All-Encompassing War: An Exploration of Information Disorder Countermeasures through Smooth and Striated Space

Abstract

A key challenge facing Western policymakers and professionals in the telecommunications and digital media industries is the use of digital information to further adversarial state's political agendas as part of a broader war effort through "information disorders" like disinformation and malinformation. These efforts create and exploit differences and divides in society to weaken the capacity for resistance, to which scholars, policymakers, and professionals are exploring countermeasures to these efforts juxtaposed against the need to preserve broader democratic ideals. The known need for the development of a unified strategic concept to develop and coordinate effective countermeasures motivates cross-disciplinary reviews of current and proposed countermeasures as well as the use of common theoretical lenses. In this article, I use Gilles Deleuze and Felix Guattari's notions of smooth and striated space to explore current and proposed information disorder countermeasures arranged along offensive, defensive, and supporting approaches. This analysis highlights opportunities to develop coherence across these categories of approaches that reflects the information's impulse to flow across borders and boundaries (geo-political, social) that are fundamental to information disorder's power, and the broader implications for society that political information disorder and corresponding countermeasures portend.

Introduction

General Carl von Clausewitz's well-known axiom "war is politics by other means" (Clausewitz, 2010) has long-standing appeal even today as we are increasingly attuned to the multi-faceted nature of militaristic campaigns of authoritarian states. These "asymmetrical" battlefronts that combine conventional and unconventional means have always played fundamental roles in war (Murray & Mansoor, 2012; Rid, 2020). Recently, Russian efforts in the 2010s and early 2020s to soften adversaries in the West (e.g. interference in the 2016 U.S. presidential election) or assist in the attempted occupation of territory (most notably in Crimea and Ukraine) brought Russian asymmetrical warfare means into cybersecurity consciousness (Jopling, 2018).

Information warfare has and continues to play a fundamental role in hybrid warfare frameworks targeting Western democracies. Policymakers, security professionals, and scholars in the telecommunications and digital media industries are struggling to navigate the delicate balance between democratic ideals and state security stressed by information warfare practices that targets both state and civil society from an adversarial state's military apparatus. Information warfare that depends on the penetration of digital information has entangled facets of society previously conceptually and politically separated (i.e., the state, civil society, private industry) within the institution of war, producing complex questions about countering these harmful political efforts while preserving democracy that we are still coming to grips with.

Efforts to meet the challenge of information warfare have at least in part motivated the need for greater clarity around forms of purposely damaging information, to which scholars have responded by characterizing information along axes of truth and intent. A widely accepted characterization offered by Wardle and Derakhshan (2017) and Wardle (2018) characterizes three forms of "information disorder" (see Figure 1 for a diagrammatic representation of information disorder):

- *Disinformation* is false information created or disseminated with intent to harm.
- *Misinformation* is false information created or disseminated without intent to harm.
- *Malinformation* is genuine or true information created or disseminated with intent to harm.

Other forms of information disorder exist in relation to these core elements, often confusingly used alongside these definitions. "Fake news" are "news articles that are intentionally and verifiably false and could mislead readers" (Allcott & Gentzkow, 2017), including hoaxes, satire, propaganda, and commentary/entertainment (Verstraete et al., 2017). "Propaganda" is information that is designed to persuade an audience while not necessarily committing to truth or fiction, and is often connected to a state government or political entity (Wardle, 2018; Wardle & Derakhshan, 2017). The use of these terms in overlapping and interchangeable ways as they often are, when combined or in parallel with concepts like political warfare and public diplomacy, leads to conceptual confusion (Bayer et al., 2019). While disinformation is largely considered to be false information (Bontcheva & Posetti, 2020a; Robbins, 2020; Wardle, 2018; Wardle & Derakhshan, 2017), others have not made assumptions about true or false distinctions and instead defined it within malicious intent entirely (e.g., Rid, 2020), conflating disinformation and malinformation[1]. Terminological confusion is deeper than simply sloppiness, and hints at the deeply interwoven and layered nature of information disorder, particularly when considering state-originating malicious intent as part of hybrid warfare frameworks.

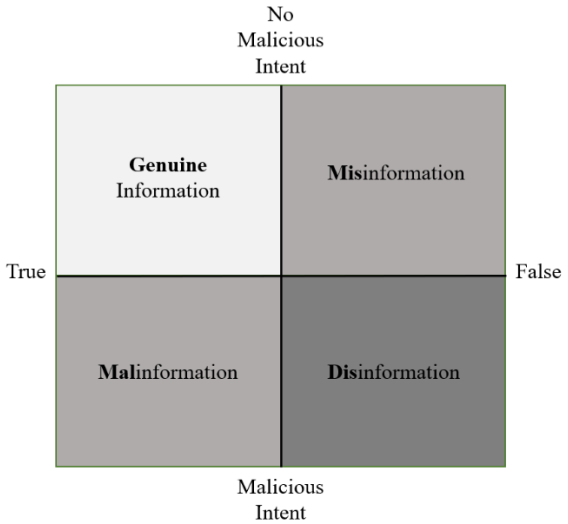

Figure 1: Information disorders, arranged along true-false and malice-no malice axes.

[1] Although it should be noted this is not intended as a critique of this work, as Rid remains clear and consistent about his definitions within the context of the book. Rather, this is meant to illustrate the variety of definitions and uses among scholars.

When states engage in information disorders, they do so with inherent malicious intent to further a political or tactical end. The mechanism of this convergence is the exploitation of perceived divides that can weaken an adversary on multiple fronts through the amplification of "unruly counterpublics" (Bjola & Papadakis, 2021) that corrupt democratic discourse by promoting destructive psycho-social conditions like extremism and polarization. This is driven by the deeply networked societies of today where information is by and large transmitted quickly and widely through digital media, lending a novel spin on asymmetrical warfare adapted for the digital Internet age (Hwang, 2019).

Russian general Valery Gerasimov articulated this component within a broader, cohesive conventional and unconventional strategic and tactical repertoire of warfare within the digital age (Gerasimov, 2016), setting the stage for cyber- and information- spaces as an arena of confrontation with adversaries in the West. The so-called "Gerasimov Doctrine" alongside growing awareness of Russia's fostering of information disorder has invigorated scholarship from a multitude of disciplines, including military studies, cybersecurity, communication, information studies, political science, and international relations, as well as brought in contributions from psychology and public health. While this is indicative of a vibrant body of scholarship, the trick going forward appears bridging the disparate and distinct perspectives together towards a cohesive, "unified strategic concept" (Hwang, 2019). Proper theoretical foundations can provide a conceptual bridge across perspectives by highlighting the nature of information, data, and cyberspace within and across societies, and how hybrid warfare frameworks exploit it (and what the development of a unified strategic concept portends).

I seek to contribute to this necessary effort through this article, applying Gilles Deleuze and Felix Guattari's (1987) concepts of striation, smoothness, and nomadism from to information, data, and cyberspace to critically examine how Western leaders are trying to meet the information dimension of hybrid warfare through current and proposed countermeasures. First, I provide a brief historical perspective on information disorder within warfare. This leads into a discussion and rationale for applying concepts of striation, smoothness, and nomadism to information disorder. These concepts then form the foundation for typologizing and hierarchically organizing the current and proposed counters to information disorder developed in the West. We close with a discussion of what this model and theoretical perspective surfaces about the trajectory of hybrid warfare thinking from the perspective of information, data, and cyberspace.

The Trajectory of Information Disorder in Warfare

A Brief Historical Perspective

Asymmetrical warfare that engages both conventional and unconventional practices as cohesive aspects of a war effort have been practiced for centuries (Murray & Mansoor, 2012). This includes civil society preparedness and political will, information operations, and economic support as direct components of warfare in conjunction with "conventional" or kinetic aspects of warfare.

20th century Soviet so-called "active measures" were central to asymmetrical warfare practices following World War II, consisting of information operations and precise targeting of individuals.

Forgeries, public smear campaigns, assassination, and manipulating social justice activists in the West to serve Soviet ends were all conceived of and executed as pseudo-invisible political aspects of the ongoing Cold War (Rid, 2020). During this time period, the Soviet Union's active measures arm of the Komitet Gosudarstvennoy Bezopasnosti, or KGB (succeeded today by the Federal Security Service, FSB), proved to be one of the most effective and well-regarded outfits in the Soviet military (Rid, 2020). The Reagan administration (1980-88) took a decidedly aggressive stance against Russian disinformation and malinformation through its "Active Measures Working Group" (AMWG). In its final report, the AMWG described a typology of Russian active measures across black, gray, and white measures (Abrams, 2016; United States Information Agency, 1992). See Table 1 below for a reproduction of that typology.

