Democracies and the Future of Offensive (Cyber-Enabled) Information Operations

Dr. Bryan Nakayama

ABSTRACT

Cyber-enabled information operations that exploit social media to shape narratives and societal perception vex Western democracies which have long treated the free flow of information as a virtue. Despite these tensions, Western democracies have sought to adapt their cyber forces both to counter and to manipulate social media and other information operations as an offensive weapon. This article evaluates how these democracies thus far have responded to information operations with a focus on offensive information and cyber operations. The article analyzes three topics relevant to the future of democracies and cyber-enabled information operations. First, is an explanation as to why Western democracies failed to anticipate the threat of cyber-enabled information operations. Second, the article catalogs and compares how four major Western democracies have responded to information operations—US, UK, France, and Germany. The final section evaluates whether and how democracies should practice offensive cyber-enabled information operations, and why, in the end, the article concludes that democracies should avoid offensive cyber-enabled information operations because they pose three tensions that undermine democracy: Internet fragmentation, violations of democratic norms, and blowback.

Bryan Nakayama, a visiting lecturer of International Relations at Mount Holyoke College, focuses on the intersection of emerging technologies and warfare, with emphasis on cyber and information warfare. He is currently working on a book entitled *"From Aerospace to Cyberspace: The Evolution of Domains of Warfare"* that explains the rise of new domains and ways of warfare. bnakayam@mtholyoke.edu

INTRODUCTION

A common belief early in the information age was that the free flow of information in cyberspace reinforced democracy.[1] Scholars and policymakers tended to focus on the impacts of authoritarian attempts to restrict and censor —setting up a conflict between democratizing flows of information and authoritarian censorship. By the mid-2010's indications began surfacing that censorship narrowly understood as filtering information was no longer the only threat to the free flow of information as states increasingly turned to armies of online commenters to shape social media narratives. These efforts to shape social media came to the forefront with the revelations that Russia targeted the 2016 US presidential election with information operations leveraging the scale and reach of American social media platforms.[2] After the US experienced this "strategic surprise," emergent campaigns targeting other Western democracies have brought to the fore questions over how democracies should approach modern cyber-enabled information operations.[3] At the same time that democracies are enhancing their defenses against information threats, they are also integrating information warfare responsibilities into their cyber military organizations, thereby raising a host of normative concerns over the democratic practice of offensive cyber-enabled information operations.

This article explains how democracies have responded to cyber-enabled information operations and discusses whether they should use offensive cyber-enabled information operations for their own goals. Recognizing ongoing terminological debates around what constitutes a "cyber-enabled information operation," this article treats them as information operations that leverage means and dynamics unique to cyberspace—with a particular focus on operations targeting social media.[4] These information operations threaten democracies insofar as they disrupt information flow and quality,

and limited censorship needed to inform democratic debate, and they undermine social trust and faith in news media.[5] While there has been extensive debate and policy focus on how democracies are responding to cyber-enabled information operations, there has been relatively little critical evaluation of whether democracies should conduct offensive information operations.[6] This is a necessary debate as democracies update doctrine and expand the role that their cyber forces place in information warfare.

First discussed is why Western democracies failed to effectively anticipate cyber-enabled information operations, followed by an overview of how democracies have responded across two dimensions: domestic policy and foreign policy. Next offensive information operations by democracies, along with the caveat that a full embrace of these operations risks accelerating Internet fragmentation and domestic blowback. The conclusion argues that democracies on-balance should refrain from cyber-enabled information operations and focus on denial strategies against adversaries using them.

Why Surprise?

Reflecting on the relative inattention paid to how non-Western states have characterized contemporary information warfare, U.S. Cyber Command (USCYBERCOM) historian Michael Warner observes that "millions of Americans and Europeans...view their inherently liberal outlook as no more ideological than breathing, as the pragmatic response to the reality of all unbiased minds. In the same manner, they regard the Internet as something apolitical, as a public utility."[7] Another commentator noted that this is because Western democracies generally assume that free flowing information is politically and economically empowering.[8] Thus, before the rise of authoritarian cyber-enabled information operations, Internet-accessible information was generally viewed as beneficial, as opposed to being a conduit for political manipulation.

This set of beliefs hinges on the epistemological assumption of the marketplace of ideas – that debate in democratic media environments culls incorrect information and produces a form of consensus truth,[9] and the Internet enables flows of information that serves as the grist of democratic debate, thereby strengthening democracy by increasing accountability and allowing for grassroots political organization.[10] The Internet also expanded the economic reach of US and Western firms by insofar as developing and accessing new markets. This perspective originated in the 1990's from the initial set of utopian beliefs in the West that the information age and cyberspace would revolutionize politics by deconcentrating economic and political power.[11]

US policymakers believed in these salutary effects and made it a foreign policy goal during the 1990's and 2000's to promote the spread of the Internet. One key US program was Democracy Promotion during the late 2000's in which the State Department trained activists on how to bypass Internet filtering systems in authoritarian states. Secretary of State Clinton characterized censorship and filtering as an attack on the public's Internet use, making censorship

circumvention a critical element of achieving Internet freedom. Russia and China viewed these programs integral to a larger battle between their political cultures and Western liberalism—the Arab Spring, color revolutions, and domestic protests all Internet driven and dominated by Western values, which drove their approach to the Internet and cyberspace.[12] Over the 2010's Russia and China increasingly turned to large-scale narrative shaping and information disruption on social media as a means of censorship to preserve political stability.[13]

Debate over the security consequences of cyberspace often focused on the potential for a devastating surprise offensive cyberspace operation or "Cyber-9/11," which inspired discussion as to whether cyberspace operations would constitute a potent and independent form of military force akin to kinetic warfare.[14] More recently, scholarship has focused more on how cyberspace operations shape state behavior through longer-term cumulative effects or as intelligence activities.[15] Thus, debates over cyber threats has tended to focus on the potential consequences of infrastructural degradation instead of the manipulation of perception through information operations.[16] As Francois and Lin write: Russian information operations "did not register as a cyber threat according to the accepted conventions of the field, and...did not correspond to a clear and narrow type of threat in traditional cyber conflict literature until after their occurrence and nationwide exposure."[17] The broader social reception of the rise of cyberspace and information technology shaped scholarly and political expectations such that the Russian information operations emerged as a novel threat that challenged existing frameworks by which Western democracies assessed cyberspace threats.

