defence. Accessed 6 January 2025 at https://www.defence.gov.au/about/strategic-planning/2020-defence-strategic-update.

Department of Defence. 2024. National Defence Strategy. Canberra, AU: Department of Defence. Accessed 3 January 2025 at https://www.minister.defence.gov.au/media-releases/2024-04-17/2024-national-defence-strategy.

Department of Defence. 2025. People's Liberation Army–Navy (PLA–N) Vessels Operating Near Australia. Canberra, AU: Department of Defence. Accessed 10 March 2025 at https://www.defence.gov.au/news-events/news/2025-03-09/peoples-liberation-army-navy-vessels-operating-near-australia.

Department of Foreign Affairs and Trade. 2017. Guarding Against Foreign Interference. Canberra, AU: Department of Foreign Affairs and Trade. Accessed 17 January 2025 at https://www.dfat.gov.au/sites/default/files/minisite/static/4ca0813c-585e-4fe1-86eb-de665e65001a/fpwhitepaper/foreign-policy-white-paper/chapter-five-keeping-australia-and-australians-safe-secure-and-free-0.html.

Department of Home Affairs. 2024a. Countering Foreign Interference. Canberra, AU: Department of Home Affairs. Accessed 4 December 2024 at https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/countering-foreign-interference.

Department of Home Affairs. 2024b. Countering Foreign Interference in Australia. Canberra, AU: Department of Home Affairs. Accessed 20 December 2024 at https://www.homeaffairs.gov.au/nat-security/files/cfi-australia.pdf.

Department of Home Affairs. 2024c. Defining Foreign Interference. Canberra, AU: Department of Home Affairs. Accessed 7 January 2025 at https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/countering-foreign-interference/defining-foreign-interference.

Department of Justice Canada. 2024. What We Heard: Consultation on the Proposed Reforms to the Security of Information Act, Criminal Code and Canada Evidence Act. Ottawa, ON: Department of Justice Canada. Accessed 13 December 2024 at https://www.justice.gc.ca/eng/cons/fi-ie/wwh-qne.html.

Department of Justice Canada. 2025. Foreign Influence Transparency and Accountability Act S.C. 2024, c. 16, s. 113. Justice Laws Website. Ottawa, ON: Department of Justice Canada. Accessed 8 January 2025 at https://lois.justice.gc.ca/eng/acts/F-29.2/FullText.html.

Department of National Defence. 2017. Strong, Secure, Engaged: Canada's Defence Policy. Ottawa, ON: Department of National Defence Canada. Accessed 22 December 2024 at https://www.canada.ca/en/department-national-defence/corporate/reports-publications/canada-defence-policy.html.

Department of National Defence. 2020. CANSOFCOM – Beyond the Horizon. Ottawa, ON: Department of National Defence Canada. Accessed 16 January 2025 at https://www.canada.ca/en/department-national-defence/corporate/reports-publications/cansofcom-beyond-horizon.html.

Department of National Defence. 2024. Our North, Strong and Free: A Renewed Vision for Canada's Defence. Ottawa, ON: Department of National Defence Canada. Accessed 3 January 2025 at https://www.canada.ca/en/department-national-defence/corporate/reports-publications/north-strong-free-2024.html.

Department of the Prime Minister and Cabinet. 2022. Countering Foreign Interference. Wellington, New Zealand: Department of the Prime Minister and Cabinet.

Accessed 3 January 2025 at https://www.dpmc.govt.nz/our-programmes/national-security/countering-foreign-interference.

Department of the Prime Minister and Cabinet. 2023. Secure Together. Wellington, New Zealand: Department of the Prime Minister and Cabinet. Accessed 7 January 2025 at https://www.dpmc.govt.nz/sites/default/files/2023-11/national-security-strategy-aug2023.pdf.

Department of the Prime Minister and Cabinet. 2024. Strengthening resilience to disinformation. Wellington, New Zealand: Department of the Prime Minister and Cabinet. Accessed 7 January 2025 at https://www.dpmc.govt.nz/our-programmes/national-security/strengthening-resilience-disinformation.

Digital and Population Data Services Agency. 2025. The Finnish Border Guard. Helsinki, Finland: Digital and Population Data Services Agency. Accessed 12 January 2025 at https://www.suomi.fi/organization/the-finnish-border-guard/6264913c-7deb-4460-a8cc-0076dc4c3b50.

European Commission. 2025. Cyber Resilience Act. Digital Strategy. Brussels, Belgium: European Union. Accessed 16 January 2025 at https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act.

