Burnt by the Digital Sun

How the Information Environment Is Testing the Mettle of Liberal Democracies

AUTHOR
Zhanna Malekos Smith
Burnt by the Digital Sun

HOW THE INFORMATION ENVIRONMENT IS TESTING THE METTLE OF LIBERAL DEMOCRACIES

AUTHORS
Zhanna Malekos Smith

A Report of the CSIS Technology Policy Program

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES
About CSIS

The Center for Strategic and International Studies (CSIS) is a bipartisan, nonprofit policy research organization dedicated to advancing practical ideas to address the world’s greatest challenges.

Thomas J. Pritzker was named chairman of the CSIS Board of Trustees in 2015, succeeding former U.S. Senator Sam Nunn (D-GA). Founded in 1962, CSIS is led by John J. Hamre, who has served as president and chief executive officer since 2000.

CSIS’s purpose is to define the future of national security. We are guided by a distinct set of values—nonpartisanship, independent thought, innovative thinking, cross-disciplinary scholarship, integrity and professionalism, and talent development. CSIS’s values work in concert toward the goal of making real-world impact.

CSIS scholars bring their policy expertise, judgment, and robust networks to their research, analysis, and recommendations. We organize conferences, publish, lecture, and make media appearances that aim to increase the knowledge, awareness, and salience of policy issues with relevant stakeholders and the interested public.

CSIS has impact when our research helps to inform the decisionmaking of key policymakers and the thinking of key influencers. We work toward a vision of a safer and more prosperous world.

CSIS is ranked the number one think tank in the United States by the University of Pennsylvania’s “Global Go To Think Tank Index.”

CSIS does not take specific policy positions; accordingly, all views expressed herein should be understood to be solely those of the author(s).

© 2020 by the Center for Strategic and International Studies. All rights reserved.
Acknowledgments

With special thanks to Ms. Eugenia Lostri, the program coordinator and research assistant with the CSIS Technology Policy Program, for her excellent research assistance. Thank you also to Ms. Maggie Tennis and Ms. Anna Lehman-Ludwig, researchers with the CSIS Technology Policy Program, and Mr. Thomas E. Smith, for their generosity of time and support.

This material is based upon work supported by the U.S. Cyberspace Solarium Commission under contract purchase order #OCE-53. Any opinions, findings, conclusions, or recommendations expressed in this material are those of the author and do not reflect the official policy or position of the U.S. Cyberspace Solarium Commission, Department of Defense, or the U.S. government.
Abstract

How are liberal democracies balancing the right to freedom of expression with addressing false information and hostile actions in the information environment? This report begins by surveying how the United States, the United Kingdom, New Zealand, Australia, Canada, France, and Germany are grappling with this intricate Gordian knot. Next, it offers an introductory examination of “information warfare” and how it is shaping the great power competition between Russia, China, and the United States. Granted, information warfare is a hotly contested term with many competing definitions within the field of military science, as well as across Western and Eastern cultures; however, this report refers to it as the military art of using information to deliberately mislead an adversary and influence their decisionmaking for a strategic purpose. Lastly, to help inform effective policy against such persistent information threats, the report outlines a creative multi-pronged framework.
Contents

Acknowledgments IV
Abstract V
Introduction 1
Part I: Examining the Legal Landscape in the United States 3
The Jurisprudence of Free Speech in the United States 3
The Communication Decency Act of 1996 and the Counterspeech Doctrine 5
Regulating Online Paid Political Advertisements 6
Social Media Platforms Are the Modern Public Square 7
Part II: How Are Other Liberal Democracies Addressing False Information? 9
The European Commission and European Union 9
Australia 10
Canada 11
New Zealand 12
France 13
Germany 14
United Kingdom 14
Part III: A Primer for Policymakers on Information Warfare 17
What Is Information Warfare? 17
Approaches to Hostile Information Campaigns: China, Russia, and the United States 18
China and Informationized Wars 19
Russia and Information Warfare 20
Is There a Common Thread to All These Techniques? 21
Disinformation (Дезинформация) 22
What Are Active Measures? 23
The United States and Information Operations 24
The 2016 U.S. Presidential Election 24
Looking to the Future 26
Part IV: Building National Perseverance in the Information Environment 27
Focusing on Smart Power in Great Power Competition 27
Information Sharing 28
Resiliency 29
Education Initiatives to Promote Civic Literacy and Information Security Skills 33
Conclusion 35
About the Author 36
Introduction