How Western Democracies Have Responded

Fierce, jingoistic rhetoric of some policymakers notwithstanding , polling and experimental research indicate that the US and UK likely will not support retaliation with force unless cyber or information operations create lethal effects.[18] In lieu of using force, scholars have suggested several alternative responses, e.g., domestic regulation of social media,[19] policies that revitalize democratic debate and domestic information environments,[20] creation of norms against offensive cyber-enabled information operations,[21] and creation of a separate democratic intranet.[22]

In response to cyber-enabled information operations Western democracies including the US, UK, France, and Germany typically elevate and integrate information operations with existing military cyber organizations, and, other than the proposed democratic intranet, have pursued some combination of the aforementioned domestic proposals. This section briefly surveys early 2022 efforts by these four named democracies to counter and integrate cyber-enabled/information operations through domestic policy, military organization, and doctrine, and closes with observations focused on cyber-enabled information operations in Russia's 2022 invasion of Ukraine.

United States

As host to many of the world's dominant technology and social media firms such as Google, Microsoft, Twitter, and Facebook, the US is powerfully positioned to control and manage information operations, but the government has yet to meaningfully legislate the governance or structure of such operations. Congress considered the "Honest Ads Act" in 2017, which would increase disclosure and archiving requirements for political advertising on social media, but little legislative progress has occurred in the intervening years.[23] Instead, the US has focused on using law enforcement,[24] diplomatic,[25] sanctions,[26] and military measures.

The US pioneered the military approach to cyber-threats with the 2009 creation of USCYBERCOM, yet this focus did not adequately anticipate information operations that leveraged social media.[27] Initial cyberspace operations doctrine, such as the Air Force *AFDD 3-12*, explicitly distinguished cyber and information operations stating that they were distinct.[28] However, the Russian campaign against the US presidential election pushed the US military to take seriously the relationship between cyber and information operations with recent doctrine explicitly acknowledging this link.[29] At the same time that the link between information and cyber operations gained greater acknowledgment in doctrine, USCYBERCOM and the services have been moving to better integrate information operations into their respective cyber units.[30] However, the effectiveness of this integration is in question as conceptual slippage between the reality and perception of information operations persists in debates over information operations.[31] The US today is nesting its military response to cyber-enabled information operations under the aegis of its broader cyber operations framework.

Reflecting these doctrinal and organizational changes, the US military has responded to adversary information operations by employing both cyber and information operations. First, employing traditional cyberspace operations will deny adversaries the ability to conduct information operations. This can be seen in the 2018 USCYBERCOM operation, which disrupted the Internet Research Agency's internet access, thereby preventing it from accessing social media.[32] Second, while fewer details about precise methods are known the US military has countered disinformation campaigns—such as those that have targeted NATO exercises—with counter-narratives.[33] Whether these involved bot farms or other large-scale efforts to shape social media is unclear, similarly there have been no reported instances of the military seeking to shape domestic narratives. While the US had an early lead in cyberspace operations, it is rapidly expanding its information operations capability.[34]

United Kingdom

The UK's domestic policy response to information operations has intersected with a broader debate over how to manage harmful Internet content. As of 2021, the UK parliament has been debating a sweeping "Online Safety Bill" which would address a range of issues related to online content, of which tackling state-sponsored disinformation is only a part. The bill's emphasis on content moderation has drawn criticism over concerns that it may harm the

capacity for free expression.[35] To counter disinformation there also have been national education campaigns to increase societal resilience and otherwise how best to discern disinformation and evaluate news sources.[36]

Outside of domestic policy, the UK's military has expanded and integrated information operations capabilities into its military cyber forces. The second edition of the Cyber Primer argues that there is substantial overlap between information operations and cyber operations, but they are distinguished on the basis of the operating environment: cyber operations are conducted in cyberspace whereas information operations are conducted across domains.[37] Organizationally, the UK first created the National Security Communications Unit in 2018,[38] however, there is little publicly available information about the unit's activities. In 2019, the British Army re-activated and re-organized the 6th (United Kingdom) Division which is a multi-disciplinary unit tasked with integrating cyber, information, and electronic warfare.[39] Finally, in 2021 the National Cyber Force was founded, and the 2022 National Cyber Strategy document identified countering online disinformation and defending democratic integrity as key functions of the force.[40]

Like the US the UK has countered information threats with cyber and information operations. The UK conducted operations against Daesh—targeting their ability to spread propaganda online.[41] Information operations conducted by the UK have supported NATO operations by defending against false or exaggerated narratives.[42] One notable area of activity where the UK has combined cyberspace and information operations has been in responding to coronavirus misinformation. While details are thin it was revealed in 2020 that the British Army's 77th Brigade was monitoring and acting against foreign coronavirus misinformation campaigns in conjunction with GCHQ. While no details were reported, one account credited GCHQ with use of cyber operations to take down websites that were spreading misinformation.[43]

France

Unlike the UK and US, France has enacted aggressive and controversial domestic policy to counter information operations. In 2018 the French parliament approved an anti-misinformation law that centered on the news environment surrounding elections and empowered a range of actors to punish and restrict the flow of misinformation. The law defines misinformation as "inexact allegations or imputations, or news that falsely report facts, with the aim of changing the sincerity of a vote." Individuals, political parties, and the government are allowed to report misinformation and if found to be in violation judges are empowered "to act 'proportionally' but 'with any means' to halt their dissemination."[44] In addition to a reporting system, the law obligates social media firms to cooperate with takedown orders and provide tools that flag misinformation. Finally, it empowers French broadcast regulators to ensure compliance and revoke the broadcast rights of television and radio news networks.[45] Since 2018, France has expanded its legal framework for managing misinformation by, for example, obligating social media firms to delete certain types of content with as little as one hour's notice.[46]