A Typology of Active Measures, Themes, Messages, & Techniques

"BLACK" Active Measures coordinated by KGB Service A	Agents of Influence Forgeries Covert media placements Controlled media
"GRAY" Active Measures coordinated by CPSU CC International Depart.	Foreign Communist Parties Soviet-controlled International Front Organizations Soviet nongovernmental organizations Soviet Friendship Societies Foreign Policy-related research Institutes
"WHITE" Active Measures coordinated by CPSU CC Ideology Department	TASS Novosti Press Agency Radio Moscow Radio Peace and Progress Other Soviet media Information department of Soviet embassies

Table 1: Typology of Active Measures, reproduced from United States Information Agency (1992)

As indicative of the AMWG's typology, active measures transcend the government apparatus: "white" measures producing media institutions (e.g., TASS), "gray" measures producing trans-national organizations (e.g. pro-Russian NGOs), and covert "black" measures influence operations and operatives (e.g. agents of influence) have varying and frequently obfuscated connections to the Kremlin. Moreover, while AMWG constructed this typology before the onset of trans-national digital media and digital information, this "broader than the state" feature of active measures has powerful implications for information disorder countermeasures.

Digital Disinformation Today

Bodine-Baron et al.'s (Bodine-Baron et al., 2018) "disinformation chain" captures organizational structure of Russian state information disorder production and dissemination, modeling the connective flow from state leadership to media consumers, organs/proxies, and amplification channels. Organs and proxies constitute media and research institutions such as the aforementioned TASS, while amplification channels consist of the assemblage of tools and platforms designed to introduce disinformation and malinformation (developed between state leadership and media organs/proxies) into the media practices of consumers.

The disinformation chain represents both a continuation and evolution of the AMWG's final report. In the case of the former, media and research institutions of "white" measures constitute

organs and proxies within the disinformation chain, developing and deploying media and messaging in line with Russian state interests. Social media and digital technologies likewise provide access to large numbers of information consumers that can be targeted by media institutions, trans-national organizations, and agents of influence, e.g. professional hockey player Alexander Ovechkin's pro-Putin and implied pro-invasion stance on Ukraine as disseminated through Instagram (Abrams, 2016). Advancing tools in artificial intelligence and machine learning too can enhance the richness of forgeries, such as "deepfakes" that mimic a person's likeness, e.g. a political figure, to be shared through digital media channels (Miyamoto, 2021; Woolley & Howard, 2016).

At the same time, the AMWG's typology does not directly represent the outsized impact of access and amplification channels like social networks via social media platforms. Digital technologies are emerging that introduce new or substantially evolved forms of disinformation, such as social media bots (Hwang, 2019; Jopling, 2018), algorithms (e.g. suggested friends, some of whom may be agents of influence or bots themselves) (Miyamoto, 2021), online trolls that harass and confuse journalists, dissidents, and media consumers (Helmus et al., 2018; Jones, 2018; Jopling, 2018), and fake "sock puppet" accounts surreptitiously managed by an unknown entity with the intent to deceive (Miyamoto, 2021). The amplification efficacy of these types of technologies stem from their obfuscation and automation (Hwang, 2019), where tools like bots, algorithms, and agents acting through sock puppet accounts "hide in plain sight." Automation and obfuscation carries significant capacity to exploit social and cultural differences by surreptitiously embedding disinformation in media that connect with idiosyncratic features of psychology and personal background (Erlich & Garner, 2021).

While analyzing the Finnish response to Russian disinformation and propaganda, Bjola and Papadakis (Bjola & Papadakis, 2021) argues that, at a fundamental level, information disorder today targets the "public sphere." Originally introduced by German philosopher Jürgen Habermas, the public sphere is a gathering of people as a public to articulate "the needs of society with the state" (Habermas, 2010). It is composed of the relationship between a macro-sphere, or the "will-formation" components of society from political leadership and the state, and the micro-sphere, the "opinion-formation" components built on civil society (Bjola & Papadakis, 2021). Information disorder like disinformation and malinformation "work" insofar as they break down the connections that hold a public sphere together through the creation, support, and amplification of "unruly counterpublics," or destructive discourses that exploit and polarize along societal divides.

Information disorder spread through social and digital media naturally finds and exploits these divides to produce unruly counterpublics, enhanced through obfuscation and automation the digital environment provides. Information disorder is not confined to a single platform, spanning and coordinating across several at any given time, nor is it confined to a single stratum of society or democratic process (e.g., elections). Disorder's reach reflects a fundamental truth about digital information: it resists attempts to restrict in any sense. Fundamental understanding for countering disinformation and malinformation with malicious political intent must centralize understanding the tools and tactics of information disorder creation and spread within information's desire to flow throughout society, culture, and politics.

Striation, Smoothness, and Nomadism in Information Warfare

I turn to Gilles Deleuze and Felix Guattari's *A Thousand Plateaus* (Deleuze & Guattari, 1987c) to frame information's desire to flow, and in turn the tools and tactics of information disorder. Deleuze and Guattari characterize spaces as exhibiting two natures: "striated" space is characterized by allocations and divisions, such as the grid of an urban center, and is homogeneous insofar as similarities emerge from between stratified territory; "smooth" space on the other hand is characterized by the lack of such divisions, enabling a movement through space that is neither restricted nor constrained by the delineation of spaces. It is heterogeneous, as smooth space preserves differences. It is the subservience of the points to the line, whereas striation is the subservience of the line to the point (Deleuze & Guattari, 1987a)[2].

In cyberspace, the smoothness/striation dialectic constructs space as a "virtual topography" (Nunes, 1999). This virtual topography is hybrid: aspects of smoothness and striation exist "in mixture" (Deleuze & Guattari, 1987a). On the one hand, the Internet striates space by dividing users into communities and commensurate groups on platforms, and establishes "information highways" that ferry information from point to point, i.e. lines between servers and users (Nunes, 1999). On the other hand, information also has a flow within cyberspaces, not necessarily always moving with purpose as it transmits from one user or server to the next, finding "lines of flight" with no pre-determined end, such as in chains of retweets.

Information disorder plays upon the smoothness/striation dialectic simultaneously. In many cases it targets particular communities and the digital spaces they inhabit, in this way dependent upon a striated notion of cyberspace as a point of entry. However, its *spread* leverages smooth information flow that passes through potential targets in the creation of unruly counterpublics. An example of this is the "useful idiot" who, upon exposure to some form of disinformation or malinformation disseminates it to their own network in an unpredictable way that resists pre-determination of a set end point. Information disorder desires freedom of flow not just within cyberspaces, but across the social, political, and cultural landscapes in a way that constructs conflict as a "hybrid" socio-information space.

The usefulness of this lens is that it first sensitizes us to the dynamic that exists between smoothness and striation in cyberspace which highlights how information (and information disorder) behaves in this space and what makes it so challenging to counter. But more importantly it sensitizes us to how this same dynamic is reflected in current and proposed countermeasures. When policies and proposals make incorrect assumptions about the information space, particularly missing its broader hybrid socio-information space embeddedness, they risk missing critical features of digital information disorder that limit efficacy, either currently or in long-term. Controlling a phenomenon that desires hybridized freedom of flow necessitates policies and proposals that center this complex reality.

[2] For readers unfamiliar with *A Thousand Plateaus,* clearly stating the definitions of smoothness and striation is difficult to do so concisely, so I recommend reading (Deleuze & Guattari, 1987a) to comprehend, paying close attention to the models presented to understand this concept.

A Model of Information Disorder Countermeasures

With this sensitization in mind, I turn my attention to the current and proposed countermeasures to state-produced information disorder, particularly disinformation and malinformation (i.e., the purposefully malicious ones). I analyzed 23 articles that describe or discuss current and/or proposed countermeasures to information disorder, with a particular focus on hostile state actors like Russia (with occasional mention of China). While there are already excellent quality literature reviews on disinformation already (e.g. (Haciyakupoglu et al., 2018), I opted for achieving "theoretical saturation" whereby data is collected until the appearance of new information or themes attenuates beyond a certain point (Glaser & Strauss, 1967), i.e. the model stabilizes. I opted for this method over adhering to an arbitrary definition of what constitutes an acceptable stopping point, which strict adherence to can be counterproductive (Low, 2019).

