STRATEGIC STUDIES QUARTERLY - PAR AVION

Comprehensive Security Approach in Response to Russian Hybrid Warfare

Lt Col Tuukka Elonheimo, Finnish Air Force

Abstract

This article assesses why open, digitalized Western democracies are prone to hybrid warfare and analyzes versatile overt and covert mixed warfare methods in the modern information-dependent and interconnected environment. It also draws on various hybrid warfare influence methods and explains the broader concept and essence of Russian hybrid warfare. Besides analyzing structural hybrid warfare challenges, the article assesses and proposes means and practices to mitigate, act against, and deter overt or covert hybrid offensives. The article argues that Russian mixed warfare methods in tandem create a potential threat to Western democracies' unity and decision-making. However, these Western states could mitigate and prevent the implications of hybrid warfare by increasing comprehensive security, cooperation, situational awareness, preparedness, and resilience. The article identifies that the combined use of proper coordination, cooperation, information sharing, education, and readiness among authorities, governmental and nongovernmental organizations, businesses, and citizens could diminish these multifaceted, ambiguous hybrid aggressions.

*****

Introduction

Deception, asymmetrical methods, and propaganda have been part of Russia's warfare and strategic mindset for centuries. After the Cold War, the US and NATO shifted to counterinsurgency operations, and the global war on terrorism became synonymous with "endless wars."[1] In contrast, Russia and China have increased their relative status in strategic competition and learned to use all national power instruments—diplomatic, information, military, and economic (DIME)—in tandem.[2] Russia has narrowed the technological gap with Western militaries in conventional warfare and blatantly increased clandestine operations below the armed conflict level. Since the Russian asymmetric approach combines a wide variety of traditional and nontraditional war-fighting methods, many Western sources have defined it as "hybrid warfare."[3]

Manifold hybrid warfare attacks challenge Western democracies' cohesion, decision-making, and cooperation by creating a wedge with dissonance. Concurrently, strategic leaders, state authorities, and citizens encounter volatile, uncertain, complex, and ambiguous (VUCA) digital environments.[4] Thus, this article examines modern, open democracies' vulnerabilities to malicious Russian hybrid warfare and explains Russian strategies to provide security actors with a framework to make recommendations for increasing readiness, countermeasures, resilience, and deterrence.

Though Russian military literature and the wars against Chechnya and Georgia reveal many characteristics of this new approach, hybrid warfare shocked Westerners when the war broke in 2014.[5] The unmarked "green men" occupying Crimea and harmful cyberattacks against Ukraine's infrastructure were a wake-up call for Western decision-makers.[6] Subsequently, the threat of military invasion, the shoot-down of an airliner, and disinformation campaigns revealed how broad and sneaky hybrid warfare is. Russian clandestine strategies aim to disseminate uncertainty and friction (Clausewitz) in governments' and citizens' daily lives. The strategic fog creates ambiguity in the targeted state, complicating the tracking of the original perpetrator. It enables Russia to conceal its operations in the physical and nonphysical war-fighting domains. Russian hybrid warfare's digital revolution creates complex threats and multifaceted challenges to open Western democracies. However, a comprehensive security approach, cooperation, and joint procedures generate an adequate foundation for increasing resilience, strengthening overall preparedness, mitigating ramifications, and deterring against hybrid offensives. This article first analyzes why contemporary Western societies are vulnerable to the influences of a hybrid strategy and draws on recent events to illustrate Russia's use of hybrid warfare. After describing the instruments of hybrid warfare, the article assesses the essence of Russian hybrid warfare and examines and compares comprehensive security approaches and procedures to mitigate and counter hybrid warfare aggressions. Finally, based on the analysis of Russian hybrid warfare activities, the article recommends actions for security decision-makers to resist and respond to future hybrid warfare.

Vulnerabilities of a Modern Digital Information Society

A lie gets halfway around the world before the truth has a chance to get its pants on.
—Winston Churchill

The digital revolution, global networks, lightspeed information flow, and internet dependency have dramatically changed technological opportunities to influence and manipulate. Additionally, cyber espionage, subversion, and sabotage intensify the digital mess, overwhelm cognition, and complicate decision-making. Faceless hackers conceal their subtle denial-of-service attacks, email phishing, and troll accounts in the shadows of countless bits and clandestine Internet Protocol addresses.[7] Social media applications have become today's spyware, propaganda amplifiers, and nonkinetic weapon platforms. Unfortunately, the human capacity to handle information has not matched the weaponized digital information flow. Consequently, cyberattacks create novel security and privacy problems for governments and citizens. Cold War megaphones and leaflets have changed to cyberattacks and smartphone tweets, spreading without geographic barriers, manipulating opinions, destabilizing cohesion, and shaping targeted states' physical and cognitive environments.[8] In a digital, social-media-oriented society, the spread of confusing fake news, agitating diaspora, and increasingly unhealthy polarization are dangerous weapons to separate people into "us versus them."[9]

The worldwide digital environment increases connectivity and links individuals and organizations to a massive amount of data. However, concurrently, the enormous flow of information—the paradox of plenty—hampers the ability to handle, assess, and comprehend it all. Thus, individuals are losing their focus, attention, and capacity to make circumspect decisions.[10] The cyber domain creates security threats that reveal the weaknesses of open democracies and security organizations.[11] Malware programs, hacking algorithms, facial recognition systems, and cyberattacks enable advanced aggressions against diverse target audiences with low costs from attackers' homes. States with aggressive physical or digital influences can utilize non-state proxy actors to conceal their involvement, making covert approaches tempting.[12] Even if the targeted state could detect, track, and identify the attacker, it might lack the legislative mandate to block and prevent attacks. Identification and attribution are primary deficiencies in the battle against cyber and information warfare.

Artificial intelligence (AI) technology exponentially increases the speed, precision, reach, and efficacy of saturation campaigns.[13] Democratic values, like freedom of speech, restrain and complicate resisting assertive hybrid warfare. Who has the authority to censor gossip or the capacity to protect vital security interests in cyberspace? In a post-truth world, fact-checking organizations, empirical science, and investigative journalism cannot keep pace with exponentially booming fake news and deep fakes.[14] Sneaky adversaries disrupt online banking with denial-of-service attacks, blackmail individuals and organizations with stolen personal emails, and interfere in presidential elections.[15]

Altogether, digitalization, modern communications, and cybersecurity leave plenty of room for Russian hybrid warfare. Indeed, Russia knows how to weaponize the information and combine all-domain asymmetrical warfare to target a wide range of audiences: the military, the government, institutions, media, businesses, individuals, and civil society. Experts at the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) have aptly recognized how the fragmentation of truth, media-industry changes, the hegemony of private media, and new technologies foster hybrid warfare.[16] These information domain trends and risks—combined with open democratic societies' tendency to act by the book concerning norms and rules of law—open the gateway for internal or external aggressors to exploit vulnerabilities.[17] As a concept, hybrid warfare welcomes all these information-era technological developments and tendencies. Overwhelmed by gigabytes of provocative targeted hostile narrative, people and state actors are confused. It is an efficient, easy, and cheap modus operandi.