In conjunction with an aggressive domestic policy regime to manage misinformation, the French military is vigorously integrating information operations and cyber operations. While France's 2018 Offensive Cyber Doctrine focused primarily on cyberspace operations without extensive discussion of their link to information operations,[47] the October 2021 doctrinal publication "Éléments Public De Doctrine Militaire De Lutte Informatique D'influence" emphasizes the role of information operations. Integrating military and non-military disciplines such as the social sciences, the doctrinal statement centers "information space" operations on countering adversary information campaigns.[48] This new doctrinal focus on information operations complements the French Ministry of Defense's efforts to expand existing cyber forces.[49]

France's strong domestic policy regime and recent expansions of information and cyber forces make more challenging discerning the French military's role in countering foreign disinformation campaigns. Yet France is the only Western democracy credited by Facebook with running a coordinated disinformation campaign using its website. In December 2020 Facebook reported that it had taken down a network of French-linked Facebook accounts that had been waging a coordinated disinformation campaign in Mali and the Central African Republic to counter a disinformation campaign funded by a Russian oligarch.[50] This is one of the few known instances of contemporary offensive cyber-enabled information operations attributed to a Western democracy.

Germany

Overall, Germany has faced comparatively fewer foreign information threats,[51] with disinformation around the recent election coming largely from domestic sources.[52] Similar to France, in 2017 Germany enacted a law to strengthen regulation of social media content. However, this law focused primarily on enforcing take-down requirements for hate speech and other abusive content, but unlike the French law, is less directed against foreign-led coordinated disinformation campaigns.[53]

Germany's military response is led by the Cyber and Information Domain Service which was established in 2017. The service combines offensive cyber, electronic warfare, and information activities in one organization.[54] Additionally, in September 2021 Germany adopted a new cybersecurity strategy that emphasized the link between information and cyber operations.[55] However, given the relative newness of the command combined with the fact that Germany has previously prioritized defensive over offensive cyber efforts, there is little available knowledge of offensive German information or cyber operations.

Russia's Invasion of Ukraine

The 2022 Russian invasion of Ukraine will serve as a key event for evaluating the role of cyber-enabled information operations and democratic responses. However, at the time of writing in Spring 2022, the invasion remained in its early stages yet certain preliminary

observations can be made since information operations are ongoing. First, social media and Internet infrastructure firms have been extremely proactive in restricting and banning Russian users and in particular Russian state media outlets.[56] This may eventually lead to the creation of a de facto authoritarian internet as Russia responds by on-shoring internet infrastructure and increasing the scope of state censorship.[57] Second, the US and UK chose a risky public diplomacy strategy—traditional informational operations—in the run-up to the invasion by publicly messaging about Russia's invasions plans in hopes of disrupting them.[58] To help shape narratives on social media, the White House also briefed social media influencers.[59] Finally, Ukraine seems to have won the perception war on social media—for now—through the creative use of memes and gripping first-person narratives to shape global public opinion in their favor.[60] These preliminary observations suggest that private firms and democracies have been much more proactive in shaping the information environment in the run-up the invasion.

Offensive Cyber-enabled Information Operations by Democracies

The previous section briefly summarizes how powerful Western democracies recently have steadily integrated offensive cyber and information operations in both doctrine and organization, giving comparatively little attention to how and whether to use cyber-enabled information operations. As democracies further integrate disciplines necessary for information operations into their cyber forces, there will be an increasing temptation and capacity to use offensive cyber-enabled information operations. There has been little public or scholarly debate over the costs and benefits of employment by democracies of offensive cyber-enabled information operations. This section first outlines how the US pioneered cyber-enabled information operations. Second, it discusses three tensions which democracies must contend with if they are to practice offensive information operations: Internet fragmentation, threats to democratic norms, and blowback.

The United States as Democracy's Pioneer of Offensive Cyber-Enabled Information Operations

While the US engaged in psychological warfare and information operations throughout the War on Terror and Iraq War, these operations were more closely tied to specific military objectives.[61] One of the first instances of large-scale social media manipulation was conducted by the US against Cuba to promote a democratic revolution. More recently, inspired by the role Twitter played in Iran's 2009 Green Movement, the U.S. Agency for International Development (USAID) leveraged a stolen database of Cuban cell phone numbers to create an SMS-based Twitter-like social network called ZunZuneo, which was designed to foment anti-regime activity:

> the US government planned to build a subscriber base through "non-controversial content:"... Later when the network reached a critical mass of subscribers, perhaps hundreds of thousands, operators would introduce political content aimed at inspiring Cubans to

> organize "smart mobs" – mass gatherings called at a moment's notice that might trigger a Cuban spring, or, as one USAID document put it, "renegotiate the balance of power between the state and society."[62]

A key component of the program was profiling and studying the Cuban ZunZuneo subscriber base by assessing political loyalty and openness to revolution. The goals were to "move more people toward the democratic activist camp without detection" and help organize anti-regime "smart mobs." ZunZuneo reached 40,000 Cuban subscribers by early 2011, but USAID ultimately shut-off the service in 2012.[63] USAID's role in the platform was obfuscated through complicated contracting relationships, and ZunZuneo's website had fake advertising placements to render it more authentic. ZunZuneo and USAID ties were not publicly revealed until a 2014 Associated Press report and later congressional investigations.[64]

Other instances of social media manipulation were the product of attempts to reduce terrorist recruitment in Afghanistan and the Middle East. For example, in 2011 it was revealed by the Guardian that the US military had contracted for a platform to manage fake social media persona as part of *Operation Earnest Voice*, to counter online recruitment by terrorist organizations and the Taliban.[65] In testimony to Congress, U.S. General James Mattis described their goal thusly: "we challenge their propaganda. We disrupt the recruiting... We bring out the moderate voices. We amplify those. And in more detail, we detect and we flag if there is adversary, hostile, corrosive content in some open-source Web forum, [and] we engage with the Web administrators to show that this violates Web site provider policies." Responding to criticism of this program, Mattis argued "in today's changing world, these are now traditional military activities. They're no longer something that can only be handled by Voice of America or someone like that."[66] Together, these demonstrate the extent to which the US helped pioneer offensive cyber-enabled information operations with either the goal of spreading democracy or reducing the reach of terrorist recruiters. However, the recent rapid expansion of these capabilities by the US and other Western democracies demands careful consideration of impacted democratic values.