Following this analysis of the literature, I produced a typological model of countermeasures (See Figure 2). This resulting model is hierarchical around three major categories: a) defensive countermeasures; b) offensive countermeasures; and c) supporting countermeasures. I will discuss these in turn.

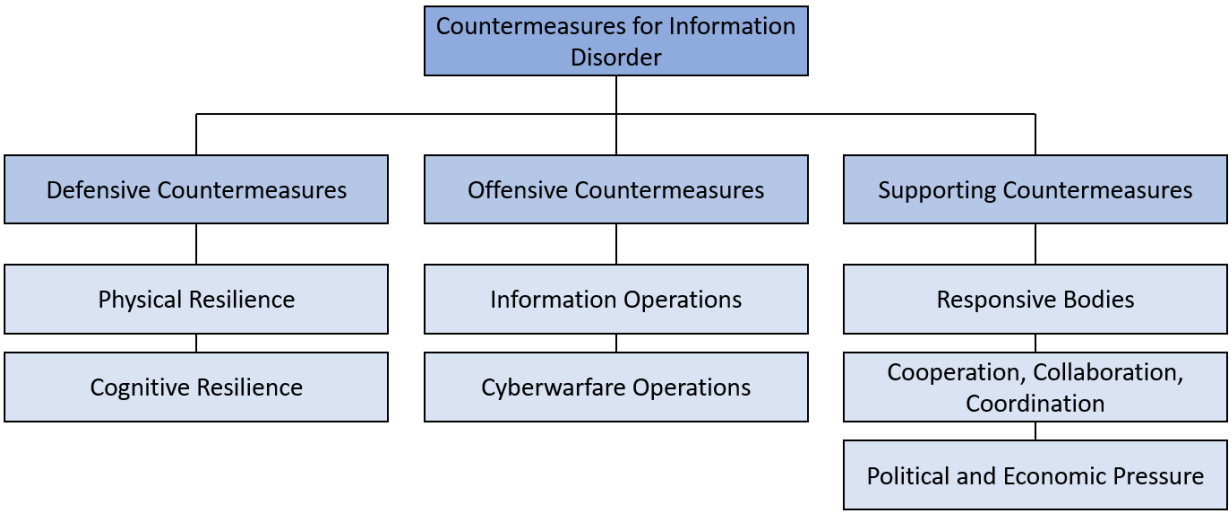

Figure 2: Typological hierarchy of information disorder countermeasures.

Defensive Countermeasures

Current and proposed defensive countermeasures pertain to two primary conditions: either a) managing the information and information flows within a nation's borders, or b) fostering a well-prepared and aware citizenry that can appropriately detect, manage, and challenge information disorder as it is encountered. Bjola and Papadakis (Bjola & Papadakis, 2021) label these *physical resilience* and *cognitive resilience*, respectively. Together, they compose *digital resilience* as a means of highlighting that the object of protection is the public sphere and its "dissolution posed by the digital rise of unruly counterpublics" (p. 16). In focusing on combating fake news (an intimately related concept to information disorder), (Haciyakupoglu et al., 2018) instead arranged approaches along a temporal scale (pre-emptive, immediate, and long term) where physical and

cognitive resiliency are mostly considered immediate or long-term responses (whereas pre-emptive responses I have mostly placed within supporting countermeasures.

Physical Resilience

Bjola and Papadakis liken physical resilience to an "antiviral drug" of sorts, and serves as a reactionary approach as compared to the long-term response of cognitive resilience (Bjola & Papadakis, 2021). Hwang (Hwang, 2019) similarly characterizes these measures as centered within public systems as the construction of "defensible publics" which detect and foster "robust social networks within society" (p. xiv).

Fact-checking operations serve as a well-known example of this. The civilian-led "Baltic Elves" monitor and analyze information threats in Estonia (Robbins, 2020). Polygraph.info, a website where journalists expose Russian disinformation in both English and Russian, provides a fact-checking hub with an eye towards bridging Russia and the West (Perkins, 2018). Hall (Hall, 2017) reports Lithuanian citizens identifying hate speech and pro-Russian accounts alongside blogging and media to identify and delete extreme pro-Russian comments on social media platforms, Czechia's anti-fake news unit, and Ukraine's "StopFake" program that fact checks and discredits Kremlin disinformation. Fact-checking emphasizes civil society mobilization in stopping disinformation in the public sphere (Robbins, 2020), as well as the role professionals in key positions can play in information curation, such as diplomats (Bjola, 2018).

Bontcheva and Posetti (Bontcheva & Posetti, 2020b) produced a typology of responses to disinformation that consolidates aspects of fact-checking (investigation and monitoring) within a larger set of responses intended to preserve the information ecosystem. This includes targeting producers and distributors with campaigns and policy, and targeting the technical (e.g., algorithmic) aspects of disinformation, such as those used by social media platforms. This latter proposal speaks to physical resiliency being also viewed in technical terms, such as developing laws and technology like classifiers to detect bots and fake news (Gradoń et al., 2021; Haciyakupoglu et al., 2018; Kertysova, 2018; Verstraete et al., 2017). The noted weakness about many cutting-edge technical approaches is its lack of transparency that makes it difficult to communicate the rationale behind automated identification of false or misleading information (Kirchner & Reuter, 2020).

Much of the described and proposed effort focuses on social media companies, as discussed by Bodine-Baron et al. (2018) with regards to private industry-centered approaches like algorithm revision and professional codes of conduct, and their issues with preserving freedom of speech on digital platforms. Kertysova (2018) suggests that social media platforms can de-emphasize and correct false content and promote greater accountability and transparency in algorithms that underlie these platforms. Polyakova and Fred (2019) likewise propose a raft of approaches for social media companies to take, such as reforming algorithms and even the concerning proposal to eliminate anonymous accounts. However, social media companies' profit-driven interests make efforts to counter disinformation challenging as sensationalism can drive sales (Polyakova & Fred, 2019).

Markets however can also be leveraged to counter information disorder. For instance, Verstraete et al. (2017) draw on Lawrence Lessig's (1998) four modalities to constrain behavior (law, norms, markets, and architecture) to present many different means of countering digital information disorder, including fostering physical resiliency. Google is blocking ad revenue to information disorder sources, leveraging market disincentives. Multiple platforms are explicitly tagging results with fact-checking flags, leveraging architectures (in the form of code). Verstraete et al. propose (or cite other's proposals) to leverage the law such as through defamation exceptions to remove libelous statements, markets like Arbel's "truth bounties" that reward people for proving stories false, coding architecture such as using algorithmic evaluation of news, and norms such as through alerting users when they are risk of consuming false information. There is notable overlap across these modalities when considered within a digital resilience framing, as Verstraete et al. point out that efforts in markets, law, and architecture can promote certain norms, which has a strong connection to cognitive resilience.

Cognitive Resilience

Cognitive resilience focuses on the individual constituents of the public sphere, and how they respond to disinformation. The objective is to prevent information disorders from "taking root and being internalised by members of the target audience" (Bjola & Papadakis, 2021), citing (Hansen, 2017). While (Bjola & Papadakis, 2021) analysis conceptualizes cognitive resilience in terms of media literacy and strategic communication, I also argue that the fostering of trust in institutions (media, scientific, government) constitute an additional form through likewise fostering awareness and critical thinking capacities in members of the public.

Educational and training programs to develop media literacy are popularly cited and proposed as an area of continual advancement in developing resiliency (Bontcheva & Posetti, 2020b; Haciyakupoglu et al., 2018; Hall, 2017; Jopling, 2018; Kertysova, 2018; Miyamoto, 2021; Perkins, 2018). While physical resiliency can be analogized to an anti-viral, cognitive resiliency is akin to a vaccination (Bjola & Papadakis, 2021). In countries like Estonia with a long history of being targeted by, building media literacy through education is a national mandate that begins in Kindergarten and continues all throughout educational life, integrating media literacy concepts such as manipulation of statistics to serve malign ends or art classes that focus on how the eye can be tricked to perceive certain things while ignoring others (Yee, 2022). Haciyakupoglu et al. (2018) speaks to these as long-term responses, alongside developing media literacy, as are approaches to fostering social norms that challenge disinformation, such as through better information sharing practices (p. 12), with due credence given to how efforts in other areas like in law and coding architectures can shift norms (Verstraete et al., 2017).