Russian Hybrid Warfare: Case Studies

> *The most complete and happy victory is this: to compel one's enemy to give up his purpose while suffering no harm oneself.*
>
> —Flavius Belisarius (505–565 CE)

Clausewitz classically argued that war is a continuation of policy by other means. He also stated that the nature of war (primordial violence, hatred, and enmity) does not change, whereas the character of war does.[18] To the same extent, in his book *Every War Must End*, Fred Charles Iklé demonstrates how complicated the rational calculus about wars' gains and losses are before and during the conflict.[19] Since Putin's reign, Russian actions have challenged these traditional principles and theories of war by raising the armed conflict threshold. Is Russia trying to continually shake the balance of war's cost-benefit model, blur the distinction between peace and war, and muddle the distinction among deterrence, persuasion, and coercion?

Truly, Russian hybrid warfare tries to obscure the character of warfare and, more importantly, bring ambiguity, chaos, and friction to day-to-day decision-making, policy formulation, and society's vital functions.[20] The following discusses how Russia's hybrid warfare gray zone intentionally challenges Western state officials, military leaders, and citizens. It also outlines the essence and cumulative effects of hybrid warfare.

Threat or Use of Military Forces

Western media often erroneously relates Russian hybrid warfare to nonmilitary actions instead of hard military power. However, the presence and threat of military capabilities are essential for Russian coercion and hybrid warfare. Russia has aggressively increased its sphere of influence militarily to advance strategic objectives in the European theater over the last decades.[21] Its initiatives include reopened and reconstructed military bases, new weapons systems, an increased military footprint in the Arctic, snap exercises, blue water deployments, show-of-force strategic bomber flights, and force-projection demonstrations. These efforts, along with brutal power military campaigns in Syria and Ukraine, indicate Russia's willingness to use its military instruments to regain regional hegemony.

Anti-access/area denial (A2/AD) capability development has increased worries among NATO, the US, and European Union (EU) states. Though these "keep-out zones" are not impenetrable, Russian long-range missiles and air defense challenge any force projection from Western states.[22] Militarily weaker neighbor states are under constant surveillance and within weapon range. This vulnerability increases pressure, coercion potential, and Russia's capacity to gain a military advantage. Special operation forces and unmarked soldiers occupying Crimea and the subsequent military operations inside eastern Ukraine demonstrated efficient influencing without ever declaring war.[23] Russia's fast operation tempo, overwhelming confusion campaign, and clandestine military operations surprised the Western intelligence community. Overall, Russia modernized and made its armed forces more versatile. From A2/AD systems to nuclear weapons, it can challenge, harass, and deter US and NATO forces—at least in a significant regional-level conflict.[24]

Russia possesses a broad array of electronic warfare capacities. Interference and jamming capabilities blur the difference between normal conditions and conflict—typical Russian gray zone operations. Russia has harassed military and civilian traffic through widely spoofing and jamming Global Positioning System (GPS) signals in conflict zones near Russian territory and Arctic areas.[25] Military and commercial aircraft were exposed to GPS jamming in Scandinavia during the Russian-Belarussian joint exercise in 2017.[26] Similarly, ships operating in the Black Sea have reported losing position keeping and receiving GPS signal errors. However, Russia's disinformation campaign denies all accusations of any Russian electronic warfare attacks against space-based positioning, navigation, and timing (PNT) services.

Russia has used electronic warfare, force projection, long-range weapon systems, and multilayered defense systems in the Syrian and Ukrainian conflicts and close to Russian territory. Experiences from conflicts and increasingly advanced joint wartime exercises (for example, Zapad 2017) demonstrate Russia's offensive A2/AD capabilities and its potential to challenge NATO.[27] Broad military capacity and decisive use of all necessary means bolster the Russian military as a potent instrument of power and intimidate states even without immediate geographic contact with Russia. Using the military as a vital instrument of power provides an essential grounding for other Russian instruments of power and hybrid warfare execution.

Cyberwarfare

Clandestine cyber operations—ranging from espionage to subversion, sabotage, and identity theft—challenge state security organizations and everyday internet users.[28] To the same extent, the Russian readiness, nerve, and arrogance to expand cyberattacks in the digital world underline its comprehensive competition against adversaries. Russia's vague undercover cyberattacks create a curtain of uncertainty, complicating recognition, mitigation, and prevention of malicious cyberattacks.

The first well-known cyberattack series halted numerous Estonian administration and business sites after Russian-led protests over a WWII memorial dispute.[29] Contemporary Estonia was one of the most digitalized countries, tempting Russian hackers to target the government, banks, and media.[30] Though Estonian experts traced the denial-of-service attacks and connected the dots to the Kremlin, Russia adamantly denied all accusations.[31] Hence, Russia showed cyber dominance and paved the way to continue this new modus operandi without disruptions or international charges.

Similar cyberattacks followed the Estonian case. During the Russian invasion of Georgia in 2008, the cyberattack target was Georgia's defense communications. Likewise, in 2015, Russian hackers distributed malware into the Ukrainian electrical grid. It caused a power interruption for millions of people and highlighted Ukraine's energy and cyber vulnerabilities as well as Russia's power.[32] In 2017, Russia again targeted Ukraine through its financial and federal infrastructure. However, the NotPetya cyberattack had harmful global implications and spread quickly across Windows operating systems, affecting, for example, global transportation companies from Masters to FedEx.[33] NotPetya and other destructive cyber operations illustrate that people are usually the weakest link and that cyberattacks have pervasive physical and cognitive ramifications, usually with limited responses from targeted states.[34]

Information Warfare

Russia has a long history of demonstrating its mastery of information warfare, but the focus in Putin's regime has shifted to manipulating foreign target audiences. Admittedly, propaganda and censorship have a strong position internally. Nevertheless, Russian information warfare increasingly undermines other states' decision-making, deteriorates societal cohesion, and disputes foreign leaders' authority and competence. Authoritarian Russia has solidified its role as a modern propaganda hegemony. Conversely, democracies have problems retaliating against this new soft and hard power mixture.