Tensions over Democratic use of Offensive Cyber-enabled Information Operations

Democracies far more than autocracies depend on vibrant information ecosystems to enable democratic debate and accountability. The expansion of the democratic use of offensive cyber-enabled information operations brings with it a host of potential issues that challenge the open Internet and risk further eroding the trust of democratic publics in shared sources of information. This section flags three sources of tension that arise from the democratic embrace of cyber-enabled information operations: first, further Internet fragmentation; second, threats to democratic norms; and finally, information blowback against democratic societies.

Tensions over misinformation and information operations play a key role in accelerating the fragmentation of the Internet and the rise of a "cyber-Westphalia." While some scholars believe that the Internet fragmenting into democratic vs authoritarian networks would be

a positive development,[67] that also would undermine certain benefits of the original cyberspace framework.[68] The reality and perception of information operations was a key driver in the early 2010's push towards greater Internet fragmentation. Chinese and Russian decision-makers viewed the Arab Spring and other political upheavals of the late 2000's/early 2010's as evidence of a novel information warfare threat from the West, and, in particular, the US.[69] While there is no evidence that these upheavals were the product of a US or otherwise Western subversion campaign, the US did aggressively intervene to maintain information flows during the Arab Spring by, for example, having the Voice of America dynamically alter content to defeat web filtering.[70] These efforts to circumvent content filtering combined with the social media manipulation in Operation Earnest Voice contributed to the threat perception of Russian and Chinese decision-makers. Over the next few years, both countries increased their censorship and perception shaping activities—notably with Russia creating a censorship regime akin to China's "Great Firewall."[71] The reaction of France and Germany to information operations—creating or intensifying social media censorship regimes—thus mirrors the earlier actions of Russia and China. Moreover, democratic censorship of disinformation vectors risks increasing Internet fragmentation by prompting a tit-for-tat dynamic. For example, when YouTube deleted several German-language channels run by Russia Today for engaging in COVID disinformation, Russia threatened to block YouTube entirely.[72] Sadly, this threat suggests that Internet fragmentation may occur even if democracies avoid because even defensive measures invite retaliation.

The second tension over democratic offensive information operations is potential threats to democratic norms. Discussing the revelations surrounding the French disinformation campaign in Mali and the Central African Republic the French researcher Alexandre Papaemmanuel comments that: "... to become tougher, should democracies follow the example of authoritarian regimes?... It's a slippery slope."[73] Core democratic norms include freedom of expression and maintaining an information-rich civil society. Offensive cyber-enabled information operations threaten these norms by expanding the government's role in shaping the information environment using methods that are not clearly attributable. This risks both the normative claims that democracies make about their values to the rest of the world as well as the existence of free and open information ecosystems at home. At the same time that the French military was conducting cyber-enabled information operations in Africa, the French government issued a report cautioning against offensive actions.[74] An anonymous European disinformation researcher, commenting on the French campaign, remarked that "You can't complain that Russia is doing this sort of thing, and then turn around and do it yourself."[75] Democracies risk the charge of hypocrisy as different parts of their governments work at cross purposes—some trying to maintain a free and open information ecosystem while others seek to shape perception.

The final tension for the democratic use of offensive information operations is blowback: the unintended consequences that may arise from expanding offensive information capabilities. Western democracies are the home to many private cyber security and surveillance firms that have been implicated in human rights abuses and play a significant contracting role in the provisioning of cyber security.[76] A similar pattern is emerging in information operations and social media disinformation with the rapid rise of firms located in Western democracies offering "disinformation for hire." These firms have been implicated in social media disinformation campaigns in 48 countries worldwide with operations ranging from coronavirus disinformation to targeting elections.[77] At the same time that these firms expand international operations, Western democracies such as the UK, US, and Germany have been wracked by large-scale domestic disinformation campaigns targeting elections led by public relations firms and politicians.[78] The embrace by democracies of offensive information operations risks expanding and deepening the network of private actors conducting disinformation campaigns. Another blowback risk is increasing cynicism about the trustworthiness of news in democratic societies. Many democracies already face declining levels of trust in news media[79] and social media firm's algorithmic curation and content moderation has been frequently attacked as partisan in the US.[80] This decline in trust extends to interactions among social media users, with those accused of being a "Russian bot" becoming a common practice in anglophone social media.[81] Thus, offensive use of information operations by democracies risks increasing this distrust by deepening the perceived partisan bias of social media firms and new media and decreasing social trust. Taken together, the expansion of firms specializing in disinformation and the declining trust in social and news media institutions creates unique risks for democracies that depend on a trusted and vibrant information ecosystem, and they undermine the potential for the development of international norms that could restrain authoritarian misinformation campaigns.

CONCLUSION

Despite the rush of democracies to overtly embrace cyber-enabled information operations in their military organizations and doctrine, there has been little evaluation of whether the democratic employment of these operations for offensive purposes is useful or desirable. This article sought to lay out a broader overview of the terrain of democratic offensive information operations to help create a foundation for this debate and in so doing, identify key tensions in the democratic use of these operations.