Using false information to disorient and mislead an adversary is not a new tactic in contemporary warfighting. As the Chinese military strategist Sun Tzu observed centuries ago, "all warfare is based on deception." Moreover, false signaling isn’t even unique to the human species, for animals and insects predate us in using mimicry to trick predators and ensnare prey. What sets human beings apart, however, is our systematic production and instantaneous distribution of false information to influence others. The advent of digital media platforms has given new meaning to the adage that a lie can travel halfway around the world while the truth is still putting on its shoes. As society grows increasingly connected to and dependent upon information and communication technologies (ICTs) to facilitate everyday activities, our exposure to the malicious use of ICTs increases as well. In recognition of these risks, the 2019 Joint Statement on Advancing Responsible State Behavior in Cyberspace warned that "State and non-state actors are using cyberspace increasingly as a platform for irresponsible behavior from which to target critical infrastructure and our citizens, undermine democracies and international institutions and organizations, and undercut fair competition in our global economy."

How are liberal democracies balancing the right to freedom of expression with addressing false information and hostile information campaigns? This report begins in Part I by surveying how the United States is endeavoring to address these information environment challenges. The information environment, as defined under the 2018 Joint Concept for Operations in the Information Environment, is an aggregate of “numerous social, cultural, cognitive, technical, and physical attributes that act upon and impact knowledge, understanding, beliefs, world views, and, ultimately, actions of an individual, group, system, community, or organization.”

Next, Part II examines how the United Kingdom, New Zealand, Australia, Canada, France, and Germany are similarly engaging with this Gordian knot. The focus shifts in Part III to hostile information campaigns by providing a basic overview of “information warfare” from the perspective of the Armed Forces of the Russian Federation, Ministry of National

4. Ibid.
Defense of the People’s Republic of China, and the U.S. Department of Defense. Granted, information warfare is a hotly contested term with many competing definitions within the field of military science, as well as across Western and Eastern cultures; however, it is defined here as the military art of using information to deliberately mislead an adversary and influence their decision making for a strategic purpose. To help inform effective policy against such persistent information threats, Part IV concludes by outlining a creative multi-pronged framework. While there is no single solution for mitigating the adverse effects of hostile information campaigns, the report draws inspiration from the Italian Renaissance polymath Leonardo da Vinci. From his Art and Life notebook observations on truth, da Vinci posited “There is nothing hidden under the sun. Fire must represent truth because it destroys all sophistry and lies, and the mask is for sophistry and lies, which conceal truth.”5 Thus, as a thematic scaffolding for our inquiry, this report extends da Vinci’s juxtaposition of fire as a revealer of truth, to inform policy development—the da Vinci F.I.R.E. Model—which features (F)ocusing on Smart Power in Great Power Competition, (I)nformation Sharing, (R)esiliency, and (E)ducation.

Part I: Examining the Legal Landscape in the United States

The Jurisprudence of Free Speech in the United States

While the history of the right of free speech in the United States could easily lend itself to an entire treatise, this report will briefly sketch its contours. The First Amendment of the U.S. Constitution protects the freedom of speech and recites that “Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.”

The right to free speech, however, is not an unfettered absolute right. Turning to its early origins, Michael Chertoff, former Secretary of the Department of Homeland Security, notes that the First Amendment “was adopted in an age when there was no such thing as an “objective” or ‘professionalized’ media. Early America was an age of rough and tumble, politically activist, and even scurrilous press . . . In 1798, the Federalists reacted by passing the Sedition Act, which criminalized false statements that criticized the federal government.”

The 1798 Sedition Act was reviled by the Anti-Federalists and eventually retired under the Jefferson administration. Over a century later, the U.S. Supreme Court said in New York Times Co. v. Sullivan (1964) that “Although the Sedition Act was never tested in this Court, the attack upon its validity has carried the day in the court of history.” This is a significant dictum because it suggests that the early founders were at least aware that the right of free speech would implicate both factual and fraudulent forms of speech.