Russia's state-driven media, officials, proxies, trolls, and politicians promote ideas, rumors, and conspiracy theories favorable to Russia, unconfirmed truths via official digital channels, and biased social media accounts. Open information networks and technologies give Russian influencers a fast and cheap means to spread propaganda globally.[35] As an authoritarian state, Russia effectively controls influencers, proxy actors, and agents to conceal the Kremlin's fingerprints. Russia and China have spent millions of dollars increasing an asymmetric, aggressive, information warfare–based "sharp power."[36] Their sharp power creates a hostile environment, amplifying distrust and discord among people and state institutions by piercing and penetrating political and informational environments. Thus, the Kremlin has used sharp power, which is more harmful than traditional culture-based soft power, to meddle in other nations' elections and corrupt information in recent years.[37]

Russia's meddling in the 2016 US presidential election is the most visible example of comprehensive information warfare. Though foreign interference efforts have always played a role in policy making, handy, cheap new technologies made organized propaganda and disinformation campaigns more efficient and widespread than ever before.[38] Strategic-level information warfare undermined the US-led liberal world order and the populace's belief in the democratic presidential election system, developing a clear advantage for Trump.[39] Russian intelligence agencies illegally intruded and interfered with Hillary Clinton's and the Democratic National Committee's email accounts and leaked content on WikiLeaks, causing political and social discord in America.[40] Russian intelligence agencies cunningly exploited all modern digital networks' vulnerabilities. More importantly, the nonregulated human social media networks multiplied the effects of distortion, dispute, and distrust.[41]

According to the intelligence community's assessments, President Putin ordered the multifaceted 2016 US presidential election meddling campaign—demonstrating how centralized hybrid warfare is in Russia.[42] The all-encompassing information campaign consisted of cyber espionage and intrusions against political organizations and electoral boards, public disclosure of collected data, propaganda, Russian state-owned news agency (Russia Today, Sputnik) misinformation campaigns, and fake social media profiles controlled by professional trolls from the so-called Internet Research Agency in St. Petersburg.[43] One worrisome phenomenon was that information warfare targeted partisan winners and losers differently; the campaign was not directed against the whole country like the examples of Pearl Harbor and 9/11.[44] Social-engineered divisive information warfare increased partisanship in the US and was a detrimental sting against democracy.

Nonmilitary Coercion and Intimidation

One parlous trend in the Russian tool kit is the use of nonmilitary intimidation and coercion. State actors or proxies have used various illegal methods like blackmailing, assassinations, criminality, economic extortion, and intentional immigration agitation as part of broader coercion.

Russia exploited the European immigrant crisis in 2015 to overwhelm authorities by intentionally opening usually closely controlled border crossing points into Finland and Norway. Abruptly pushing thousands of immigrants into these countries paralyzed normal operations and required additional personnel to handle the chaos. The massive influx of immigrants also challenged the abilities of essential service providers—such as border, police, military, justice, healthcare, and security personnel—to perform their duties. Further, the disorder created by Russia's targeted immigration tactics intensifies the polarization and diversion in the targeted nation. The results fan the flames of discord, inducing diaspora and fueling racial prejudices that can spark demonstrations and violence. Russia clearly demonstrated that it has the ability and means to direct chaos toward targeted state decision-makers and authorities.

Russia uses proxy forces to amplify hybrid warfare dominance, hide its tracks, and prevent legal accountability for its actions. In Crimea, the pro-

Russian nationalist motorcycle club Night Wolves paved the way for Russian special operation forces by collecting intelligence, exploiting offensive protests, and distributing propaganda.[45] Criminal organizations' intimidation and covert illegal influencing provide state-level deniability, therefore constituting non-state proxy actors as an integral and growing part of the future of hybrid warfare.[46]

Additionally, Russia employs private military companies (PMC) in the conflicts in Ukraine and Syria. Its use of PMCs surfaced after Russian Wagner fighters lost their lives in a US airstrike in Syria.[47] PMCs play an increasingly important role, giving Russian leadership a compelling instrument of power to multiply the effects in the cyber and military battlefields and provide the guise of plausible deniability in dirty, dangerous, and illegal operations.[48]

Since Putin came to power, assassinations have reappeared as a method of influence. The Kremlin has systematically denied its involvement in high-level poisonings and provided alternate evidence and conspiracy theories as distractions.[49] However, the evidence—the sources of poison (dioxin, polonium, Novichok) and/or Russian security services members' presence—clearly links the assassinations to Russia.[50] Victims have posed a significant opposition or loyalty threat to Putin's power. Though the poisonings of journalist Anna Politkovskaya, anti-Russian Ukraine presidential candidate Viktor Yushchenko, ex-Russian intelligence officers Alexander Litvinenko and Sergei Skripal, and opposition leader Alexei Navalny have not been fatal in every case, Moscow's message and direct action against any anti-Kremlin group or individual have been unambiguous.[51] Fear is an efficient weapon in silencing unwanted messengers.

The Essence of Russian Hybrid Warfare: Gerasimov Doctrine and Whole-of-Government Approach

Though the previously discussed influence methods might seem isolated and disparate, the Russian hybrid warfare concept is a decisive cumulative approach organized by a centralized command. In hybrid warfare, several state and non-state actors combine kinetic, cyber, physical, psychological, social, and nonphysical actions to cause intimidation, instability, polarization, escalation, and powerlessness to act in a targeted state. Hybrid warfare's essence is to operate in all domains across the conflict spectrum, undermining a targeted state's relative power, cohesion, and decision-making capacity below the level of a declaration of war.[52] Thus, as Russian general Valery Gerasimov stated, "War in general is not declared; it simply begins with already developed military forces."[53] Blurring the line between peace and war and obscuring normal conditions with the fog of war are fundamental principles in Russian hybrid warfare. Its ultimate aim is to wear out, frustrate, confuse, disintegrate, and undermine adversaries without giving them a legal or moral means to respond.

Russia exploits the principles of Chinese military strategist Sun Tzu, "gaining the material and moral advantages such [that the] battle is won before it is fought" when attacking continuously against an enemy's vulnerabilities.[54] Today, Russian economic or military power is not strong enough to directly challenge the US or NATO. Hence, Putin's concealed offensives target societies' weaknesses (cybersecurity, legislation holes, morale, and unity) to diminish the adversaries' relative strength in the long-term power competition.[55]

Hybrid warfare is a whole-of-government approach, controlled and masterminded by Russia at the highest levels.[56] A NATO paper observes that "President Putin is the architect of strategy, a new/old Russian strategic method that can be summed up as the conduct of war via 5Ds: destabilization, disinformation, strategic deception, disruption, and, if need be, destruction."[57] As previous hybrid warfare cases reveal, Putin's authoritarian government effectively demonstrated all 5Ds during the 2010s. Affordability, effectiveness, and authoritarianism are some reasons why Russia has shifted toward the model of hybrid warfare characterized by centralized command and decentralized operation. Attacking democracies' weaknesses with cyber, information warfare, covert operations, and proxy forces rather than building a conventional arms race is a more effortless way to challenge US, NATO, and EU cohesion. However, it must be noted that Russia is still augmenting its conventional warfare ability by developing traditional land, air, sea, and space capabilities, the nuclear triad, A2/AD systems, cyber, and emerging hypersonic weapons.