Should democracies employ offensive cyber-enabled information operations? This article concludes that the risks of conducting these operations outweigh their benefits. Globally, democracies are at a critical impasse with declining trust in democratic institutions and a seeming reversal in their expansion and consolidation. One element of this democratic decline is the increasing cynicism towards democratic institutions, debate, and news media.[82] The offensive employment of information operations risks deepening the challenges that democracies currently face. Instead, democracies should pursue two strategies: first, domestic regulation of "disinformation for hire" firms that specialize in private social media shaping and information operations. Proliferation of these firms seriously threatens the viability of democratic information ecosystems that would help counter charges of hypocrisy. Second, democracies should employ denial strategies against actors conducting offensive information operations.[83] More important than shaping partisan narratives in their favor, democracies should deter or compel adversaries by reducing their ability to conduct these operations.

NOTES

1. Larry Jay Diamond and Marc F. Plattner, *Liberation Technology: Social Media and the Struggle for Democracy* (Baltimore: Johns Hopkins University Press, 2012); Ryan Kiggins, "Open for Expansion: US Policy and the Purpose for the Internet in the Post-Cold War Era," *International Studies Perspectives* 16, no. 1 (2015): 86–105; Daniel McCarthy, *Power, Information Technology, and International Relations Theory: The Power and Politics of US Foreign Policy and Internet* (London: Palgrave Macmillan, 2015).
2. Eric Lipton, David Sanger, and Shane Scott, "The Perfect Weapon: How Russian Cyberpower Invaded the U.S," *The New York Times,* December 13, 2016.
3. Camille Francois and Herb Lin, "The Strategic Surprise of Russian Information Operations on Social Media in 2016 in the United States: Mapping a Blind Spot," *Journal of Cyber Policy* 6, no. 1 (February 2021): 9-30. Sarah Kreps. *Social Media and International Relations* (Cambridge: Cambridge University Press, 2020).
4. For an extended discussion of what makes cyber-enabled information operations unique, see: Herbert Lin and Jaclyn Kerr, "On Cyber-Enabled Information Warfare and Information Operations," in *Oxford Handbook of Cyber Security*, ed. Paul Cornish (Oxford: Oxford University Press, 2021).
5. Kreps, *Social Media, and International Relations,* 25-26. Henry Farrell and Bruce Schneier, "Common-Knowledge Attacks on Democracy.," *Berkman Klein Center* 2018-7 (2018).
6. Poynter, "A Guide to Anti-Misinformation Actions around the World," *Poynter,* August 14, 2019, https://www.poynter.org/ifcn/anti-misinformation-actions/.
7. Michael Warner, "Invisible Battlegrounds: On Force and Revolutions, Military and Otherwise," in *Palgrave Handbook of Security, Risk, and Intelligence.*, ed. Robert Dover (London: Palgrave Macmillan, 2018), 256.
8. Laura Rosenberger, "Making Cyberspace Safe for Democracy," *Foreign Affairs,* January 25, 2021, https://www.foreignaffairs.com/articles/china/2020-04-13/making-cyberspace-safe-democracy.
9. Farrell and Schneier, "Common-Knowledge Attacks on Democracy."
10. Kiggins, *Open for Expansion.*
11. Vincent Mosco. *The Digital Sublime: Myth, Power, and Cyberspace* (Cambridge: MIT Press, 2005).
12. Michael Warner, "The Character of Cyber Conflict," *Texas National Security Review*, September 17, 2020, https://tnsr.org/roundtable/policy-roundtable-cyber-conflict-as-an-intelligence-contest/.
13. Ryan Fedasiuk, "A Different Kind of Army: The Militarization of China's Internet Trolls," *Jamestown Foundation,* April 12, 2021, https://jamestown.org/program/a-different-kind-of-army-the-militarization-of-chinas-internet-trolls/.; Adrian Chen, "The Agency," *The New York Times Magazine,* June 2, 2015, https://www.nytimes.com/2015/06/07/magazine/the-agency.html; Elsa Kania, in *Information Warfare in the Age of Cyber Conflict*, ed. Christopher Whyte, A. Trevor Thrall, and Brian M. Mazanec (Abingdon: Taylor & Francis Group, 2021), 46-53.
14. Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: Ecco, 2012); Adam P. Liff, "Cyberwar: A New 'Absolute Weapon'? the Proliferation of Cyberwarfare Capabilities and Interstate War," *Journal of Strategic Studies* 35, no. 3 (2012): 401-428; Timothy J. Junio, "How Probable Is Cyber War? Bringing IR Theory Back in to the Cyber Conflict Debate," *Journal of Strategic Studies* 36, no. 1 (2013): 125-133.; Lucas Kello, *The Virtual Weapon and International Order* (New Haven: Yale University Press, 2018); Thomas Rid, *Cyber War Will Not Take Place* (New York: Oxford University Press, 2013); Brandon Valeriano and Ryan C. Maness, *Cyber War Versus Cyber Realities: Cyber Conflict in the International System* (Oxford: Oxford University Press, 2015).; Nadiya Kostyuk, and Yuri Zhukov, "Invisible Digital Front: Can Cyber Events Shape Battlefield Events?" *Journal of Conflict Resolution,* 63, no. 2 (2019): 317–347.
15. Richard J. Harknett, and Max Smeets. "Cyber Campaigns and Strategic Outcomes." *Journal of Strategic Studies*, Journal of Strategic Studies, 2020-03, 1–34; Robert Chesney, and Max Smeets, "Introduction: Is Cyber Conflict an Intelligence Contest?" *Texas National Security Review* 3, no. 4 (2020). https://tnsr.org/roundtable/policy-roundtable-cyber-conflict-as-an-intelligence-contest/; Jon R. Lindsay, "Military Organizations, Intelligence Operations, and Information Technology," *Texas National Security Review* 3, no. 4 (2020), https://tnsr.org/roundtable/policy-roundtable-cyber-conflict-as-an-intelligence-contest/; Joshua Rovner, "What Is an Intelligence Contest?" *Texas National Security Review*, Texas National Security Review, 3, no. 4 (2020-09-17), https://tnsr.org/roundtable/policy-roundtable-cyber-conflict-as-an-intelligence-contest/; Michael Warner, "The Character of Cyber Conflict." *Texas National Security Review* 3, no. 4 (2020), https://tnsr.org/roundtable/policy-roundtable-cyber-conflict-as-an-intelligence-contest/; Michael Poznansky, "Covert Action, Espionage, and the Intelligence Contest in Cyberspace., *War on the Rocks* (2021),https://warontherocks.com/2021/03/covert-action-espionage-and-the-intelligence-contest-in-cyberspace/; Benjamin Jensen, "The Cyber Character of Political Warfare," *Brown Journal of World Affairs* XXIV, no. 1 (2017): 157-171.