Federal Bureau of Investigation. 2024. Combating Foreign Influence. Washington, D.C.: FBI. Accessed 1 December 2024 at https://www.fbi.gov/investigate/counterintelligence/foreign-influence.

Federal Bureau of Investigation. 2025. Combating Foreign Influence. Washington, D.C.: FBI. Accessed 13 January 2025 at https://www.fbi.gov/investigate/counterintelligence/foreign-influence.

Finnish Border Guard. 2025a. EU-HybNet Project. Helsinki, Finland: Finnish Border Guard. Accessed 8 January 2025 at https://raja.fi/en/eu-hybnet-project.

Finnish Border Guard. 2025b. The Finnish Border Guard. Suomi.fi. Helsinki, Finland: Finnish Border Guard. Accessed 16 January 2025 at https://www.suomi.fi/organization/the-finnish-border-guard/6264913c-7deb-4460-a8cc-0076dc4c3b50.

Finnish Defence Forces. 2025. Countering Cyber Threats Calls for International Cooperation and Training. Helsinki, Finland: Finnish Defence Forces. Accessed 4 January 2025 at https://puolustusvoimat.fi/en/-/countering_cyber_threats_calls_for_international_cooperation_and_training.

Finnish Security and Intelligence Service. 2025. Intelligence and Influence Operations Are Targeting Finland. Helsinki, Finland: Finnish Security and Intelligence Service. Accessed 10 January 2025 at https://supo.fi/en/intelligence-and-influence-operations.

Fridman, O. 2018. Russian "Hybrid Warfare": Resurgence and Politicization. Oxford: Oxford University Press. https://doi.org/10.1093/oso/9780190877378.001.0001.

Global Affairs Canada. 2023. G7 Rapid Response Mechanism Annual Report 2022. Ottawa, ON: Global Affairs Canada. Accessed 11 December 2024 at https://www.international.gc.ca/transparency-transparence/rapid-response-mechanism-mecanisme-reponse-rapide/2022-annual-report-rapport-annuel.aspx?lang=eng.

Government Communication Service. RESIST 2 Counter Disinformation Toolkit. London, UK: Government Communication Service. Accessed 8 January 2025 at https://gcs.civilservice.gov.uk/publications/resist-2-counter-disinformation-toolkit.

Granholm, F., D. Tin, and G. R. Ciottone. 2022. "Not War, Not Terrorism: The Impact of Hybrid Warfare on Emergency Medicine." American Journal of Emergency Medicine 62: 96–100. https://doi.org/10.1016/j.ajem.2022.10.021.

Hoffman, F. G. 2007. Conflict in the 21st Century: The Rise of Hybrid Wars. Arlington, VA: Potomac Institute for Policy Studies. https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf.

Home Office. 2024a. Foreign Influence Registration Scheme Factsheet. London, United Kingdom: Home Office. Accessed 6 January 2025 at https://www.gov.uk/government/publications/national-security-bill-factsheets/foreign-influence-registration-scheme-factsheet.

Home Office. 2024b. Foreign Interference: National Security Bill Factsheet. London, United Kingdom: Home Office. Accessed 15 December 2024 at https://www.gov.uk/government/publications/national-security-bill-factsheets/foreign-interference-national-security-bill-factsheet.

Huber, T. M. 2002. Compound Warfare: That Fatal Knot. Fort Leavenworth, KS: U.S. Army Command and General Staff College Press.

https://www.armyupress.army.mil/Portals/7/combat-studies-institute/csi-books/compound_warfare.pdf.

Ito, R. 2022. "Hybrid Balancing as Classical Realist Statecraft: China's Balancing Behaviour in the Indo-Pacific." International Affairs 98(6): 1959–1975. https://doi.org/10.1093/ia/iiac214.

Jackson, N. 2019. "Deterrence, Resilience and Hybrid Wars: The Case of Canada and NATO." Journal of Military and Strategic Studies 19(4): 104–125. ISSN: 1488-559X.

Janicatova, S. and Mlejnkova. 2021. "The Ambiguity of Hybrid Warfare: A Qualitative Content Analysis of the United Kingdom's Political-Military Discourse on Russia's Hostile Activities." Contemporary Security Policy 42(3): 312–344. https://doi.org/10.1080/13523260.2021.1885921.

Justice and Community Safety Directorate. 2024. Countering Foreign Interference. Canberra, AU: Justice and Community Safety Directorate. Accessed 13 December 2024 at https://www.justice.act.gov.au/security-and-emergency-management/countering-foreign-interference.