Bodine-Baron et al. (2018) developed a "disinformation chain" that sequences the relationships of various actors in spreading disinformation and malinformation from Russian sources to targets in the West, and seeks to upset this chain by fostering "consumer knowledge," such as through education at the high school level, that both mitigates the effect of disinformation and deters its use (p. 27). Likewise, (Perkins, 2018) recommends enhanced media literacy and critical thinking skills for Americans at various age groups in the form of government-backed videos and public

service announcements delivered to citizens (thus working hand-in-hand with strategic communication).

The United States however remains behind other Western nations in fostering media literacy, with more focus on physical resilience (Yee, 2022). Nations like Finland and Estonia in close proximity to Russia appear to assume the presence of disinformation in their information ecosystems by virtue of both Russian cross-border broadcasts and domestic Russian diaspora, so cognitive resiliency is prioritized over correcting or restricting information (Hall, 2017; Jopling, 2018).

Bjola and Papadakis also propose strategic communication for fostering cognitive resiliency. These typically state-driven approaches seek to craft a "clear and coherent strategic narrative" to counter information disorder, such as part of a broader containment strategy (Bjola & Pamment, 2016). This typically entails reaching out to groups that are targeted by disinformation (Bontcheva & Posetti, 2020b) in a way that can raise awareness and refute false or misleading claims (Robbins, 2020; Talabi et al., 2022). Similar ideas can be integrated directly into how information is presented, such as with warnings of false or misleading information that promote transparency (Kirchner & Reuter, 2020) and pre-emptive inoculation (Lewandowsky & van der Linden, 2021). These practices can not just be used to better inoculate a group to information disorder, but to respond to its immediate upkeep through crisis communications (Haciyakupoglu et al., 2018).

Finally, the fostering of trust in democratic institutions like a free media, science, and governing bodies is another aspect of cognitive resilience insofar as it provides foundations for being adequately critical of information and curtail the formation of destructive publics (with due credence to the openness to criticality of institutions) (Bontcheva & Posetti, 2020b). Practices like transparency, such as in social media companies (Polyakova & Fred, 2019) and how they present information (Kirchner & Reuter, 2020), journalism (Bontcheva & Posetti, 2020b), governing bodies (de Jong et al., 2017) are mentioned as ways to build trust in countering information disorder. Civil society can likewise be empowered to participate in these measures through the development of trust and information sharing (Miyamoto, 2021).

Offensive Countermeasures

In contrast to defensive countermeasures, "offensive" countermeasures, i.e., operations are designed to impact the information and cyber space of adversarial states. I identified two forms of proposed offensive countermeasures: a) information operations that seek to influence adversarial states, or b) cyberwarfare operations that attempt to damage or hinder digitally based infrastructure.

Information Operations

The first of these, information operations, seek to influence either the civil society (micro-sphere) or decision-making bodies (macro-sphere) of adversarial states, or states vulnerable to targeted information disorder campaigns that seek to expand adversarial "spheres of influence," such as those on NATO's eastern flank. There are or have been Western efforts to communicate and inform the civil societies of Western actions and policies in the international sphere include explaining American foreign policy to the Russian public through broadcasting (Perkins, 2018), beaming fact-

based programming into Europe, particularly those close to Russia's sphere of influence (Hall, 2017), or more generally strengthening the media environment in that region through positive narrative projection (Hedling, 2021). Bodine-Baron et al. (Bodine-Baron et al., 2018) proposes promoting democracy in Russia as a form of deterrence (although they point out that U.S. efforts in this direction are minimal). Likewise, broadcasting initiatives like Radio Free Europe/Radio Liberty (Haines, 2015; Hall, 2017), the Voice of America (Hall, 2017), and CIA operation QRHELPFUL that supported pro-democracy in Poland during Cold War (Jones, 2018) all sought to influence the micro-sphere with a pro-Western or pro-Democracy message as a form of deterrence.

Decision-making bodies, or the "macro-sphere," are likewise targets, as described by the Reagan administration's explicit desire to "change the Soviet system" (Jones, 2018). (Bodine-Baron et al., 2018) motivates this by pointing out that information disorder campaigns would not have occurred without high-level decision-making. Promotion of democracy is therefore used to punitive effect with a goal of shaping adversarial decision-making. For instance, the principle anxiety of Russian decision-makers in preserving or enhancing Russia's place in the international order is preventing the rise of democracy within its borders and perceived sphere of influence (Ambrosio, 2007; Carothers, 2006; Meredith, 2013; Noutcheva, 2018). Macro-sphere targeted campaigns could deter these malign activities. However, it could be perceived as meddling and in turn escalate aggressions (Bodine-Baron et al., 2018), not to mention that broadcasting initiatives from the Cold War era appeared to do little to dissuade Russian active measures (Jones, 2018; Rid, 2020) and so may lack overall efficacy as a tool of deterrence.

Cyberwarfare Operations

In tandem to information operations is the use of cyber warfare as a retaliatory and deterrence mechanism. The use or threat of cyberattacks that include distributed-denial-of-service (DDoS), sensitive data hacks, and viruses can deter or punish malicious information actions. Several scholars and security practitioners have proposed expanding these offensive cyber capabilities (Bodine-Baron et al., 2018; Jones, 2018; Jopling, 2018; Perkins, 2018), although these could escalate aggressions between Russia and the West (as with any offensive operation).

Hwang (Hwang, 2019), viewing offensive operations to counter disinformation more broadly and with a technological orientation, proposes a logic that generalizes across offensive practices: effective obfuscation (obfuscating the origins of a measure), effective iteration (learning and adapting over time), and effective automation (leveraging tools like algorithms on social platforms or bots to maximize scale and reach of persuasion). Thus, while defensive operations are conceptualized within SDMTs, so too can offensive operations be optimized.

Supporting Countermeasures

There are also current and proposed countermeasures that are neither directly offensive nor defensive, but rather support the efficacy other policies and practices or foster their development with necessary infrastructure. Here I discuss a) the bodies of leadership and organization in response to disinformation; b) the cooperation, collaboration, and coordination between different responsive bodies; and c) political and/or economic pressure.

Responsive Bodies

To meet the challenge of information disorder, thought leaders are examining the function of existing organizational responsive bodies (organizations, groups, institutions), or proposing new ones to fill identified gaps within state, private industry, and civil society sectors. For instance, European efforts to foster cognitive resilience have lead to anti-fake news groups in Germany, Czechia, and Ukraine (Hall, 2017); the Estonia Defense League that runs an anti-propaganda blog and responds to physical, cyber, and educational threats (Robbins, 2020); multi-national units to counter disinformation within Europe, NATO, and the EU (Jopling, 2018); and multi-national rapid alert systems for information sharing across the EU/European Council (Robbins, 2020). Proposals to expand these bodies focus on establishing lead agencies and inter-agency organizations to coordinate efforts in the US (Perkins, 2018; Polyakova & Fred, 2019), and better resource and back strategic communications groups like EastStratCom (Polyakova & Fred, 2019).

Cooperation, Collaboration, Coordination

A closely related theme emergent from the development of responsive bodies is the level of cooperation, collaboration, and coordination these bodies can or should enable. As indicative of the state of defensive countermeasures, countering information disorder involves multiple facets of societies, from state to private industry to civil society. The widespread nature of information disorder highlights the need and current shortcomings in cooperation, collaboration, and coordination among responsive bodies.

Drawing on the Reagan administration's AMWG, Perkins (Perkins, 2018) argues for an "interagency" that focuses exclusively on disinformation, staffed by experts and with the power to establish relationships with private industry. Jackson and Lieber (Jackson & Lieber, 2020) argue for a similar interagency approach, but highlights the challenge that a "territorial mindset" that, while being a feature of democratic governance, makes interagency collaboration difficult as egos and power dynamics come into play.

State or multi-national governing bodies also must continue to foster enhanced collaboration. NATO for instance must enhance the coherence and coordination between member states, as well as improving coordination between NATO and the European Union (Jopling, 2018). Growing trans-Atlantic partnerships between Europe and North America likewise are recommended by Polyakova and Fred (Polyakova & Fred, 2019) in the form of a "counter-disinformation coalition" to share experiences, information, and engage with private industry.

The collaboration from state bodies to private industry is likewise proposed as necessary, particularly with regards to social media companies. Haciyakupoglu et al.'s (Haciyakupoglu et al., 2018) literature review suggests this, as well as involving collaboration with NGOs in a pre-emptive manner. Public-private partnerships are also argued for by Bodine-Baron et al. (Bodine-Baron et al., 2018), extended to academia too to explore in particular the technical aspects of disinformation's spread, such as algorithms, data, and software.