The essence of hybrid warfare is associated with Russian general Valery Gerasimov's chief of General Staff doctrine about nonlinear warfare and its predominant nonmilitary methods in modern conflicts.[58] The doctrine includes Gerasimov's well-known illustration of Russian new-generation warfare that shows phases of a crisis and the role of nonmilitary and military measures.[59] The doctrine reveals how all instruments of power (DIME) have a role and how nonmilitary measures dominate (4:1 correlation) in a modern, nonlinear hybrid warfare environment.[60]

Maskirovka, Reflexive Control, and Centralized Command

Admittedly, giving a single, clear definition of *Maskirovka* (deception) is difficult, but understanding its vital role in hybrid warfare from the tactical to strategic level is essential.[61] Russia has expanded the traditional tactical- and operational-level battlefield *Maskirovka* for a broader, all-domain strategy and power competition concept.[62] Successful Russian strategic deception confuses the adversary's observe-orient-decide-act (OODA) loop and gains an advantage in time and space.[63] Along with using deception, centralizing command and control has created an edge in operational tempo and decision-making. In 2014, President Putin linked situation centers and created a new interagency information sharing and commanding system, the National Defense Management Center (NDCM).[64] The NDCM works in a national security framework connecting all critical actors, departments, agencies, and systems. The controlled, centralized whole-of-government approach creates an advantage to develop and implement comprehensive Russian defense strategies and plans.[65]

Russia has a long strategic military history in reflexive control that combines deception, effective persuasion, and manipulation to compel adversaries to inevitably act according to select information fed by the Russian state or proxy actors.[66] Reflexive control is a crucial element in Russia's hybrid warfare playbook. Instead of straightforward occupation and large-scale military force operations, Russia exploits covert and overt indirect approaches to change the targeted state's or group's behavior to one that favors Russia. Hybrid warfare subdues the adversary to cooperate either by coercion or by allowing the adversary to lead toward the desired direction.[67] Russian actions in Ukraine and against NATO ultimately worked according to its concept of reflexive control. Denial and deception campaigns showed the red line for NATO expansion, deterred the West from intervening in the crisis militarily, and managed to support pro-Russian separatists and public opinion in Ukraine.[68] In sum, hybrid warfare challenges the international community, state-level decision-makers, and individuals by increasing confusion and coercion, applying overwhelming pressure, and masking the line between conflict and peace with multiple military and nonmilitary actions.[69]

Countering Hybrid Warfare: Comprehensive Security Approach

> *Hybrid is the dark reflection of our comprehensive approach. We use a combination of military and non-military means to stabilize countries. Others use it to destabilize them.*
>
> —Jens Stoltenberg, NATO Secretary General, 2015

The following discussion analyzes countermeasures that states and organizations should implement against hybrid warfare. Above all, it explores why comprehensive security provides a well-suited concept to improve readiness, situational awareness, resilience, and deterrence. Researchers at the Hybrid CoE compared the best hybrid warfare countermeasures among Britain, Finland, Sweden, France, Estonia, and the EU. They found shared features in the following areas: a whole-of-government / whole-of-society approach, vulnerability assessment, cyber defense, creativity in reaching out to the private sector, and improvement of situational awareness and (counter) intelligence.[70] The following countermeasures analysis encompasses but is not limited to Hybrid CoE's findings.

Recognizing the Problem, Assessing Vulnerabilities, and Improving Situational Awareness

First, states and security actors should identify the problem, increase understanding of hybrid warfare, assess vulnerabilities, and explore countermeasures. Russia's versatile multidomain attacks rapidly challenged politicians, senior leaders, military officers, and NGOs. However, countermeasures have developed more slowly. The symmetrical force-on-force response does not necessarily secure one's vulnerabilities or deter attackers because the defender must employ a wide array of actions concurrently in all domains and with all resources and instruments of power (DIME).

Cooperation between authorities, businesses, NGOs, and citizens aids in recognizing and understanding cumulative weaknesses and opportunities before and during attack. Situational analysis and information sharing form the primary layer of an efficient defense against hybrid attacks. A thorough assessment reveals what elements require protection, how best to influence the adversary, and which authority has the optimal resources to implement the actions. Nevertheless, most cases are usually so complicated that counteractions outweigh a single authority's resources and know-how. For that reason, the government should gather information broadly, foster interagency cooperation, and ask for other entities' help if the situation dictates. Collaboration supports connecting the dots, examining creative countermeasures, seeing the whole picture, and sensing time-critical information requirements. All of these elements are required to increase situational awareness and mitigate hybrid aggressions.

Today's complex hybrid operating environment sets high situational awareness requirements from the tactical through the strategic level across states and organizations. The EU has recognized the importance of information and intelligence sharing and the value of revealing best practices and lessons learned. [71] Security agencies should enhance monitoring warnings and indications. However, the main problem usually is that intelligence information does not spread across a broad range of stakeholders, which hampers early warning signs.[72] Western civilian-military intelligence exploits multiple intelligence, surveillance, and reconnaissance (ISR) capabilities, but cyberspace and the digitalized environment also require more robust counterintelligence. Some countries have recognized this need and proactively made cyber intelligence legislation changes to enhance intelligence collection within and outside the country.[73] Detection through indicators and warnings enables the monitoring of Russia's "known unknowns." Additionally, the systematic analysis discovers "unknown unknowns."[74]

One challenge with hybrid warfare is that the targeted state is continuously reactive. A hybrid attacker disturbs the decision-making process by saturating the information domain. The targeted state therefore needs to sharpen its OODA cycle to operate faster than the adversary. Maintaining situational awareness superiority and the operations tempo is exceptionally challenging for reactive defenders but not impossible. As discussed, recognizing and analyzing the situation among critical actors is the first significant step in building a coherent counteraction strategy. After a multifaceted collaborative analysis, the following essential questions arise: What should be done? Who has the overall responsibility for responding? And when is the best time to act? These crucial questions must be answered before any actions can be implemented. The following describes deterrence methods against hybrid warfare.

Deterring against Hybrid Warfare

How to deter against hybrid warfare is a relevant question for tomorrow's decision-makers. Deterring hybrid warfare is more complicated than deterring traditional conventional military attacks. Nevertheless, hybrid deterrence generally employs the same elements as traditional deterrence—a balance of escalation, signaling, and denial and punishment.[75]

States should incorporate proportional punishment methods in their arsenal because current hybrid attackers survive largely unpunished or encounter only economic sanctions.[76] According to Hybrid CoE research, states need to focus on future-oriented, strategic deterrence.[77] That is, they should increase their ability to impose costs against aggressors in addition to responding reactively and mitigating threats.[78] Deterrence by punishment has usually been absent against attacks below the level of armed conflict, allowing the hybrid attacker to get away without appropriate countermeasures. A shift from a responsive to a preventive role prevents further aggression by creating cost-benefit calculus problems for adversaries while strengthening resistance and increasing trust among citizens and allies. All DIME instruments and the influence spectrum from soft to hard power should be on the table when deciding on deterrence, retaliation, and counteractions. Otherwise, states are handicapped by limiting themselves to using only part of their power and ability to respond. Sanctions have been imposed, but the West needs more tools to be strategically predictable while still being operationally and tactically unpredictable.