Lanoszka, A. 2016. "Russian Hybrid Warfare and Extended Deterrence in Eastern Europe." International Affairs 92(1): 175–195. https://doi.org/10.1111/1468-2346.12509.

Lind, W. S. and G. A. Thiele. 2015. 4th Generation Warfare Handbook. Kouvola, Finland: Castalia House. ISBN: 9789527065754.

MI5. 2025. Countering State Threats. London, United Kingdom: MI5. Accessed 4 January 2025 at https://www.mi5.gov.uk/what-we-do/countering-state-threats.

Ministry for Ethnic Communities. 2024. Foreign Interference Harms the Rights and Freedoms of People in New Zealand. Wellington, New Zealand: Ministry for Ethnic Communities. Accessed 13 December 2024 at https://www.ethniccommunities.govt.nz/programmes/security-and-resilience/foreign-interference-harms-the-rights-and-freedoms-of-people-in-new-zealand/.

Ministry for Ethnic Communities. 2025. The Government is Changing the Law to Protect New Zealand from Foreign Interference. Wellington, New Zealand: Ministry for Ethnic Communities. Accessed 10 January 2025 at

https://www.ethniccommunities.govt.nz/programmes/security-and-resilience/crimes-act-amendment/.

Ministry for Foreign Affairs. 2025a. Cyber Security and the Cyber Domain. Helsinki, Finland: Ministry for Foreign Affairs. Accessed 7 January 2025 at https://um.fi/cyber-security-and-the-cyber-domain.

Ministry for Foreign Affairs. 2025b. Educated Decisions: Finnish Media Literacy Deters Disinformation. Helsinki, Finland: Ministry for Foreign Affairs. Accessed 1 January 2025 at https://finland.fi/life-society/educated-decisions-finnish-media-literacy-deters-disinformation/.

Ministry of Defence. 2014. Allied Joint Doctrine for Psychological Operations. London, United Kingdom: Ministry of Defence. Accessed 8 December 2024 at https://assets.publishing.service.gov.uk/media/5a80ce48e5274a2e87dbbecb/20150223-AJP_3_10_1_PSYOPS_with_UK_Green_pages.pdf.

Ministry of Defence. 2021. Integrated Operating Concept. London, United Kingdom: Ministry of Defence. Accessed 13 January 2025 at https://assets.publishing.service.gov.uk/media/612f91b28fa8f50328e2c8f5/Integrated_Operating_Concept_2025.pdf.

Ministry of Defence. 2023. Annual Report and Accounts 2022–23. London, United Kingdom: Ministry of Defence. Accessed 3 January 2025 at https://assets.publishing.service.gov.uk/media/64b91b2d06f78d000d7425b4/MoD_Annual_Report_and_Accounts_2022-23.pdf.

Ministry of Defence. 2024. Government Defence Report. Helsinki, Finland: Ministry of Defence. Accessed 3 January 2025 at https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/166004/PLM_2024_7.pdf?sequence=4&isAllowed=y.

Ministry of Justice. 2018. Regeringens Proposition till Riksdagen med Förslag till Lagar om Ändring av Gränsbevakningslagen och Utlänningslagen och till Vissa Lagar som har Samband med Dem (HE 201/2017). Finlex. Helsinki, Finland: Ministry of Justice. Accessed 11 December 2024 at https://www.finlex.fi/en/government-proposals/2017/201.

Ministry of Justice. 2022. Hallituksen Esitys Eduskunnalle Laeiksi Väliaikaisesta Poikkeamisesta Ulkomaalaislaista ja Turvapaikkalaista sekä Eräiksi Niihin Liittyviksi Laeiksi (HE 193/2022). Finlex. Helsinki, Finland: Ministry of Justice.

Accessed 5 January 2025 at https://www.finlex.fi/fi/hallituksen-esitykset/2022/193.

Ministry of Justice. 2025. Countering Foreign Interference. Wellington, New Zealand: Ministry of Justice. Accessed 1 January 2025 at https://www.justice.govt.nz/justice-sector-policy/key-initiatives/countering-foreign-interference/.

Ministry of the Interior. 2017. Rajavartijoiden Toimivaltuuksiin Laajennuksia Hybridiuhkiin Vastaamiseksi [Expansion of Border Guard Powers to Respond to Hybrid Threats]. Helsinki, Finland: Ministry of the Interior. Accessed 6 January 2025 at https://intermin.fi/-/rajavartijoiden-toimivaltuuksiin-laajennuksia-hybridiuhkiin-vastaamiseksi?languageId=en_US.