Economic and Political Pressure

Finally, nations or multinational institutions can apply political and economic pressure to deter or punish information disorder campaigns, in addition to other forms of warfare, primarily in the form of sanctions. The West already uses sanctions as a tool with regularity, such as in targeting Russian sovereign debt, oligarchs, and products in the international market (Jopling, 2018; Polyakova & Fred, 2019). Perkins (Perkins, 2018) argues for heavy expansion of sanctions against anyone who facilitates Russian information disorder, further restricting financial gain from Western markets. At the same time, circumvention of sanctions via sanction-busting necessitates continuing evolution of the sanctioning apparatus to maintain their efficacy (Jopling, 2018).

Sanctions are also related to the impression they leave in the international community as a form of shaming (Bodine-Baron et al., 2018), which is itself another aspect of supporting countermeasures: leveraging the indignation of the international community. While not necessarily measurable in the same "dollars and cents" form of economic sanctions, they still incur a political cost which plays upon the anxiety of Russian decision-makers about their state's place in the international order and correlates with information operations campaigns that target the macro-sphere of society. This amounts to highlighting the malign activities of these actors (Jones, 2018) in a way that raises the political cost of information disorder campaigns.

The Smoothness/Striation Dynamic in The Institution of War

The current and immediate trending state (as suggested by most proposals) reflects assumptions that are stem from the impulse for free flow that information disorder displays. This is readily apparent when we consider that, while North American nations focus primarily on physical resiliency as opposed to European nations that place more emphasis on cognitive resiliency, both approaches make a shared assumption: that information disorder is already present within their information ecosystems. Its penetration is therefore a foregone conclusion. This is noteworthy insofar as it stands in contrast to authoritarian nations: The "Great Firewall of China" that was implemented in 2008 (Sonali et al., 2019) works by identifying and blocking information from particular "IP addresses, TCP ports, DNS requests, HTTP requests, circumvention tools, and even social networking sites" (Ensafi et al., 2015); and Russia has likewise accelerated its separation from external information since its invasion of Ukraine, blocking or restricting information from popular social media sites like Facebook and Twitter (Manson, 2022).

As mentioned earlier, the concepts of smoothness and striation sensitize us to the nature of information disorder along this dynamic and the reflection (or lack thereof) of these qualities in policies and proposals for countering information disorder. The widespread and deeply embedded nature of information disorder in the West is indicative of an information environment that desires smoothness. Authoritarian states however seek striation that mirrors geo-political borders, a process termed "balkanization." The smooth/striation dynamic portrays the global political information environment as asymmetrical, whereby democratic nations in the West adopt information smoothness (albeit not without an ongoing discourse between democratic freedoms and national security) while adversarial authoritarian nations seek to induce striation while leveraging information space smoothness to disseminate and spread information disorder.

Accepting this asymmetry however casts key trends in countering information disorder, while also portending opportunities that are in line with their overall trajectory. The broad emphasis on coordination, collaboration, and information-sharing between sectors of society (Bodine-Baron et al., 2018; Haciyakupoglu et al., 2018; Polyakova & Fred, 2019), between agencies of government (Jackson & Lieber, 2020; Perkins, 2018), and different national governments (Jopling, 2018; Polyakova & Fred, 2019) characterize a response to the smoothness of information disorder's flow. Hanlon's (Hanlon, 2018) broadly captures this characteristic in pointing out how disinformation is resistant to striated-based thinking that confines it to particular platforms, events, or sectors of society. Conception of defensive countermeasures are connected through these coordinating bodies that bridge sectoral and national divides, in essence seeking to match the smoothness of information disorder flow through deep interconnectedness.

Promoting this interconnectedness however can still be further enhanced, which represents a potentially fruitful continuation of the trajectory of Western countermeasures, as well as portending broader societal shifts that require constant monitoring.

Offensive-Defensive Coherence

Polyakova and Fred discuss the "forward-defense" as an approach to countering malign information actors by way of deploying offensive measures to defend one's own information and cyber spaces (Polyakova & Fred, 2019). While their application entails offensive operations as deterrence and punishment (thus making defense easier), combining thinking around defense and offense in a deeper way can have multiple benefits. For one thing, there is a strong connection between practices for resiliency and information operations: programs to educate cover media literacy within the West while operations like Voice of America and Radio Free Europe likewise educate citizens of adversarial states about Western and American policies. Using education and media literacy as a starting point, we can develop programs that educate citizens both in the West and in adversarial states (albeit through differing modes of delivery as necessitated by those states' information control policies). These "combined measures" have the added benefit of promoting greater information sharing between offensive and defensive thinking on information disorder, bringing scholars, industry leaders, and policymakers into a conceptual space that is more broadly perceptive of information warfare than strictly their own disciplines or interests (See Figure 3 below for one such proposed combined measure).

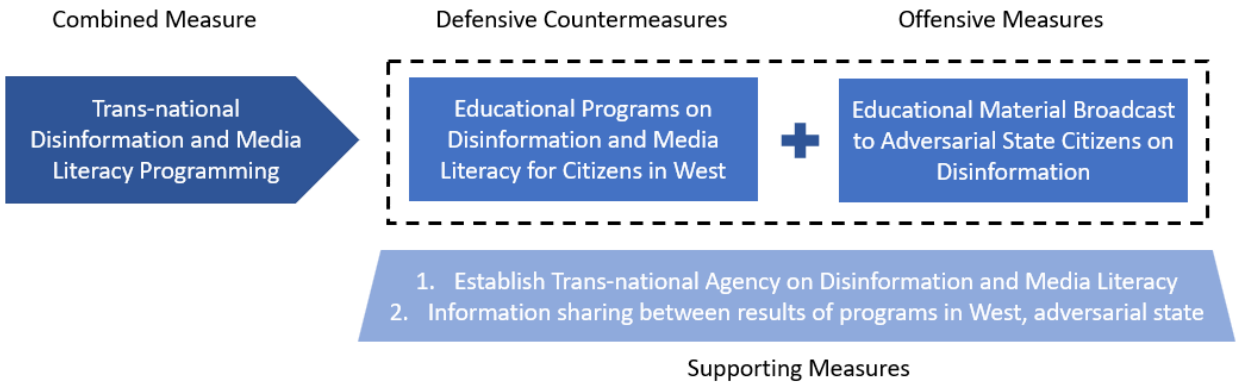

Figure 3: Example of combined countermeasure.

There are of course numerous practical, legal, and political challenges to these measures, many of which are touched on by the scholarship already, but the takeaway should be that progress towards a "unified strategic concept" as described by Hwang (Hwang, 2019) will benefit from, if not necessitate, the cooperation, coordination, and collaboration of leaders from multiple disciplines under the major facets of disinformation *in coherence*: defense, offense, and support.

Thinking Beyond the Military-Security Apparatus

Civil society and private sector involvement is the central component of developing resiliency but are largely ignored when it comes to offensive operations that seek to deter or punish. Instead, information operations are conceptualized as a part of the state (e.g., Radio Free Europe as a U.S. government funded organization) and cyberwarfare is conceptualized as a part of the state's military apparatus. This feature of the thinking around deterring and punishing disinformation campaigns misses the fact that these actors are already involving themselves in offensive operations, such as hacker group Anonymous targeting Russian institutions and government data following the latter's escalation of their invasion of Ukraine (Pitrelli, 2022) or the information operations and cyberattack campaigns Ukrainian resistance is currently undertaking (work forthcoming). This is a noteworthy observation within the context of how policymakers and scholars differentiate responsibilities between offensive and defensive operations: there is a desire to empower civil society actors and to articulate private sector responsibilities with regards to resilience, but little commensurate interest in involving them in operations that reach into adversarial states. This also has implications for developing offensive-defensive coherence, as territorial borders between who can participate in either aspect of challenging information disorder need to be reviewed and potentially broken down with the knowledge that information disorder is a "whole-of-society" challenge and not just the domain of a nation's military-security institution.

The Broad Implications of a State of All-Encompassing War

I would like to take a step back at this time and consider the trajectory of countermeasures to information disorder within the broader context of what a combination of the emerging hybrid warfare frame of mind and the hybrid socio-information space of trans-national information flow. Manuel DeLanda (1991) characterizes a shift in warfare when mobile artillery became widely

available, which forced changes in strategic and tactical approaches to war and its architecture. Artillery, once the domain of relatively static armies due to their size and difficulty in transporting (e.g., a trebuchet) became available in a mobile form, such as cannons pulled by horses. DeLanda describes this as the *nomadization* of the army, drawing on the concept of nomad inseparable from Deleuze and Guattari's smoothness/striation dynamic. Nomadization entails that artillery as part of the army could be deployed in a smooth, unbounded way, distanced from any central location or fortification and instead in the field. High walls that were once useful for keeping invaders out became little more than bigger targets, rendered obsolete by the availability of mobile artillery.