Researcher Mikael Wigell recommends democratic deterrence as a new strategic concept. In this concept, states can turn democratic vulnerabilities into strengths through implementing deterrence by denial and punishment.[79] More precisely, Western societies should demonstrate that security and democracy do not rule each other out but support each other hand in hand. Russian hybrid warfare specifically targets the dilemma between security and freedom of speech. However, if democracies close their societies, they will act according to the Russian reflexive control playbook and "voluntarily take a predetermined action towards censorship and totalitarianism."[80] In the long run, democratic deterrence strengthens democratic values, freedom of speech, equality, and security infrastructures to improve governance, resilience, and robustness—an excellent deterrent against Russia's actions.[81]

Continuous competition below armed conflict, new disruption methods in cyberspace, and the role of disinformation are trends that force targeted states to find new methods to mitigate and deny risks.[82] Cyber deterrence is a relatively new and unexamined field. Cyberspace is like the Wild West, where rules-based norms and countermeasures chase hostile technological and conceptual development. An Estonian cyber case demonstrates the difficulty of defining a collective response against cyberattack. Estonia asked NATO to invoke Article V (an attack on one is an attack on all). However, NATO responded that it had no retaliation options because a cyberattack was not equivalent to an armed attack.[83] After a decade, the same cyber-related proportionality, attribution, and retaliation problems are still on the table. States and international organizations should establish rules, treaties, and legitimacy agreements regarding cyberspace aggression, as with nuclear and conventional weapons during the Cold War. Before solving cyber-deterrence implementation, digital security legislation rules and the status of non-state actors require critical analysis.

Deterrence by denial enhances resilience by using a total defense concept encompassing a broad spectrum of collaborating security actors.[84] Sweden, Norway, and Finland have a tradition of this whole-of-government approach. Essentially, Finland's comprehensive security is more like a whole-of-society approach because—along with authorities, business operators, civil organizations, and citizens—it assists everyday resilience and security.[85]

Finnish comprehensive security model. Finland's comprehensive approach secures society's vital functions through collaboration among authorities, the business community, organizations, nongovernmental organizations (NGO), and citizens. The government released its *Security Strategy for Society* guidance, where it harmonizes national preparedness principles and directs readiness actions for different branches.[86] Finland's long tradition in comprehensive security (WWII total defense concept) and broad whole-of-society integration have increased interest among states and organizations struggling with harmful Russian hybrid attacks.[87]

Interagency collaboration and cooperation are commonplace in many states, but what makes Finland's model unique and efficient is its connectivity to state and non-state actors.[88] Hybrid warfare targets authorities, businesses, and organizations, increasing the role of NGOs and the private sector in the globally connected security realm. No organization or decision-maker can have situational awareness without information from other stakeholders. Thus, sharing best practices, knowledge, actions, and systems across civilian and state authorities enhances state-led security. A comprehensive approach where information flows freely between stakeholders improves identifying signals and threats early enough to start the required analyzing, assessing, and decision-making processes.

The comprehensive security approach works best to combine information and actions across central, regional, and local actors. Departments' strategic guidance should smoothly operationalize to concrete actions at the regional and local levels. Specifically, communication, cooperation, and procedures must be practiced and tested across horizontal and vertical command chains. In the Finnish model, joint preparedness is a general principle to enhance resilience, strengthen security procedures, and augment a sense of security.[89]

The comprehensive security model necessitates commitment, active joint planning, training, and implementation. Otherwise, the ambitious whole-of-society approach does not concretize. In a challenging, uncertain threat environment, broad cooperation, information sharing, and communication increase know-how and trust among key players, enabling better decisions, risk analysis, and the discovery of cost-efficient ways to improve weaknesses and situation-specific solutions.[90]

Hybrid warfare comprises various cross-domain power instruments. Correspondingly, a comprehensive security model should exploit multidomain and DIME instruments, including but not limited to national military defense, diplomacy, information, cyberspace, economics, internal security, physical infrastructure, psychological resilience, and leadership. When the whole-of-society model excels, responsibilities, resources, and actions align with a matrix of actors. The concept corresponds to joint military operations where a supported commander has the overall coordination responsibility and primary resources, but supporting commanders underpin joint efforts with their knowledge and resources. As a result, a comprehensive security model responds efficiently to clandestine cyberattacks, border security intrusions, or election meddling at the top and grassroots levels.

NATO and EU countermeasures. Also, organizations like NATO and the EU have recognized actions against hybrid warfare. NATO's immediate responses focus on cost-efficient, concrete steps to improve realistic exercises, intelligence, strategic communication, new technologies, and education.[91]

Sharpening early warning systems, ISR capabilities, and joint force readiness is a clear-cut requirement for the military.[92] Similarly, military and security providers should address vulnerabilities in cyberspace and innovate gray zone influencing. There needs to be a thorough inspection and adjustment of legislation, the rules of engagement, and identification procedures to discover and address any existing loopholes. NATO is anxious about hybrid warfare's influence in the Baltic states, where a sizable Russian ethnic population might give Russia self-justification for interfering in interstate affairs.[93] To counter hybrid warfare, NATO has underlined securing critical information, networks, and capabilities and finding simple ways to respond, resist, and deter. Defensive and offensive cyberspace capabilities are under states' sovereignty; however, inside NATO member states, a needed critical discussion is whether cyberattacks correlate with armed aggression.

The EU's countermeasure approach sets principles to mitigate the threat by improving understanding of hybrid warfare, recognizing countries' vulnerabilities, improving awareness, building resilience, deterring aggression, stepping up strategic communication, and promoting collaboration with EU and NATO countries.[94] Specifically, countermeasures mirror the states' whole-of-government model but at the organizational level. Member states have varying vulnerabilities, such as inefficient military, energy dependencies, and/or sensitive ethnicity issues. Additionally, along with national weaknesses, the EU should analyze its institutional weaknesses and the risks threatening all member states, including cyberattacks and energy security.[95]

A key finding at the EU and NATO organizational levels is that ultimately states are responsible for countering the hybrid threats. Therefore, national sovereignty and sensitive weaknesses inside states complicate reactions at the more significant organizational level. Nevertheless, the EU and NATO should also improve resilience and deterrence against hybrid warfare. Developing cooperation between the EU, NATO, and their member states in exercises, workgroups, and development programs is vital to improving overall understanding and sharing best practices across security actors. One excellent example of concrete collaboration was creating the Hybrid CoE to conduct research and organize training and exercises.[96]

Recommendations

The comprehensive security model is an overarching framework to counter hybrid warfare. However, there are plenty of single and combined measures that states and security organizations can use to counter and mitigate hybrid warfare. The following highlights actions that increase resilience at the national security level and recommends concrete, immediate responses to improve readiness and deterrence for malicious Russian hybrid warfare.

Though open societies today are digitally vulnerable and reactive, states and security providers should not acquiesce to fate in response to hybrid warfare. Rather, democracies should mitigate risks and explore countermeasures to increase overall resilience against cyber and information war. Fostering democratic values, amplifying truth-based narratives, embracing transparent governance, encouraging all-encompassing education, using critical thinking, and facilitating cooperation among authorities and businesses are essential skills in countering adversaries' aggressions.