Ministry of the Interior. 2018. Rajavartiolaitoksen Valtuuksia Puuttua Hybridiuhkiin On Tarkoitus Lisätä [Powers of the Finnish Border Guard to Intervene in Hybrid Threats to Be Strengthened]. Helsinki, Finland: Ministry of the Interior. Accessed 15 January 2025 at https://intermin.fi/-/rajavartiolaitoksen-valtuuksia-puuttua-hybridiuhkiin-on-tarkoitus-lisata?languageId=en_US.

Ministry of the Interior. 2019. Rajavartiolaitoksen Valtuuksia Puuttua Hybridiuhkiin Lisätään [Powers of the Finnish Border Guard to Intervene in Hybrid Threats to Be Strengthened]. Helsinki, Finland: Ministry of the Interior. Accessed 30 December 2024 at https://intermin.fi/-/rajavartiolaitoksen-valtuuksia-puuttua-hybridiuhkiin-lisataan?languageId=en_US.

Ministry of the Interior. 2025a. Government Programme Measures to Reform Border Security. Helsinki, Finland: Ministry of the Interior. Accessed 17 January 2025 at https://intermin.fi/en/border-management/government-programme-measures-to-reform-border-security.

Ministry of the Interior. 2025b. Finland and NATO. Helsinki, Finland: Ministry of the Interior. Accessed 1 January 2025 at https://intermin.fi/en/current-issues/finland-and-nato.

Ministry of the Interior. 2025c. Hybrid Threats and Hybrid Influence Activities. Helsinki, Finland: Ministry of the Interior. Accessed 2 January 2025 at https://intermin.fi/en/national-security/hybrid-threats.

Ministry of the Interior. 2025d. Hybridiuhat. Helsinki, Finland: Ministry of the Interior. Accessed 13 January 2025 at https://intermin.fi/hybridiuhat.

Multinational Capability Development Campaign. 2017. MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare. Multinational Capability Development Campaign. London, United Kingdom: Government of the United Kingdom. Accessed 2 January 2025 at https://assets.publishing.service.gov.uk/media/5a8228a540f0b62305b92caa/dar_mcdc_hybrid_warfare.pdf.

Multinational Capability Development Campaign. 2018. Hybrid Warfare and Its Countermeasures. Multinational Capability Development Campaign. London, United Kingdom: Government of the United Kingdom. Accessed 20 December 2024 at https://assets.publishing.service.gov.uk/media/5b2906b4ed915d2cc681ac94/MCDC_CHW_Information_Note-Hybrid_Warfare_and_its_Countermeasures-March_2018.pdf.

Multinational Capability Development Campaign. 2019. MCDC Countering Hybrid Warfare Project: March 2019 Countering Hybrid Warfare. Multinational Capability Development Campaign. London, United Kingdom: Government of the United Kingdom. Accessed 14 January 2025 at https://assets.publishing.service.gov.uk/media/5c8141e2e5274a2a51ac0b34/concepts_mcdc_countering_hybrid_warfare.pdf/.

Murray, W. and R. Mansoor. 2012. Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present. Cambridge: Cambridge University Press. https://doi.org/10.1017/CBO9781139199254.

Nasu, H. 2019. "Challenges of Hybrid Warfare to the Implementation of International Humanitarian Law in the Asia-Pacific." In Asia-Pacific Perspectives on International Humanitarian Law, ed. S. Linton, T. McCormack, and S. Sivakumaran, 220–230. Cambridge: Cambridge University Press. ISBN: 1108497241.

National Cyber Force. 2025. About Us. London, United Kingdom: National Cyber Force. Accessed 2 January 2025 at https://www.gov.uk/government/organisations/national-cyber-force/about.

National Cyber Security Centre Finland. 2025. Kyberkestävyyssäädös (Cyber Resilience Act, CRA). Helsinki, FL: National Cyber Security Centre Finland. Accessed 7 January 2025 at https://kyberturvallisuuskeskus.fi/en/toimintamme/saantely-ja-valvonta/kyberkestavyyssaados-cyber-resilience-act-cra.

National Cyber Security Centre. 2022. Cyber Threat Report 2021/2022. Wellington, New Zealand: National Cyber Security Centre. Accessed 22 December 2024 at https://www.ncsc.govt.nz/assets/NCSC-Documents/2021-2022-Cyber-Threat-Report.pdf.