Widespread information disorder practices likewise portend a shift in the architecture of war. Like the breaking down of high castle walls, information disorder within Western democracies evades attempts to prevent its flow. It has a *nomadic impulse* that induces a smoothness across the hybrid socio-information space that information disorder exists within. The nomadic impulse of information disorder has in turn lead to a smoothness of the topology of warfare, doing away with typical indicators of its striation such as established frontlines. Just as mobile artillery changed the architecture of war. The trajectory of modern war is increasingly (to borrow the technological model of smoothness and striation (Deleuze & Guattari, 1987a)) like felt over fabric, where interconnected fibers weave throughout society in unpredictable ways to come together to form a texture free of identifiable fronts, and in turn separate military and civil societies. This is at least partially a result of the shift over time of war from something conducted over and on geographic space to something that's also fought with equal intensity in cyber space.

So, what are the possible results of matching the trajectory of information disorder's nomadic impulse with commensurate policies? It portends the beginning of a shift in the institution of war as no longer the domain of the state's military institutions on a new scale. The hybrid conception of war passes its practice into the state of all-encompassing, where civil society, private industry, and everything in-between are as much included in the practices of war as soldiers and generals. Information is given comparable regard to artillery, and a tweet is tantamount to a bullet.

This also may portend a move beyond the notion of hybrid warfare frameworks as still being a conception of asymmetrical warfare. This is because, while asymmetrical warfare is constitutive of multiple battlefronts arrayed throughout the spaces of adversaries, the "whole-of-society" shift that information warfare brings is moving towards such deep embeddedness so as to be something qualitatively distinct. This can be captured in an expression: if war is everywhere, then war is nowhere. All actors within society are exposed to it and can likewise (sometimes unwittingly) play an active role in it, involving themselves in the practice of warfare. Thus, the hybrid conception of warfare, information's central role in it, and information's nomadic impulse (as indicative of information disorder) results in a battlefield so imbued into the fabric of society so as to be indistinguishable from it. War then becomes a way of life, invisible by virtue of its ubiquitous embeddedness while simultaneously all-encompassing.

The natural and more immediate trends then will likely be the greater involvement of all sectors of society in not just building resiliency, but also participation in offensive operations that currently the domain of a state's military apparatus. For instance, civil society actors are already becoming more involved in conducting cyberwarfare, such as in DDOS or hacking. To what degree the state

assists, directs, or coordinates with actions like this remains to be seen, but it is suggestive of the trend of all-encompassing warfare in the name of information and cyber security.

Concluding Remarks

Russia's renewed aggression against Ukraine reminded the West of not just Russia's readiness to commit to a full-scale invasion of its neighbors, but also the integration of information- and cyber-space efforts into those full-scale war efforts. Most notable is the political use of information disorder, particularly disinformation and malinformation (which can further spur misinformation). In this article, I sought to analyze the space of countermeasures to information disorder in the literature and view them through a lens that highlights the fundamental realities of information in today's digital environment.

There are two layers to what I have claimed in this piece: a) that there are opportunities to leverage greater coherence across societal sectors and geo-political boundaries that reflect the purposeful leveraging of information disorder smoothness to further political aims, and that in fact Western policies for countering information disorder may very well be trending in this direction; and b) that this direction will have deep implications for societal organization in the long-term, which will continue to stress the tenets of democracy. While we know that hybrid warfare frameworks (although itself not a new concept) are challenging how Western security and military leaders think about conflict, it cannot be overstated that conflict is trending away from being the strict domain of a state's security apparatus. Rising hybrid warfare policies are motivating a whole-of-society war-readiness that reflects the nomadism of information and portends a state of all-encompassing war. For policymakers and professionals in the telecommunications and digital media industries, leveraging the whole-of-society approach can produce novel and efficient countermeasures, but the broader implications have untold and potentially deep consequences for the state-civil society distinction and democracy in the digital information age.

References

Abrams, S. (2016). Beyond Propaganda Soviet Active Measures in Putin's Russia Beyond Propaganda: Soviet Active Measures in Putin's Russia. *Connections: The Quarterly Journal*, *15*(1), 5–31.

Allcott, H., & Gentzkow, M. (2017). Social Media and Fake News in the 2016 Election. *Journal of Economic Perspectives*, *31*(2), 211–236. https://doi.org/10.1257/jep.31.2.211

Ambrosio, T. (2007). Insulating Russia from a colour revolution: How the Kremlin resists regional democratic trends. *Democratisation*, *14*(2), 232–252.

Bayer, J., Bitiukova, N., Bard, P., Szakacs, J., Alemanno, A., & Uszkiewicz, E. (2019). *Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States*. European Parliament.

Bjola, C. (2018). The "dark side" of digital diplomacy: Countering disinformation and propaganda. *Countering Online Propaganda and Extremism*, *January*, 1–10. https://doi.org/10.4324/9781351264082

Bjola, C., & Pamment, J. (2016). Digital Containment: Revisiting Containment Strategy in the Digital Age. *Global Affairs*, *2*(2), 131–142.

Bjola, C., & Papadakis, K. (2021). Digital propaganda, counterpublics, and the disruption of the public sphere: The finnish approach to building digital resilience. In *The World Information War: Western Resilience, Campaigning, and Cognitive Effects* (pp. 186–213). https://doi.org/10.4324/9781003046905-15

Bodine-Baron, E., Helmus, T., Radin, A., & Treyger, E. (2018). Countering Russian Social Media Influence. In *Countering Russian Social Media Influence*. https://doi.org/10.7249/rr2740

Bontcheva, K., & Posetti, J. (Eds.). (2020a). *Balancing Act: Countering Digital Disinformation While Respecting Freedom of Expression*. International Telecommunication Union (ITU).

Bontcheva, K., & Posetti, J. (Eds.). (2020b). *Balancing Act: Countering Digital Disinformation While Respecting Freedom of Expression*. International Telecommunication Union (ITU).

Carothers, T. (2006). The backlash against democracy promotion. *Foreign Affairs*, 55–68.

Clausewitz, C. V. (2010). *On War*. Pacific Publishing Studio.

de Jong, S., Sweijs, T., Kertysova, K., & Bos, R. (2017). *Inside the Kremlin House of Mirrors: Liberal Democracies can Counter Russian Disinformation and Societal Interference*.

DeLanda, M. (1991). *War in the Age of Intelligent Machines*. Zone Books.

Deleuze, G., & Guattari, F. (1987a). 1440: The Smooth and the Striated. In *A Thousand Plateaus: Capitalism and Schizophrenia* (pp. 474–500). University of Minnesota Press.

Deleuze, G., & Guattari, F. (1987b). *A Thousand Plateaus: Capitalism and Schizophrenia*. University of Minnesota Press. https://doi.org/10.4324/9780203584200

Deleuze, G., & Guattari, F. (1987c). *A Thousand Plateaus: Capitalism and Schizophrenia*. University of Minnesota Press. https://doi.org/10.4324/9780203584200

Ensafi, R., Winter, P., Mueen, A., & Crandall, J. R. (2015). Analyzing the Great Firewall of China Over Space and Time. *Privacy Enhancing Technologies Symposium (PETS)*, 61–76. https://doi.org/10.1515/popets-2015-0005

Erlich, A., & Garner, C. (2021). Is pro-Kremlin Disinformation Effective? Evidence from Ukraine. *International Journal of Press/Politics*, 1–24. https://doi.org/10.1177/19401612211045221

Gerasimov, V. (2016). The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations. *Military Review*, 23–29.

Glaser, B. G., & Strauss, A. (1967). *The Discovery of Grounded Theory: Strategies for Qualitative Research*. AldineTransaction.

Gradoń, K. T., Hołyst, J. A., Moy, W. R., Sienkiewicz, J., & Suchecki, K. (2021). Countering misinformation: A multidisciplinary approach. *Big Data & Society*, *8*(1), 205395172110138. https://doi.org/10.1177/20539517211013848

Habermas, J. (2010). The Public Sphere: An Encyclopedia Article. In *Crime and Media: A Reader* (pp. 11–19). Routledge.