Achieving Resilience: Learning by Doing

Authorities should train and educate personnel on the need for coordination, decision-making, and analysis when responding to threats. Since hybrid warfare targets the whole of government and society at large, states require comprehensive means to mitigate threats jointly across authorities, organizations, and citizens. Thus, it is essential to expose strategic and tactical decision-makers to solving wicked problems beforehand: sweat during peacetime saves blood in war. Officials should organize tabletop, command post, and real-life exercises using hybrid warfare cases. By teaching and communicating, working, and coordinating with state actors, NGOs, industries, and officials, the state can develop enlightened, broad-minded leaders and operationally excellent actors to counter the fog of Russian hybrid warfare.

Moreover, joint training exponentially increases mutual trust between actors, easing and harmonizing actions during a crisis. Making sharing best practices and information a habitual skill is one beneficial outcome of joint training and collaboration. No authority, official agency, or department can handle complicated effects alone. Educating and linking civilian and military leadership to work jointly maximizes leveraging the best tools in a crisis, thus developing resilience and deterrence. All-encompassing training that includes partners fosters critical thinking. A lack of time and resources can hinder multinational training opportunities. However, even short training events and briefings among allies might innovate thinking about readiness, resilience, and deterrence. Investment in education is the most efficient way to increase the state's resilience and deterrence options in the long run.

Besides emphasizing cognitive concepts, officials should address vulnerabilities in the security infrastructure. Hybrid threat mitigation and deterrence require secure networks, virus protections, cyber defensive measures, and advanced surveillance systems, along with improved physical infrastructural security measures. When procuring military or state-owned complex systems, security specialists should have a role in considering cyberspace effects and vulnerabilities in the hardware and software. Likewise, since it is a human who usually leaves the cyber door open, organizational culture and concepts should support responsible digital behavior.

Improving Information, Intelligence, and Situational Awareness

Because there are no quick wins against dirty information warfare, that realm might be the hardest to mitigate. However, Western democracies should continue to maintain credibility, trustworthiness, transparency, and truth as weapons to educate and enlighten their citizens against modern disinformation. In the battle against information warfare, the West might suffer some short-term losses against authoritarian state aggressive narratives. However, truth and the ability to read information and media are the only ways to maintain trust, control the narrative, and influence people in the long run.

Educating people on how to analyze information and media is a resource well spent. All age groups should know an online code of conduct and evaluate the legitimacy of media sites. At the state level, resilience against cyberattacks and data breaches increases when all employees' basic cyber knowledge is encouraged. Policy makers, spokespersons, and military leaders should be trained in strategic communication. Usually, the deeper the crisis, the more involved a human perspective should be in strategic communication and narratives. Selecting articulate, credible spokespersons to represent organizations is an excellent way to improve resilience against harmful hybrid attacks.

We need to adapt, act, and outthink more quickly than our foes. States should improve ISR connectivity among key agencies to foster shared interagency situational awareness. The government should reduce silo structure, reducing tempo and leaving decision-makers to operate with an incomplete picture. Thus, a comprehensive whole-of-government/society model would be the preferred option to increase hybrid warfare responsiveness. Organizational learning and sharing best practices should be commonplace not just in a particular department but broadly across authorities and organizations with roles in national security. We should ask questions like who else needs to know, which organization has the best resources, and how can we best counter, limit, mitigate, and deter the subsequent hybrid warfare attacks?

Undertaking such actions leads to increased requirements for situational awareness, intelligence, and decision-making. In most cases, a single state, agency, or business partner does not have all the resources or know-how to solve the problem. Therefore, interagency cooperation, information sharing, and state-level communication are vital.

However, these endeavors cannot succeed without clear commitment, organized procedures, and training. Broad countermeasures against hybrid warfare, in the long run, require that the state implement a whole-of-government approach. At best, it should involve private-sector players and the education of its citizens.

Conclusion

This article analyzed Russian hybrid warfare actions and the vulnerabilities of modern digitalized societies and outlined the broader concept of hybrid warfare. It identified effective countermeasures against hybrid warfare and introduced a comprehensive security model as a critical resilience and deterrence approach.

While propaganda, asymmetric operations, and dispersal of cohesion are not new coercion methods, in today's intertwined global, uncertain, ambiguous, and automatized world, the effectiveness of these tools has increased manifold. The challenge is especially significant in open, modern, information-driven democracies where affected individuals or institutions do not necessarily understand that they are intentionally targeted.

Russian hybrid warfare creates instability with multidomain attacks and clandestine operations. The combined impact of hybrid attacks undermines targeted states' situational awareness, cohesion, and decision-making in all war-fighting domains, including cyber and information. With this intention, Russia aims to achieve its options in a cumulative approach by competing, challenging, and targeting its adversaries below the level of open conflict or war. Attacking against weaknesses in Western legislation, morale, and unity makes an adversary relatively weaker. Diminishing an adversary is easier for Russia to accomplish than increasing its strengths. By doing so, Russia aims to increase its relative position and revive its role as a great power, at least in the Eurasian area.

President Putin and his high elite mastermind hybrid warfare in an entirely centralized way, and it truly is a whole-of-government approach. Similarly, combining a comprehensive national security approach and cooperation provides the best platform and measures for targeted states to act against, mitigate, and deter overt and covert hybrid assaults. Joint training, education, and information sharing improve resilience and preparedness. Enhancing the nation's security, resistance, and countermeasures in a complex hybrid warfare environment necessitates the transition from reactive operations to existing, well-trained, and practiced active day-to-day operational principles. Additionally, preventing further hybrid warfare attacks requires fostering state-level deterrence and retaliation measures.

Increasing awareness of hybrid warfare, Russian deception-centric thinking, and appropriate countermeasures is essential for tomorrow's decision-makers, strategic leaders, state authorities, and even citizens. Exploiting an adversary's vulnerabilities has always been part of a winning strategy, as seen in Sun Tzu and Clausewitz's writings. Indeed, Russian hybrid warfare is just another means to exploit adversaries' weaknesses. However, Western democracies and security organizations can turn the tables and counter hybrid warfare by changing their reactive mindset to taking active measures.

Lt Col Tuukka Elonheimo, Finnish Air Force

Colonel Elonheimo has served as the deputy chief of Air Force operations, Finnish Air Force Command; chief of flight operations, Finnish Air Force Command; and strategic plans team chief, Plans and Policy Division, Finnish Defense Command. He also held staff positions as an operational and strategic planning expert. Colonel Elonheimo is a graduate of Air War College, Air University, Maxwell AFB, and completed a two-year general staff officer's degree at the Finnish National Defense University.

Notes

[1] James A. Winnefeld, Michael J. Morell, and Graham Allison, "Why American Strategy Fails: Ending the Chronic Imbalance between Ways and Means," *Foreign Affairs*, 28 October 2020, 3, https://www.foreignaffairs.com/.