National Cyber Security Centre. 2023. Cyber Threat Report 2022/2023. Wellington, New Zealand: National Cyber Security Centre. Accessed 8 January 2025 at https://www.ncsc.govt.nz/resources/ncsc-annual-cyber-threat-reports/2023-web.

National Cyber Security Centre. 2024. UK and Allies Expose Cyber Campaign of Attempted Political Interference. London, United Kingdom: NCSC. Accessed 10 January 2025 at https://www.ncsc.gov.uk/news/uk-and-allies-expose-cyber-campaign-attempted-political-interference.

National Intelligence Council. 2021. Foreign Threats to the 2020 US Federal Elections. Washington, D.C.: NIC. Accessed 14 January 2025 at https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf.

National Intelligence Council. 2024a. Conflict in the Gray Zone: A Prevailing Geopolitical Dynamic Through 2030. Washington, D.C.: NIC. Accessed 2 January 2025 at https://www.dni.gov/files/ODNI/documents/assessments/NIC-Unclassified-Conflict-In-The-Gray-Zone-July2024.pdf.

National Intelligence Council. 2024b. Updated IC Gray Zone Lexicon: Key Terms and Definitions. Washington, D.C.: NIC. Accessed 11 December 2024 at https://www.dni.gov/files/ODNI/documents/assessments/NIC-Unclassified-Updated-IC-Gray-Zone-Lexicon-July2024.pdf.

National Security Agency/Central Security Service. 2022. How NSA, U.S. Cyber Command Are Defending Midterm Elections: One Team, One Fight. Washington, D.C.: NSA/CSS. Accessed 8 January 2025 at https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/3136987/how-nsa-us-cyber-command-are-defending-midterm-elections-one-team-one-fight.

National Security and Intelligence Committee of Parliamentarians. 2023. Special Report on Federal Policing Mandate of the Royal Canadian Mounted Police. Ottawa,

ON: National Security and Intelligence Committee of Parliamentarians. Accessed 9 December 2024 at https://www.nsicop-cpsnr.ca/reports/rp-2023-11-fp/RCMP_FP_report_EN.pdf.

National Security and Intelligence Committee of Parliamentarians. 2024a. National Security and Intelligence Committee of Parliamentarians Annual Report 2023. Ottawa, ON: National Security and Intelligence Committee of Parliamentarians. Accessed 10 January 2025 at https://www.nsicop-cpsnr.ca/reports/rp-2024-ar-2023/nsicop-2023-ar-en.pdf.

National Security and Intelligence Committee of Parliamentarians. 2024b. Special Report on Foreign Interference in Canada's Democratic Processes and Institutions. Ottawa, ON: National Security and Intelligence Committee of Parliamentarians. Accessed 5 January 2025 at https://www.nsicop-cpsnr.ca/reports/rp-2024-06-03/special-report-foreign-interference.pdf.

Naval Postgraduate School. 2025. Center on Combating Hybrid Threats. Monterey, CA: Naval Postgraduate School. Accessed 3 January 2025 at https://nps.edu/web/ccht.

New Zealand Defence Force. 2017. Future Land Operating Concept 2035. Wellington, New Zealand: New Zealand Defence Force. Accessed 14 December 2024 at https://www.nzdf.mil.nz/assets/Uploads/DocumentLibrary/Future-Land-Operating-Concept-2035-1.pdf.

New Zealand Defence Force. 2023. Annual Report 2023. Wellington, New Zealand: New Zealand Defence Force. Accessed 17 January 2025 at https://www.nzdf.mil.nz/assets/Uploads/DocumentLibrary/NZDF-Annual-Report-2023.PDF.

New Zealand Government. 2024. Protecting New Zealand from Foreign Interference. Wellington, New Zealand: New Zealand Government. Accessed 11 January 2025 at https://www.beehive.govt.nz/release/protecting-new-zealand-foreign-interference.

New Zealand Security Intelligence Service. 2025. Countering Espionage and Foreign Interference. Wellington, New Zealand: New Zealand Security Intelligence Service. Accessed 1 January 2025 at https://www.nzsis.govt.nz/our-work/countering-espionage-and-foreign-interference.

North Atlantic Treaty Organization. 2024. Countering Hybrid Threats. Brussels, Belgium: North Atlantic Treaty Organization. Accessed 6 January 2025 at https://www.nato.int/cps/en/natohq/topics_156338.htm.