NOTES

16. Martin Libicki, "The Convergence of Information Warfare," in *Information Warfare in the Age of Cyber Conflict*, ed. Christopher Whyte and A. Trevor Thrall (Abingdon: Taylor & Francis, 2021), 15-27.; Mark Pomerleau, "More Work Needed to Integrate Cyber and Information Ops, Former Official Says," C4ISRNet, March 6, 2021, https://www.c4isrnet.com/information-warfare/2021/03/05/more-work-needed-to-integrate-cyber-and-information-ops-former-official-says/; Herbert Lin, "Election Hacking, as We Understand It Today, Is Not a Cybersecurity Issue," Lawfare, October 31, 2019, https://www.lawfareblog.com/election-hacking-we-understand-it-today-not-cybersecurity-issue.
17. Francois and Lin, *The Strategic Surprise of Russian information operations*, 16.
18. Ryan Shandler et al., "Cyber Terrorism and Public Support for Retaliation – A Multi-Country Survey Experiment," *British Journal of Political Science*, 2021, 1-19; Sarah Kreps and Jacquelyn Schneider, "Escalation Firebreaks in the Cyber, Conventional, and Nuclear Domains: Moving Beyond Effects-Based Logics," *Journal of Cybersecurity* 5, no. 1 (2019).
19. Rosenberger, *Making Cyberspace Safe for Democracy*.
20. Christopher Whyte, "How Deep the Rabbit Hole Goes: Escalation, Deterrence, and the 'Deeper' Challenges of Information Warfare in the Age of the Internet," in *Information Warfare in the Age of Cyber Conflict*, ed. Christopher Whyte, A. Trevor Thrall, and Brian M. Mazanec (Abingdon: Taylor & Francis, 2021), 238-245.
21. Brian M Mazanec and Patricia Shamai, "Stigmatizing Cyber and Information Warfare: Mission Impossible?," in *Information Warfare in the Age of Cyber Conflict*, ed. Christopher Whyte, A. Thrall, and Brian Mazanec (Abingdon: Taylor & Francis, 2021), 230-238.
22. Rosenberger, *Making Cyberspace Safe for Democracy*.
23. "The Honest Ads Act." Office of U.S. Senator Mark R. Warner, May 2019, https://www.warner.senate.gov/public/index.cfm/the-honest-ads-act.
24. "Grand Jury Indicts Thirteen Russian Individuals and Three Russian Companies for Scheme to Interfere in the United States Political System," Justice News. Department of Justice, February 16, 2018, https://www.justice.gov/opa/pr/grand-jury-indicts-thirteen-russian-individuals-and-three-russian-companies-scheme-interfere.
25. Andy Greenberg, "US Hits Russia with Biggest Spying Retaliation 'since the Cold War,'" Wired, December 29, 2016, https://www.wired.com/2016/12/obama-russia-hacking-sanctions-diplomats/.
26. Karoun Demirjian, "Senate Overwhelmingly Passes New Russia and Iran Sanctions," *The Washington Post*, June 15, 2017, https://www.washingtonpost.com/powerpost/senate-overwhelmingly-passes-new-russia-and-iran-sanctions/2017/06/15/df9afc2a-51d8-11e7-91eb-9611861a988f_story.html.
27. Francois and Lin, *The Strategic Surprise of Russian Information Operations.*
28. Air Force, *AFDD 3-12 Cyberspace Operations* (Washington, DC: Air Force, 2011).
29. Joint Chiefs of Staff, *JP 3-12 Cyberspace Operations* 2018 (Washington, DC: Chairman JCS, 2018), ix.
30. Gina Harkins, "Fake News Is Wreaking Havoc on the Battlefield. Here's What the Military's Doing About It," Military.com, August 17, 2020, https://www.military.com/daily-news/2020/08/16/fake-news-wreaking-havoc-battlefield-heres-what-militarys-doing-about-it.html.
31. Herbert Lin, "Doctrinal Confusion and Cultural Dysfunction in the Pentagon over Information and Cyber Operations," *Lawfare*, March 31, 2020, https://www.lawfareblog.com/doctrinal-confusion-and-cultural-dysfunction-pentagon-over-information-and-cyber-operations.
32. Ellen Nakashima, "U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms," *The Washington Post*, February 27, 2019, https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html.
33. Harkins, "Fake News Is Wreaking Havoc on the Battlefield."
34. Brandi Vincent, "The Marines Are Copying the Air Force's Efforts to Counter Online Disinformation," Defense One, September 14, 2021, https://www.defenseone.com/threats/2021/09/military-intel-officials-highlight-efforts-counter-online-disinformation/185346/.
35. Heather Burns, "Why the Online Safety Bill Threatens Our Civil Liberties," Politics.co.uk, May 27, 2021, https://www.politics.co.uk/comment/2021/05/26/why-the-online-safety-bill-threatens-our-civil-liberties/.
36. BBC, "Fake News and How to Spot It to Be Taught in Schools - CBBC Newsround," BBC News, July 15, 2019, https://www.bbc.co.uk/newsround/48988778.