[2] Joint Chiefs of Staff, Joint Doctrine Note 1-18, *Strategy*, 25 April 2018, GL-1, vii, https://www.jcs.mil/.

[3] András Rácz, *Russia's Hybrid War in Ukraine: Breaking the Enemy's Ability to Resist*, FIIA Report 43 (Helsinki: The Finnish Institute of International Affairs, 2015), 40–43, https://www.fiia.fi/.

[4] James W. Browning, *Leading at the Strategic Level in an Uncertain World* (Washington, DC: Dwight D. Eisenhower School for National Security and Resource Strategy National Defense University, 2013), 18–19.

[5] Rácz, *Russia's Hybrid War in Ukraine*, 28–37.

[6] Carl von Clausewitz, ed. and trans. Peter Paret and Michael Howard, *On War* (Princeton, NJ: Princeton University Press, 1989), 119–20.

[7] Benjamin Buchanan, *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics* (Cambridge, MA: Harvard University Press, 2020), 230–32.

[8] Laura Rosenberger, "Making Cyberspace Safe for Democracy: The New Landscape of Information Competition," *Foreign Affairs* 99, May/June 2020, 146–59, https://www.foreignaffairs.com/.

[9] Hybrid Center of Excellence (CoE), *Trends in the Contemporary Information Environment: Hybrid CoE Expert Pool Meeting on Information,* Hybrid CoE Trend Report 4 (Helsinki: The European Centre of Excellence for Countering Hybrid Threats, May 2020), 22, https://www.hybridcoe.fi/.

[10] Joseph S. Nye, Jr., "Countering the Authoritarian Challenge – Public Diplomacy, Soft Power, and Sharp Power," *Horizons,* no. 15 (Winter 2020): 98, http://www.cirsd.org/.

[11] Department of Defense, *Cyber Strategy Summary 2018* (Washington, DC: Department of Defense, 2018), 1, https://media.defense.gov/.

[12] Magnus Normark, *How States Use Non-State Actors: A Modus Operandi for Covert State Subversion and Malign Networks*, Hybrid CoE Strategic Analysis 15 (Helsinki: The European Centre of Excellence for Countering Hybrid Threats, April 2019), 2–3, https://www.hybridcoe.fi/.

[13] Ralph Thiele, "Artificial Intelligence – A Key Enabler of Hybrid Warfare," Hybrid CoE Working Paper 6 (The European Centre of Excellence for Countering Hybrid Threats, Helsinki, 6 March 2020), 6, https://www.hybridcoe.fi/.

[14] Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare* (New York: Farrar, Straus, and Giroux, 2020), 11.

[15] Buchanan, *Hacker and the State*, 212–13.

[16] Hybrid CoE, *Trends in the Contemporary Information Environment,* 4, 7.

[17] Hybrid CoE, *Countering Disinformation: News Media and Legal Resilience*, Workshop organized by the Hybrid CoE and the Media Pool, part of the Finnish Emergency Supply Organization, 24–25 April 2019, Hybrid CoE Paper 1 (Finland: The European Centre of Excellence for Countering Hybrid Threats, November 2019), 10, https://www.hybridcoe.fi/ .

[18] Clausewitz, *On War*, 87–89.

[19] Fred Charles Iklé, *Every War Must End*, rev. ed. (New York: Columbia University Press, 2005), 1–16.

[20] Patrick Cullen, *Hybrid Threats as a New "Wicked Problem" for Early Warning*, Hybrid CoE Strategic Analysis 8 (Helsinki: The European Centre of Excellence for Countering Hybrid Threats, May 2018), 2, https://www.hybridcoe.fi/.

[21] Elbridge Colby and Jonathan Solomon, "Facing Russia: Conventional Defence and Deterrence in Europe," *Survival* 57, no. 6 (November 2015): 21, https://doi.org/10.1080/00396338.2015.1116146.

[22] Robert Dalsjö, Christofer Berglund, and Michael Jonsson, *Bursting the Bubble? Russian A2/AD in the Baltic Sea Region: Capabilities, Countermeasures, and Implications*, FOI-R-4651-SE (Stockholm: Swedish Defense Research Agency, March 2019), 9, https://www.foi.se/.

[23] Heidi Reisinger and Aleksandr Goltz, *Russia's Hybrid Warfare: Waging War below the Radar of Traditional Collective Defence*, NATO Defense College Research Paper no. 105 (Rome: NATO Defense College, Research Division, November 2014), 3–5, http://www.ndc.nato.int/.

[24] Colby and Solomon, *Facing Russia*, 22.

[25] Todd Harrison et al., S*pace Threat Assessment 2020* (Washington, DC: Center for Strategic and International Studies, March 2020), 25–27, https://www.csis.org/.

[26] Harrison et al., *Space Threat Assessment 2020, 25–27.*

[27] Harrison et al., 25–27.

[28] William A. Perkins, "Component Integration Challenges Presented by Advanced Layered Defence Systems (A2/AD)," *Three Swords Magazine,* no. 33 (March 2018): 56, https://www.japcc.org/.

[29] Department of Defense*, Cyber Strategy Summary 2018*, 1.

[30] Emily Tamkin, "10 Years after the Landmark Attack on Estonia, Is the World Better Prepared for Cyber Threats?," *Foreign Policy,* 27 April 2017*,* https://foreignpolicy.com/.

[31] Tamkin.

[32] Tamkin.

[33] Joseph S. Nye, "Deterrence and Dissuasion in Cyberspace," *International Security* 41, no. 3 (January 2017): 48–49, https://doi.org/10.1162/ISEC_a_00266.

[34] US Cyberspace Solarium Commission, *Cyberspace Solarium Commission Report* (Arlington, VA: US Cyberspace Solarium Commission, March 2020), 8, https://sites.google.com/.

[35] Buchanan, *Hacker and the State*, 288–305.

[36] Rid, *Active Measures,* 12.

[37] Nye, "Countering the Authoritarian Challenge," 105.

[38] Nye, 104–5.

[39] Marek N. Posard et al., *From Consensus to Conflict: Understanding Foreign Measures Targeting U.S. Elections* (Santa Monica, CA: RAND Corporation, 2020), 1, https://www.rand.org/.

[40] Buchanan, *Hacker and the State,* 213–20.

[41] Nye, "Deterrence and Dissuasion in Cyberspace," 48.

[42] US Cyberspace Solarium Commission, *Cyberspace Solarium Commission Report*, 11.

[43] US Office of the Director of National Intelligence, *Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Inci-*

dent Attribution" (Washington, DC: Office of the Director of National Intelligence, 6 January 2017), 1–4, https://www.dni.gov/files/.

44. US Office of the Director of National Intelligence, 1–4.

45. Kenneth A. Schultz, "Perils of Polarization for U.S. Foreign Policy," *Washington Quarterly* 40, no. 4 (October 2017): 21–22, https://doi.org/10.1080/0163660X.2017.1406705.