Haciyakupoglu, G., Hui, J. Y., Suguna, V. S., Leong, D., & Rahman, M. F. B. A. (2018). *Countering Fake News: A Survey of Recent Global Initiatives* (Issue March).

Haines, J. R. (2015). *Countering Russian Disinformation: Europe Dusts Off "The Mighty Wurlitzer."*

Hall, H. K. (2017). The new voice of America: Countering Foreign Propaganda and Disinformation Act. *First Amendment Studies*, *51*(2), 49–61. https://doi.org/10.1080/21689725.2017.1349618

Hanlon, B. (2018). *It's Not Just Facebook: Countering Russia's Social Media Offensive* (Issue 019).

Hansen, F. S. (2017). *Russian hybrid warfare: A study of disinformation*.

Hedling, E. (2021). Transforming practices of diplomacy: The European External Action Service and digital disinformation. *International Affairs*, *97*(3), 841–859. https://doi.org/10.1093/ia/iiab035

Helmus, T. C., Bodine-Baron, E. A. (Elizabeth A., Radin, A., Magnuson, M., Mendelsohn, J., Marcellino, W., Bega, A., Winkelman, Z., Rand Corporation. National Security Research Division., National Defense Research Institute (U.S.), International Security and Defense Policy Center., Rand Corporation, & United States. Department of Defense. Office of the Secretary of Defense. (2018). *Russian social media influence: Understanding Russian propaganda in Eastern Europe*.

Hwang, T. (2019). *Maneuver and Manipulation: On the Military Strategy of Online Information Warfare*.

Jackson, M., & Lieber, P. (2020). Countering Disinformation: Are We Our Own Worst Enemy? *The Cyber Defense Review*, *5*(2), 45–56.

Jones, S. G. (2018). *Going on the Offensive: A U.S. Strategy to Combat Russian Information Warfare*.

Jopling, Lord. (2018). *Countering Russia's Hybrid Threats: An Update* (Issue October).

Kertysova, K. (2018). Artificial Intelligence and Disinformation: How AI Changes the Way Disinformation is Produced, Disseminated, and Can Be Countered. *Security and Human Rights*, *29*, 55–81. https://doi.org/10.1163/18750230-02901005

Kirchner, J., & Reuter, C. (2020). Countering Fake News: A Comparison of Possible Solutions Regarding User Acceptance and Effectiveness. *Proceedings of the ACM on Human-Computer Interaction*, *4*(CSCW2), 1–27. https://doi.org/10.1145/3415211

Lessig, L. (1998). The New Chicago School. *The Journal of Legal Studies*, *27*(2), 661–692.

Lewandowsky, S., & van der Linden, S. (2021). Countering Misinformation and Fake News Through Inoculation and Prebunking. *European Review of Social Psychology*, *32*(2), 348–384. https://doi.org/10.1080/10463283.2021.1876983

Low, J. (2019). A Pragmatic Definition of the Concept of Theoretical Saturation. *Sociological Focus*, *52*(2), 131–139. https://doi.org/10.1080/00380237.2018.1544514

Manson, K. (2022, March). Russia's Invasion is Accelerating Splinternet, French Envoy Says. *Bloomberg US Edition*.

Meredith, K. (2013). Social Media and Cyber Utopianism: Civil Society versus the Russian State during the "White Revolution," 2011-2012. *St Antony's International Review*, *8*(2), 89–105.

Miyamoto, I. (2021). Disinformation: Policy Responses to Building Citizen Resiliency. *Connections: The Quarterly Journal*, *20*(2), 47–55. https://doi.org/10.11610/Connections.20.2.05

Murray, W., & Mansoor, P. R. (2012). *Hybrid warfare: Fighting complex opponents from the ancient world to the present*. Cambridge University Press.

Noutcheva, G. (2018). Whose legitimacy? The EU and Russia in contest for the eastern neighbourhood. *Democratization*, *25*(2), 312–330.

Nunes, M. (1999). Virtual Topographies: Smooth and Striated Cyberspace. In M. L. Ryan (Ed.), *Cyberspace Textuality: Computer Technology and Literary Theory* (pp. 61–77). Indiana University Press.

Perkins, A. M. (2018). *Soviet Active Measures Reborn for the 21st Century: What is to be done?* (Issue December). Naval Postgraduate School.

Pitrelli, M. B. (2022, July 28). Hacktivist group Anonymous is using six top techniques to "embarass" Russia. *CNBC*.

Polyakova, A., & Fred, D. (2019). *Democratic Defense against Disinformation 2.0*.

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

Robbins, J. (2020). Countering Russian Disinformation. In M. F. Cancian, C. Newlin, R. Person, J. Golby, G. Barndollar, J. McGlynn, & J. Robbins (Eds.), *The Diversity of Russia's Military Power: Five Perspectives* (pp. 32–39). Center for Strategic & International Studies (CSIS). https://doi.org/10.55540/0031-1723.2850

Sonali, C., Zang, J., Yu, Y., Sun, J., & Zhang, Z. (2019). The golden shield project of China: A decade later-an in-depth study of the great firewall. *International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*, 111–119. https://doi.org/10.1109/CyberC.2019.00027

Talabi, F. O., Ugbor, I. P., Talabi, M. J., Ugwuoke, J. C., Oloyede, D., Aiyesimoju, A. B., & Ikechukwu-Ilomuanya, A. B. (2022). Effect of a social media-based counselling intervention in countering fake news on COVID-19 vaccine in Nigeria. *Health Promotion International*, *37*(2), daab140. https://doi.org/10.1093/heapro/daab140

United States Information Agency. (1992). *Soviet Active Measures in the "Post-Cold War" Era 1988-1991*.

Verstraete, M., Bambauer, D. E., & Bambauer, J. R. (2017). Identifying and Countering Fake News. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3007971

Wardle, C. (2018). *Information Disorder: The Essential Glossary* (pp. 1–8). Harvard Kennedy School.

Wardle, C., & Derakhshan, H. (2017). Information disorder: Toward an interdisciplinary framework for research and policy making. *Council of Europe Report*, 1–108.

Woolley, S. C., & Howard, P. N. (2016). Political communication, computational propaganda, and autonomous agents: Introduction. *International Journal of Communication*, *10*.

Yee, A. (2022, January). The country inoculating against disinformation. *BBC*.

Appendix

The following tables categorize current and proposed measures to countering information disorder, particularly of a political nature.

Appendix A: Physical and Cognitive Resilience Countermeasures

Author(s), Year	Current Countermeasure	Proposed Countermeasure
Bjola, 2018	• Diplomats: ignoring trolling, other information disorders. • Diplomats: conducting fact-checking. • Diplomats: "turning the tables" on information disorder, e.g., humor.	
Bjola & Papadakis, 2021		• Education (media literacy). • Validate truth claims. • Contain emotional escalation. • Prevent radicalisation. • Reinforce integrity of the public good.
Bodine-Baron et. al., 2018	• Legislation of social media companies. • "Remove, reduce, inform" approach.	• Limit Russian proxies. • Reduce the effects of information disorder amplification. • Education (consumer knowledge, judgment).
Bontcheva & Posetti, 2020		• Education (media literacy). • Rebuild trust in institutions. • Monitoring, investigations of information disorder. • Counter-disinformation campaigns • Targeting technical aspects of digital information disorder e.g., algorithms, • Target audience of disinformation e.g., norms and ethics,
Gradon et al., 2021		• Use data science to identify information disorder (e.g. classifiers, agent-based modeling).
Haciyakupoglu et. al., 2018	• Hold social media companies accountable for spread • Law and technology to detect bots and fake news.	• Education (media literacy). • Develop measures for crisis communications and fact-checking. • Define, communication responsibilities for tech companies.
Hall, 2017	• Lithuania: citizen reporting of hate speech, pro-Russian social media accounts. • Finland: Education (media literacy).	• Enable civil society to do fact-checking, develop counter-narratives. • Education (media literacy).
Hedling, 2021		• Integrating new diplomats that can transform approaches. • Experiment, adopt new technical approaches. • Transformation in diplomacy practices could reflect changes in partners, other countries' diplomatic practices.
Horowitz et al., 2021	• Quality and innovative practices offered by public service media	

	(PSM), as countering information disorder. • PSM providing specialized programs about information disorder, stimulate critical thinking. • PSM growing online communication with youth. • PSM developing projects and collaborations to address information disorder.	
Hwang, 218		• Develop public systems of information disorder detection. • Support robust social networks. • Develop clear policies around state intervention.
Jopling, 2018	• USA: Investigate election interference. • Germany: Conducts network vulnerability analyses; imposes heavy fines on social media companies for not curating information. • Britain: coordinate politicians, media, think tanks on information disorder. • Sweden: trains election workers to spot, resist foreign influence; emphasizes education (media literacy). • Finland: emphasizes education (media literacy). • Social media removing, labeling misinformation.	• Revise educational policies around information disorder.
Kertysova, 2018	• Companies integrating algorithmic detection of information disorder.	• Develop bots to detect information disorder. • Develop better detection of "deep fakes" and other AI-generated information disorders. • Social media companies should de-emphasize, correct false content. • Social media companies should establish greater accountability, transparency in algorithms. • Consider regulating social media content. • Education (media literacy). • Enhance cybersecurity.
Kirchner & Reuter, 2020		• Transparent warnings of false or misleading information on digital platforms.
Lewandowsky & Van Der Linden, 2021		• "Inoculation" via warning people of possible misinformation using weakened examples.
Miyamoto, 2021		• Improve digital literacy. • Integrate digital security into cybersecurity awareness campaigns.