NOTES

37. Ministry of Defense, *Cyber Primer*, (London: Ministry of Defense, 2016), 59.
38. Peter Walker, "New National Security Unit Set up to Tackle Fake News in the UK," The Guardian, January 23, 2018, https://www.theguardian.com/politics/2018/jan/23/new-national-security-unit-will-tackle-spread-of-fake-news-in-uk.
39. Dan Sabbagh, "Army Fights Fake News with Propagandists and Hackers in One Unit," The Guardian, July 31, 2019, https://www.theguardian.com/technology/2019/jul/31/army-fights-fake-news-with-propagandists-and-hackers-in-one-unit.
40. "National Cyber Force Transforms Country's Cyber Capabilities to Protect the UK," gchq.gov.uk, November 19, 2020, https://www.gchq.gov.uk/news/national-cyber-force; HM Government, *National Cyber Strategy 2022*, (London: HM Government, 2022), 59.
41. Jeremy Fleming, "Director's Speech at Cyber UK 2018," gchq.gov.uk, April 12, 2018, https://www.gchq.gov.uk/speech/director-cyber-uk-speech-2018.
42. Mark Hookham, "Troops Face New Enemy - Kremlin's Fake News," *The Sunday Times,* March 18, 2017, https://www.thetimes.co.uk/article/troops-face-new-enemy-kremlins-fake-news-q0dbnfq79.
43. Helen Warrell, "UK on High Alert for Anti-Vaccine Disinformation from Hostile States," *The Financial Times,* December 11, 2020, https://www.ft.com/content/7502f1f1-e104-403d-975f-bedc6e518fe2.
44. Alexander Ricci, "French Opposition Parties Are Taking Macron's Anti-Misinformation Law to Court," Poynter, September 30, 2019, https://www.poynter.org/fact-checking/2018/french-opposition-parties-are-taking-macrons-anti-misinformation-law-to-court/.
45. Ibid.
46. Simon Chandler, "French Social Media Law Is Another Coronavirus Blow to Freedom of Speech," *Forbes,* May 14, 2020, https://www.forbes.com/sites/simonchandler/2020/05/14/french-social-media-law-is-another-coronavirus-blow-to-freedom-of-speech/.
47. Arthur Laudrain, "France's New Offensive Cyber Doctrine," *Lawfare*, October 31, 2019, https://www.lawfareblog.com/frances-new-offensive-cyber-doctrine.
48. Lukasz Olejnik, "French Doctrine of Information Operations - Engaging over Information Space," Security, Privacy & Tech Inquiries, October 22, 2021, https://blog.lukaszolejnik.com/french-doctrine-of-information-operations-engaging-over-information-space/.
49. AFP, "France To Boost Cyber Warfare Force," *Barrons*, September 8, 2021, https://www.barrons.com/news/france-to-boost-cyber-warfare-force-01631123408.
50. Facebook, "Removing Coordinated Inauthentic Behavior from France and Russia," Facebook Newsroom, December 2020, https://about.fb.com/news/2020/12/removing-coordinated-inauthentic-behavior-france-russia/.
51. Jeffrey Mankoff, "Russian Influence Operations in Germany and Their Effect," Center for Strategic and International Studies, December 17, 2020, https://www.csis.org/analysis/russian-influence-operations-germany-and-their-effect.
52. Jessica Bateman, "Germany Braces for Election Disinformation," *Foreign Policy*, September 13, 2021, https://foreignpolicy.com/2021/09/13/germany-election-disinformation-social-media/.
53. Poynter, "A guide to anti-misinformation actions around the world," Poynter, August 14, 2019, https://www.poynter.org/ifcn/anti-misinformation-actions/.
54. Council on Foreign Relations, "Germany Develops Offensive Cyber Capabilities without a Coherent Strategy of What to Do with Them," Council on Foreign Relations, December 3, 2018, https://www.cfr.org/blog/germany-develops-offensive-cyber-capabilities-without-coherent-strategy-what-do-them.
55. "The Federal Government Has Adopted the Cyber Security Strategy," Website of the German Federal Government, September 8, 2021, https://www.bundesregierung.de/breg-en/news/new-cyber-security-strategy-1958688.
56. Mark Scott and Rebecca Kern, "Social Media Goes to War," *Politico,* March 3, 2022, https://www.politico.eu/article/social-media-goes-to-war/.
57. Steven Vaughan-Nichols, "Russia may be cutting itself off from the internet," *ZDNet,* March 10, 2022, https://www.zdnet.com/article/russia-may-be-cutting-itself-off-from-the-internet/.
58. Max Colchester and Warren Strobel, "U.S., Allies Fight Information War with Russia to Deter Ukraine Invasion," *The Wall Street Journal*, https://www.wsj.com/articles/u-s-allies-fight-information-war-with-russia-to-deter-ukraine-invasion-11644402601.