Ong, W. 2018. "The Rise of Hybrid Actors in the Asia-Pacific." Pacific Review 31(6): 740–761. https://doi.org/10.1080/09512748.2018.1513549.

Parliament of Australia. 2023. Senate Select Committee on Foreign Interference Through Social Media. Canberra, AU: Parliament of Australia. Accessed 12 December 2024 at https://www.aph.gov.au/select_foreign_interference.

Parliament of Australia. 2025. Chapter 2 – Foreign Interference in Australia. Canberra, AU: Parliament of Australia. Accessed 3 January 2025 at https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Foreign_Interference_through_Social_Media/ForeignInterference47/Report/Chapter_2_-_Foreign_interference_in_Australia.

Paterson, T. and L. Hanley. 2020. "Political Warfare in the Digital Age: Cyber Subversion, Information Operations and 'Deep Fakes.'" Australian Journal of International Affairs 74(4): 439–454. https://doi.org/10.1080/10357718.2020.1734772.

Prime Minister's Office. 2016. Government Report on Finnish Foreign and Security Policy. Helsinki, Finland: Prime Minister's Office. Accessed 9 January 2025 at https://valtioneuvosto.fi/documents/10616/1986338/VNKJ092016+en.pdf.

Prime Minister's Office. 2025. Overview of Information Influence Activities. Helsinki, Finland: Prime Minister's Office. Accessed 9 January 2025 at https://valtioneuvosto.fi/en/government-communications/overview-of-information-influence-activities?gsid=0c7a8cee-84c0-44c1-b5e3-09bef4c56ce1.

Protective Security Requirements. 2025. Protection Against Foreign Interference. Wellington, New Zealand: Protective Security Requirements. Accessed 5 January 2025 at https://www.protectivesecurity.govt.nz/resources/campaigns/protection-against-foreign-interference.

Public Safety Canada. 2022. Public Safety Canada Departmental Plan 2022–23. Ottawa, ON: Public Safety Canada. Accessed 13 January 2025 at https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/dprtmntl-pln-2022-23/index-en.aspx.

Public Safety Canada. 2023a. Public Safety Canada Departmental Plan 2023–24. Ottawa, ON: Public Safety Canada. Accessed 15 January 2025 at https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/dprtmntl-pln-2023-24/index-en.aspx.

Public Safety Canada. 2023b. What We Heard Report: Consulting Canadians on the Merits of a Foreign Influence Transparency Registry. Ottawa, ON: Public Safety Canada. Accessed 17 December 2024 at https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2023-nhncng-frgn-nflnc-wwh/index-en.aspx.

Public Safety Canada. 2024a. Canada's Foreign Influence Transparency Registry. Ottawa, ON: Public Safety Canada. Accessed 12 January 2025 at https://www.canada.ca/en/public-safety-canada/news/2024/05/canadas-foreign-influence-transparency-registry.html.

Public Safety Canada. 2024b. CSIS Act Amendments: Bolstering Canada's Counter-Foreign Interference Legislation. Ottawa, ON: Public Safety Canada. Accessed 20 December 2024 at https://www.canada.ca/en/public-safety-canada/news/2024/05/csis-act-amendments-bolstering-canadas-counter-foreign-interference-legislation.html.

Public Safety Canada. 2024c. Five Country Ministerial. Accessed 1 December 2024 at https://www.publicsafety.gc.ca/cnt/ntnl-scrt/fv-cntry-mnstrl-en.aspx.

Public Safety Canada. 2024d. Foreign Interference and Canada. Ottawa, ON: Public Safety Canada. Accessed 30 December 2024 at https://www.canada.ca/en/public-safety-canada/news/2024/05/foreign-interference-and-canada.html.

Public Safety Canada. 2024e. Foreign Interference. Ottawa, ON: Public Safety Canada. Accessed 28 December 2024 at https://www.publicsafety.gc.ca/cnt/ntnl-scrt/frgn-ntrfrnc/index-en.aspx.

Public Safety Canada. 2024f. Government Introduces Legislation to Counter Foreign Interference. Ottawa, ON: Public Safety Canada. Accessed 7 January 2025 at https://www.canada.ca/en/public-safety-canada/news/2024/05/government-introduces-legislation-to-counter-foreign-interference.html.

Public Safety Canada. 2024g. Modernizing Canada's Toolkit to Counter Foreign Interference: An Act Respecting Countering Foreign Interference. Ottawa, ON:

Public Safety Canada. Accessed 11 January 2025 at https://www.publicsafety.gc.ca/cnt/ntnl-scrt/frgn-ntrfrnc/mdrnzng-tlkt-frgn-ntrfrnc-en.aspx.