		• Empower civil society to build trust, share information on political actors.
Perkins, 2018	• Social media identifying foreign entities. • Conducting fact-checking. • Educational initiatives on information disorder.	• Education (media literacy) • Enhance fact-checking.
Polyakova & Fred, 2019		• Regulate advertising, sponsored content • Mandate identification of bots, removal of inauthentic accounts. • Consider an online sign-in system for access to the internet. • Mandate a standard “terms of service”. • Targeted fixes of algorithms, e.g., de-rank rather than remove posts. • Foster resilience to information disorder. • Social media companies should reassess anonymity, start algorithmic reforms, increase transparency requirements.
Robbins, 2020	• Czechia: Mobilizing civil society in information defense • Czechia: Coordinating think tank research to review countermeasures, share information, work across variety of threats. • Estonia: Estonian Defense League manages physical, cyber resiliency; providing education for countering information disorder. • Estonia: Foreign news service chronicling information threats. • Estonia: Mobilizing civil society in information defense, e.g. The Baltic Elves. • NATO: Strategic communication to raise awareness, refute false/misleading claims.	•
Talabi et al., 2022		• Counsel people who experience fake news, information disorders.
Verstraete et al., 2017	• Restricting financial opportunities for fake news sources. • Shape digital environment (code as architecture to affect behaviors around information disorder. • Regulations, financial initiatives, coding architecture can articulate better information norms. • Social media, search engines identifying fake news via crowdsourcing, tagging, and fact-checking.	• Arbel’s "truth bounties" where people get paid to prove a story is false. • Shiffrin proposes "norm of sincerity" to govern speech. • Create social media platforms with different financial structures. • Use user feedback to determine where information appears on timeline or news feed. • Social media could evaluate news on their site using algorithms

		• Social media companies can use their reputation, credibility to fight fake news. • Social media companies could alert users when they at risk of consuming false information. • Journalism norms could improve efficacy in combating fake news by reporting context, then describing what the source said.

Table 2: Physical and Cognitive Resilience Countermeasures.

Appendix B: Information and Cyberwarfare Operations Countermeasures

Author(s), Year	Current Countermeasure	Proposed Countermeasure
Bjola, 2018		• Target "gatekeepers" of information disorder with correct information, encouragement not to promote false information. • Diplomats can discredit information disorder sources.
Bodine-Baron et. al., 2018	• Apply cybersecurity to foreign influence operations.	• Seek to shape foreign decision-making.
Hall, 2017		• Beam facts-based programming into countries targeted by political information disorder.
Hedling, 2021		• Strengthened media environment in countries targeted by political information disorder. • Positive narrative projection to targeted countries.
Hwang, 2019		• Effective obfuscation of information warfare efforts. • Effective iteration of efforts to adapt to changing environment. • Effective automation of information warfare roles through leveraging algorithms or bots to shape information environment.
Jones, 2018		• Cyber-offensive operations as deterrence.
Jopling, 2018		• Enhance retaliatory capabilities in cyberspace.
Perkins, 2018	• US: Explaining American foreign policy to citizens of adversarial states. • US: Cyber-offensive operations as deterrence.	• Increase international broadcasting. • Enhance cyber-offensive operations.
Polyakova & Fred, 2019		• Develop "forward-defense" options for deterrence, retaliation e.g., cyberattacks.

Table 3: Information and Cyberwarfare Operations Countermeasures

Appendix C: Coordination and Governance in Support of Countering Information Disorder

Author(s), Year	Current Countermeasure	Proposed Countermeasure
Bodine-Baron et. al., 2018		• Enhance cooperation, coordination among counter information disorder bodies.
Haciyakupoglu et. al., 2018		• Collaborate between industry, NGO, regional bodies on issue-focused pre-emptive measures to information disorder.
Hall, 2017	• Germany: created anti-fake news bureau. • Czechia: created anti-fake news unit. • Ukraine: created StopFake program to combat information disorder.	• Develop civil society media watchdogs. • Develop research institutions oriented to combating information disorder.
Horowitz et. al., 2021		• Enhance the public service media (PSM) sector.
Jackson & Lieber, 2020		• Enhance cooperation, coordination among counter information disorder bodies. • Overcome territorial mindset among agencies • Enhance civil society and industry partnership
Jopling, 2018	• France: hired cybersecurity experts in advance of elections. • Central, Eastern Europe: increased strategic comms budget. • NATO: developed readiness action plan, response force, joint task force • NATO: enhanced cooperation between intelligence agencies. • NATO: supporting centers of excellence (e.g., Strategic Communications Centre) • EU: Establishing institutions for countering hybrid threats (e.g., Joint Communication Hybrid Fusion Cell) • EU: Developing diplomat-led fact-checking.	• Enhance coherence, coordination in NATO, EU. • Enhance overall strategic awareness across nations, international institutions. • Establish further government units to combat fake news
Kertysova, 2018		• Consider breaking up “big tech.” • Additional funding for AI-driven solutions to information disorder.
Perkins, 2018	• US: Coordinating training and education among allied nations.	• US: Establish an interagency group focused on information disorder. • US: Establish strategic communications groups.
Polyakova & Fred, 2019		• Develop lead-agency, coalitions for countering information disorder across allied nations. • Develop rapid alert system to detect and alert on disinformation • US: Hold hearings with social media companies. • US Gov: Fund NGOs and civil society groups fighting information disorder.

		• US: Develop in-government expertise • US: Support a social media regulatory framework. • Europe: Establish, use fact-checker network. • Europe: resource and back EastStratCom group. • Europe: Continue to monitor social media implementation of Code of Practice • Europe: Empower researchers to combat information disorder. • Social media companies should enhance cross-platform coordination, coordination with non-profit groups.
Robbins, 2020	• Czechia: established CTHT, Czech Security Information Service. • Estonia: Established Estonia Defense League (EDL) which runs anti-propaganda blog, operates across variety of security threats. • NATO: Established the NATO Cooperative Cyber Defence Centre of Excellence which develops comprehensive strategy, training, exercises for cyber-readiness. • EU/European Council: created Rapid Alert System to share information across member and allied states.	
Verstraete et. al., 2017	• US: establishing regulations and sanctions punishing information violators.	• US: Federal Trade Commission (FTC) could police information if shown to harm commerce. • US: Defamation exception to first amendment, with right to delist libelous statements from the internet. • US: Reduce risk and cost for platforms to police content via Section 230 in law

Table 4: Coordination and Governance in Support of Countering Information Disorder

Appendix D: Political and Economic Pressure in Support of Countering Information Disorder

Author(s), Year	Current Countermeasure	Proposed Countermeasure
Bodine-Baron et. al., 2018	• Sanctions.	
Jones, 2018		• Warnings against states engaging in malign information activities. • Enhance sanctions (economic, diplomatic). • Highlight malign activities in international community.
Jopling, 2018	• Sanctions.	• Enhanced retaliatory capabilities in cyberspace (as threat).

		• Diversify energy to reduce dependence on adversarial states. • Focus on developing "grey zones," nations that border adversarial states such as in Eastern Europe.
Perkins, 2018	• Sanctions. • Registering foreign agents. • Pursuing recruits of adversarial states as "agents of influence."	• Enhance sanctions.
Polyakova & Fred, 2019		• Enhance sanctions.

Table 5: Political and Economic Pressure in Support of Countering Information Disorder