NOTES

59. Taylor Lorenz, "The White House is Briefing TikTok Stars about the war in Ukraine," *The Washington Post*, March 11, 2022, https://www.washingtonpost.com/technology/2022/03/11/tik-tok-ukraine-white-house/.
60. Anjana Susaria, "Why Zelenskyy's `selfie videos' are helping Ukraine win the PR war against Russia," March 1, 2022, https://theconversation.com/why-zelenskyys-selfie-videos-are-helping-ukraine-win-the-pr-war-against-russia-178117; Lizzie O'Leary, "Ukraine is Winning the Information War With Russia," *Slate*, March 4, 2022, https://slate.com/technology/2022/03/ukraine-is-winning-the-information-war-with-russia.html.
61. Ross Caputi, "The Troubling Legacies of U.S. Information Operations during the Iraq Occupation," Scholars Strategy Network, January 11, 2018, https://scholars.org/contribution/troubling-legacies-us-information-operations-during-iraq-occupation.
62. Associated Press, "US Secretly Created 'Cuban Twitter' to Stir Unrest and Undermine Government," *The Guardian*, April 3, 2014, https://www.theguardian.com/world/2014/apr/03/us-cuban-twitter-zunzuneo-stir-unrest.
63. Associated Press, "US Secretly Created 'Cuban Twitter' to Stir Unrest and Undermine Government."
64. Bernard E. Harcourt, E*xposed: Desire and Disobedience in the Digital Age* (Cambridge: Harvard University Press, 2015), 8-10.
65. Nick Fielding and Ian Cobain, "Revealed: US Spy Operation That Manipulates Social Media," *The Guardian*, March 17, 2011, https://www.theguardian.com/technology/2011/mar/17/us-spy-operation-social-networks?CMP=share_btn_tw.
66. Walter Pincus, "New and Old Information Operations in Afghanistan: What Works?" *The Washington Post*, March 28, 2011, https://www.washingtonpost.com/world/new-and-old-information-operations-in-afghanistan-what-works/2011/03/25/AFxNAeqB_story.html.
67. Rosenberger. "Making Cyberspace Safe for Democracy."
68. Chris Demchak, "Uncivil and Post-Western Cyber Westphalia: Changing Interstate Power Relations of the Cybered Age," *The Cyber Defense Review* 5, no. 1 (2016): 49-51.
69. Keir Giles, *Handbook of Russian Information Warfare* (Rome, Italy: NATO Defence College Research Division, 2016), 36-44; Warner, "The Character of Cyber Conflict."
70. McCarthy 2015, 119–121.
71. Ryan Fedasiuk, "A Different Kind of Army: The Militarization of China's Internet Trolls," Jamestown Foundation, April 12, 2021, https://jamestown.org/program/a-different-kind-of-army-the-militarization-of-chinas-internet-trolls/.; Fedasiuk 2021. Lincoln Pigman, "Russia's Vision of Cyberspace: A Danger to Regime Security, Public Safety, and Societal Norms and Cohesion," *Journal of Cyber Policy* 4, no. 1 (2018): 23-24.
72. Rachel Pannett, "Russia Threatens to Block YouTube after German Channels Are Deleted over Coronavirus Misinformation," *The Washington Post*, September 29, 2021, https://www.washingtonpost.com/world/2021/09/29/russia-ban-youtube-german-coronavirus/.
73. Quoted in AFP, "France Struggling in Sahel 'Information War'," France 24, February 11, 2021, https://www.france24.com/en/live-news/20210211-france-struggling-in-sahel-information-war.
74. Mark Scott and Elisa Braun, "France Feuds with Facebook over Disinformation Claims," *Politico*, December 17, 2020, https://www.politico.eu/article/france-facebook-disinformation/.
75. Ibid.
76. Sidney Fussell, "French Spyware Executives Are Indicted for Aiding Torture," *Wired*, June 23, 2021, https://www.wired.com/story/french-spyware-executives-indicted-aiding-torture/; Tim Shorrock, "How Private Contractors Have Created a Shadow NSA," *The Nation*, December 30, 2019, https://www.thenation.com/article/archive/how-private-contractors-have-created-shadow-nsa/.
77. Samantha Bradshaw, Hannah Bailey, and Philip Howard, *Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation* (Oxford: Project on Computational Propaganda, 2021), i.
78. Jane Lytvynenko, "In 2020, Disinformation Broke the US," BuzzFeed News, April 14, 2021, https://www.buzzfeednews.com/article/janelytvynenko/disinformation-broke-us; Isaac Stanley-Becker, "Pro-Trump Youth Group Enlists Teens in Secretive Campaign Likened to a 'Troll Farm,' Prompting Rebuke by Facebook and Twitter," *The Washington Post*, September 16, 2020, https://www.washingtonpost.com/politics/turning-point-teens-disinformation-trump/2020/09/15/c8409lae-f20a-11ea-b796-2dd09962649c_story.html; Adam Satariano and Amie Tsang, "Who's Spreading Disinformation in U.K. Election? You Might Be Surprised," The New York Times, December 10, 2019, https://www.nytimes.com/2019/12/10/world/europe/elections-disinformation-social-media.html.

NOTES

79. Michael Schudson, "The Fall, Rise, and Fall of Media Trust," *Columbia Journalism Review*, 2019, https://www.cjr.org/special_report/the-fall-rise-and-fall-of-media-trust.php; Benjamin Toff et al., "Overcoming Indifference: What Attitudes towards News Tell Us about Building Trust," Reuters Institute for the Study of Journalism, September 9, 2021, https://reutersinstitute.politics.ox.ac.uk/overcoming-indifference-what-attitudes-towards-news-tell-us-about-building-trust.
80. Emily Vogels, Andrew Perrin, and Monica Anderson, "Most Americans Think Social Media Sites Censor Political Viewpoints," Pew Research Center: Internet, Science & Tech (Pew Research Center, September 18, 2020), https://www.pewresearch.org/internet/2020/08/19/most-americans-think-social-media-sites-censor-political-viewpoints/.
81. Hanna Kozlowska, "Russian Trolls and Bots Are Successful Because We Know They Exist," Quartz, January 30, 2020, https://qz.com/1792155/russian-trolls-and-bots-are-successful-because-we-know-they-exist/.
82. Yascha Mounk, "Democracy on the Defense," Foreign Affairs, March 1, 2021, https://www.foreignaffairs.com/articles/united-states/2021-02-16/democracy-defense; 'The Global Democratic Recession. And How to Reverse It' with Larry Diamond," Indiana University, December 6, 2020, https://iu.mediaspace.kaltura.com/media/%E2%80%9CThe+Global+-Democratic+Recession.+And+How+to+Reverse+It%E2%80%9D+with+Larry+Diamond/1_gfca8m0v.
83. Erica D. Borghard and Shawn W. Lonergan, "Deterrence by Denial in Cyberspace," *Journal of Strategic Studies*, March 2021, 1-36.