46. Normark, *How States Use Non-State Actors*, 3.

47. Normark, 4–5.

48. Margarete Klein, *Private Military Companies – a Growing Instrument in Russia's Foreign and Security Policy Toolbox*, *Hybrid CoE Strategic Analysis* 17 (Helsinki: The European Centre of Excellence for Countering Hybrid Threats, 2019), 3, https://www.hybridcoe.fi/.

49. Klein, 3.

50. Sir David Omand, "From Nudge to Novichok: The Response to the Skripal Nerve Agent Attack Holds Lessons for Countering Hybrid Threats," Hybrid CoE Working Paper 2 (The European Centre of Excellence for Countering Hybrid Threats, Helsinki, 18 April 2018), 2, https://www.hybridcoe.fi/.

51. Patrik Reevel, "Before Navalny, a Long History of Russian Poisonings," ABC News, 26 August 2020, https://abcnews.go.com/.

52. Reevel.

53. John Allen et al., *Future War NATO?: From Hybrid War to Hyper War via Cyber War*, Supporting Paper of the GLOBSEC NATO Adaptation Initiative (Bratislava, Slovakia: GLOBSEC, 2017), 12, https://www.globsec.org/.

54. Maria Snegovaya, *Putin's Information Warfare in Ukraine: Soviet Origins of Russia's Hybrid Warfare*, Russian Report 1 (Washington, DC: Institute for the Study of War, September 2015), 11, http://www.understandingwar.org/.

55. Antulio J. Echevarria II, *Military Strategy: A Very Short Introduction* (Oxford: Oxford University Press, 2017), 2.

56. Snegovaya, *Putin's Information Warfare in Ukraine*, 9–11; and Timothy Thomas, "The Evolution of Russian Military Thought: Integrating Hybrid, New-Generation, and New-Type Thinking," *Journal of Slavic Military Studies* 29, no. 4 (October 2016): 554–59, https://doi.org/10.1080/13518046.2016.1232541.

57. Allen et al., *Future War NATO?*, 11.

58. Rácz, *Russia's Hybrid War in Ukraine*, 48–49.

59. Michael Kofman, "Russian Hybrid Warfare and Other Dark Arts," War on the Rocks, 11 March 2016, https://warontherocks.com/.

60. Kofman.

61. Pasi Kesseli, ed., *Venäjän Asevoimat Muutoksessa: Kohti 2030–lukua* [Russian armed forces in transition: toward the 2030s], National Defence University Series 1, Research Publication no. 5 (Helsinki: National Defence University, 2016), 23–25.

62. Timothy Thomas, "Russia's Reflexive Control Theory and the Military," *Journal of Slavic Military Studies* 17, no. 2 (April 2004): 239, https://doi.org/10.1080/13518040490450529.

63. Robert Coram, *Boyd: The Fighter Pilot Who Changed the Art of War* (New York: Back Bay Books / Little, Brown, 2004), 327–44.

64. John Allen et al., *Future War NATO?*, 12.

65. John Allen et al., 12.

66. "Russia, Reflexive Control, and the Subtle Art of Red Teaming," *Red Team Journal*. October 2016.

67. Thomas, "Russia's Reflexive Control Theory, "239.

68. Annie Kowalewski, "Disinformation and Reflexive Control: The New Cold War," *Georgetown Security Studies Review*, 1 February 2017, https://georgetownsecuritystudiesreview.org/.

69. European External Action Service (EEAS), "Food-for-Thought Paper 'Countering Hybrid Threats,'" EEAS (2015) 731, *Council of the European Union, 2015.*

70. Gregory F. Treverton et al., *Addressing Hybrid Threats* (Bromma: Swedish Defense University, 2018), 79–80.

71. EEAS, " 'Countering Hybrid Threats.' "

72. EEAS.

73. Treverton et al., *Addressing Hybrid Threats*, 79–80.

74. "MCDC Countering Hybrid Warfare Project: Countering Hybrid Warfare," Multinational Capability Development Campaign (MCDC) project, March 2019, 3–4, https://assets.publishing.service.gov.uk/.

75. "MCDC Countering Hybrid Warfare Project," 3–4.

76. Mikael Wigell, "Democratic Deterrence: How to Dissuade Hybrid Interference," FIIA Working Paper 110 (Finnish Institute of International Affairs, Helsinki, September 2019), 13, https://www.fiia.fi/.

77. Vytautas Keršanskas, *Deterrence: Proposing a More Strategic Approach to Countering Hybrid Threats*, Hybrid CoE Paper 2 (Helsinki: The European Centre of Excellence for Countering Hybrid Threats, March 2020), 6–7.

78. Keršanskas, *Deterrence*, 6–7.

79. Wigell, "Democratic Deterrence," 2.

80. Jānis Bērziņš, "The Theory and Practice of New Generation Warfare: The Case of Ukraine and Syria," *Journal of Slavic Military Studies* 33, no. 3 (July 2020): 368, https://doi.org/10.1080/13518046.2020.1824109.

81. Wigell, "Democratic Deterrence," 2.

82. Department of Defense, *Cyber Strategy Summary 2018*, 1.

83. Thomas Rid, *Cyber War Will Not Take Place* (New York: Oxford University Press, 2013), 30.

84. Wigell, "Democratic Deterrence," 11.

85. Wigell, 11.

86. *Security Strategy for Society*, Government Resolution, Security Committee of Finland, 2.11.17, 1, https://turvallisuuskomitea.fi/.

87. "Finland's Model for Comprehensive Security Viewed Effective against Hybrid Threats," press release, National Defense University, 11 June 2017, https://maanpuolustus korkeakoulu.fi/.

88. Harri Mikkola et al., *Hyvbridivaikuttaminen Ja Demokratian Resilienssi – Ulkoisen Häirinnän Mahdollisuudet ja Torjuntakyky Liberaaleissa Demokratioissa* [Hybrid influence and democratic resilience: possibilities and ability to combat external harassment in liberal democracies], FIIA Report 55 (Helsinki: Finnish Institute of International Affairs, May 2018), 117–20, https://www.fiia.fi/.

89. *Security Strategy for Society*, Government Resolution, 5.

90. *Security Strategy for Society*, 25.

91. John Allen et al., *Future War NATO?*, 15–16.

[92] John Allen et al., 15–16.

[93] David A. Shlapak and Michael Johnson, *Reinforcing Deterrence on NATO's Eastern Flank: Wargaming the Defense of the Baltics* (Santa Monica, CA: RAND Corporation, 2016), 3, https://doi.org/10.7249/RR1253.

[94] "MCDC Countering Hybrid Warfare Project," 3–7.

[95] "MCDC Countering Hybrid Warfare Project," 3–4.

[96] "A Europe That Protects: Countering Hybrid Threats," European Union External Action Service, Brussels, 13 June 2018, https://eeas.europa.eu/.

Disclaimer and Copyright

The views and opinions in *SSQ* are those of the authors and are not officially sanctioned by any agency or department of the US government.