Public Safety Canada. 2024h. Public Safety Canada Departmental Plan 2024–25. Ottawa, ON: Public Safety Canada. Accessed 5 December 2024 at https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/dprtmntl-pln-2024-25/index-en.aspx.

Public Safety Canada. 2024i. Security of Information Act, Criminal Code and Canada Evidence Act Amendments: Bolstering Canada's Counter-Foreign Interference Legislation. Ottawa, ON: Public Safety Canada. Accessed 2 January 2025 at https://www.canada.ca/en/public-safety-canada/news/2024/05/security-of-information-act-criminal-code-and-canada-evidence-act-amendments-bolstering-canadas-counter-foreign-interference-legislation.html.

Public Safety Canada. 2024j. What We Heard and Learned Report: CSIS Act Consultations. Ottawa, ON: Public Safety Canada. Accessed 21 December 2024 at https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/csis-cnslttns/index-en.aspx.

Qiao, L. and X. Wang. 1999. Unrestricted Warfare. Beijing: PLA Literature and Arts Publishing House. https://www.c4i.org/unrestricted.pdf.

Richey, M. 2018. "Contemporary Russian Revisionism: Understanding the Kremlin's Hybrid Warfare and the Strategic and Tactical Deployment of Disinformation." Asia Europe Journal 16(1): 101–113. https://doi.org/10.1007/s10308-017-0482-5.

Stănescu, M. 2023. "Understanding Hybrid Threats and Their Societal Impact—Republic of Moldova Case Study." Land Forces Academy Review 28(4): 255–264. https://doi.org/10.2478/raft-2023-0030.

SUPO (Finnish Security and Intelligence Service). 2024. The Threat of Russian Intelligence and Malign Influence Remains Elevated in Finland. Helsinki, Finland: SUPO. Accessed 14 January 2025 at https://supo.fi/en/-/the-threat-of-russian-intelligence-and-malign-influence-remains-elevated-in-finland.

The Senate. 2023. Select Committee on Foreign Interference Through Social Media. Canberra, AU: The Senate. Accessed 22 December 2024 at https://parlinfo.aph.gov.au/parlInfo/download/committees/reportsen/RB000

062/toc_pdf/SenateSelectCommitteeonForeignInterferencethroughSocialMedia.pdf.

Thompson, J. 2022. "Hybrid Warfare: Redefining and Responding to Hostile Intent." Canadian Military Journal 22(3): 62–70. ISSN: 1492-465X.

UK Legislature. 2023. National Security Act 2023. London, United Kingdom: National Archives. Accessed 19 December 2024 at https://www.legislation.gov.uk/ukpga/2023/32/part/1/crossheading/foreign-interference.

UK Parliament Defence Committee. 2023. Former MI6 Chief Sir Alex Younger to Discuss Grey Zone Threats, 10 October. London, United Kingdom: UK Parliament Defence Committee. Accessed 11 December 2024 at https://committees.parliament.uk/committee/24/defence-committee/news/204781/former-mi6-chief-sir-alex-younger-to-discuss-grey-zone-threats/.

UK Parliament. 2024. Elections: Foreign Interference, 29 July. London, United Kingdom: UK Parliament. Accessed 1 December 2024 at https://hansard.parliament.uk/Commons/2024-07-29/debates/E3A0F9FA-7831-4971-BE5F-2AB14D40A7D0/ElectionsForeignInterference.

UK Parliament. 2025. Ukraine: Frozen Russian Assets, 26 February. London, United Kingdom: UK Parliament. Accessed 17 January 2025 at https://hansard.parliament.uk/Lords/2025-02-26/debates/91CA1E59-8985-40C3-A5FD-1E7305114E64/UkraineFrozenRussianAssets.

United States Army Cyber Command. 2025. Operate, Defend, Attack, Influence, Inform!. Washington, D.C.: Army Cyber Command. Accessed 5 December 2024 at https://www.arcyber.army.mil/#:~:text=U.S.%20Army%20Cyber%20Command%20integrates,the%20same%20to%20our%20adversaries.

United States Army. 2023. Fiscal Year 2023 Annual Financial Report. Washington, D.C.: U.S. Army. Accessed 7 January 2025 at https://www.asafm.army.mil/portals/72/Documents/Audit/fy23afr.pdf.

United States Army. 2025. Psychological Operations. Washington, D.C.: U.S. Army. Accessed 19 December 2024 at https://www.goarmy.com/careers-and-jobs/specialty-careers/special-ops/psychological-operations.

United States Congress. 2017. The Evolution of Hybrid Warfare and Key Challenges. 115th Congress. Accessed 22 December 2024 at https://www.congress.gov/event/115th-congress/house-event/105746/text.

United States Congress. 2019. S.1469 – Prevention of Foreign Interference with Elections Act of 2019. 116th Congress. Accessed 13 December 2024 at https://www.congress.gov/bill/116th-congress/senate-bill/1469/text.

United States Congress. 2022. S.3600 – Strengthening American Cybersecurity Act of 2022. 117th Congress. Accessed 27 December 2024 at https://www.congress.gov/bill/117th-congress/senate-bill/3600.

United States Congress. 2023. H.R.4690 – Gray Zone Defense Assessment Act. 118th Congress. Accessed 18 December 2024 at https://www.congress.gov/bill/118th-congress/house-bill/4690/text.

United States Congress. 2024a. H.R.8314 – No Foreign Election Interference Act. 118th Congress. Accessed 10 January 2025 at https://www.congress.gov/bill/118th-congress/house-bill/8314.

United States Congress. 2024b. S.4145 – Preventing Foreign Interference in American Elections Act. 118th Congress. Accessed 6 January 2025 at https://www.congress.gov/bill/118th-congress/senate-bill/4145.

United States Department of Defense. 2005. The National Defense Strategy of the United States of America. Accessed 14 January 2025 at https://history.defense.gov/Portals/70/Documents/nds/2005_NDS.pdf?ver=tFA4Qqo94ZB0x_S6uL0QEg%3D%3D.

United States Department of Homeland Security. 2018. Foreign Interference Taxonomy. Washington, D.C.: U.S. Department of Homeland Security. Accessed 12 January 2025 at https://www.cisa.gov/sites/default/files/publications/19_0717_cisa_foreign-influence-taxonomy.pdf.

United States Department of Homeland Security. 2023. Key Findings and Recommendations… Related to the 2022 US Federal Elections. Washington, D.C.: U.S. Department of Homeland Security. Accessed 4 January 2025 at https://www.dhs.gov/publication/key-findings-and-recommendations-foreign-interference-related-2022-us-federal-elections.

United States Department of Justice and U.S. Department of Homeland Security. 2021. Key Findings and Recommendations… Related to the 2020 US Federal Elections. Washington, D.C.: U.S. DOJ and U.S. DHS. Accessed 9 January 2025 at https://www.justice.gov/opa/press-release/file/1376761/dl.

United States Department of Justice. 2019. Report on the Investigation into Russian Interference in the 2016 Presidential Election. Washington, D.C.: DOJ. Accessed 16 December 2024 at https://www.justice.gov/archives/sco/file/1373816/dl.

United States Department of Justice. 2023. Joint Statement on the 2022 U.S. Mid-Term Election. Washington, D.C.: Department of Justice. Accessed 20 December 2024 at https://www.justice.gov/opa/pr/joint-statement-departments-justice-and-homeland-security-assessing-impact-foreign-0.

United States Department of Justice. 2024. Foreign Agents Registration Act. Washington, D.C.: DOJ. Accessed 17 January 2025 at https://www.justice.gov/nsd-fara.

United States Department of the Treasury. 2024. Treasury Takes Action… Russia's Foreign Malign Influence Operations. Washington, D.C.: Department of the Treasury. Accessed 6 January 2025 at https://home.treasury.gov/news/press-releases/jy2559.

United States Special Operations Command. 2023. FY 2023 USSOCOM Financial Statement Reporting Package. Washington, D.C.: USSOCOM. Accessed 9 January 2025 at https://www.socom.mil/Documents/FY2023%20USSOCOM%20Financial%20Statement%20Reporting%20Package.pdf.

Wegge, N. and T. Wetzling. 2020. "Countering Hybrid Threats Through Signals Intelligence and Big Data Analysis?" In International Relations in the 21st Century, ed. T. Røseth and J. M. Weaver, 69–88. Cham: Palgrave Macmillan. https://doi.org/10.1007/978-3-030-34004-9_4.

Yin, R. K. 2018. Case Study Research: Design and Methods (6th ed.). Los Angeles: SAGE Publishing. ISBN 9781506336169.

MH
MAGISTER HUBUNGAN INTERNASIONAL

http://ejournal.fisip.unjani.ac.id/