Some legal theorists support U.S. Justice Louis Brandeis’s illustrious concurring opinion in Whitney v. California, 274 U.S. 357 (1927), wherein he opined that the

6. U.S. Const. amend. I.
8. Ibid.
remedy for false speech was more speech.\textsuperscript{10} Justice Brandeis’s vision, also known as the counterspeech doctrine, was: “If there be time to expose through discussion the falsehood and fallacies, to avert the evil by the processes of education, the remedy to be applied is more speech, not enforced silence. Only an emergency can justify repression. Such must be the rule if authority is to be reconciled with freedom.”\textsuperscript{11} Over time, however, with the public’s use of social media news sites and bad actors’ employment of artificial intelligence and machine learning tools to generate fraudulent content, some scholars have questioned the saliency of the counterspeech doctrine. Professor Philip Napoli at Duke University reasons that this doctrine is challenged by contemporary digital media ecosystems that engender echo chambers.\textsuperscript{12} Napoli is also critical of the configurations of certain digital media outlets’ ad-placement algorithms, noting that it permits “fake news” sites to be “on more or less equal footing with other online content providers. Even recent, initial efforts to ban known fake news outlets from major ad networks (a response to the post-2016 fake news revelations) appear to have—at least initially—proven not entirely effective.”\textsuperscript{13}

Speaking to the issue of artificial intelligence-generated fake personas, this is becoming an increasing challenge for users of social media platforms like LinkedIn, a professional social-networking site.\textsuperscript{14} Why? Because the ability to generate fake accounts with false profile images (i.e., a deepfake-generated profile photo) is rendered easier for malicious actors using AI tools.\textsuperscript{15} What are deepfakes? According to the U.S. Government Accountability Office (GAO), a deep fake is “a video, photo, or audio recording that seems real but has been manipulated with AI. The underlying technology can replace faces, manipulate facial expressions, synthesize faces, and synthesize speech.”\textsuperscript{16} The GAO expressed concern for the potentiality of deepfakes to be used as means for exploitation, disinformation, and non-consensual pornography.\textsuperscript{17} Slate describes deepfakes as “realistic-looking content developed using machine learning algorithms” and opines that they will “herald a new era of information warfare.”\textsuperscript{18} Deepfakes are also a major concern of the U.S. Intelligence Community and were identified in the 2019 Worldwide Threat Assessment report.\textsuperscript{19} The report warns that adversaries and strategic competitors “probably will attempt to use deepfakes to create convincing—but false—image, audio, and video files to augment influence campaigns directed against the United States and our allies and partners.”\textsuperscript{20} With those concerns, what role do publishers of information play here?

\begin{itemize}
\item \textsuperscript{10} Whitney v. California, 274 U.S. 357, 377 (1927).
\item \textsuperscript{11} Ibid.
\item \textsuperscript{13} Ibid., 72.
\item \textsuperscript{15} Ibid.
\item \textsuperscript{17} Ibid.
\item \textsuperscript{18} Ibid.
\item \textsuperscript{20} Ibid.
\end{itemize}
The Communication Decency Act of 1996 and the Counterspeech Doctrine

Although section 230 of the Communication Decency Act of 1996\textsuperscript{21} shields social media companies from being held liable for publishing content posted by its users, President Donald Trump’s 2020 “Executive Order on Preventing Online Censorship” sought to reduce those controversial protections.\textsuperscript{22} The executive order (EO) highlights that “Twitter, Facebook, Instagram, and YouTube wield immense, if not unprecedented, power to shape the interpretation of public events; to censor, delete, or disappear information; and to control what people see or do not see.”\textsuperscript{23} The EO recounts the societal harms from online platforms that engage in “selective censorship” such as inhibiting national discourse and cites thousands of Americans as having reported “online platforms ‘flagging’ content as inappropriate, even though it does not violate any stated terms of service; making unannounced and unexplained changes to company policies that have the effect of disfavoring certain viewpoints; and deleting content and entire accounts with no warning, no rationale, and no recourse.”\textsuperscript{24} From that standpoint, does this type of activity render the counterspeech doctrine a less sustainable solution?

Perhaps time will tell; however, Chertoff reasons that society cannot afford to take a passive approach and hope that this problem will resolve itself.\textsuperscript{25} He recommends enacting new policies to “deny the ability of automated networks of bots or zombie computers to influence search engines,” in addition to identifying foreign actors that purchase advertisements and barring content that is a direct incitement to violence or illegal activity; which are not protected forms of free speech.\textsuperscript{26} Focusing on the incitement to violence concern, Twitter’s hateful conduct policy prohibits users from using the platform to incite violence and its violent threats policy prohibits users from “glorifying violence.”\textsuperscript{27} The hateful conduct policy reads: “You may not promote violence against or directly attack or threaten other people on the basis of race, ethnicity, national origin, caste, sexual orientation, gender, gender identity, religious affiliation, age, disability, or serious disease.”\textsuperscript{28} In the wake of the protest demonstrations and unfortunate looting in Minneapolis following George Floyd’s tragic death, President Trump posted on Twitter “when the looting starts, the shooting starts.” This post garnered the attention of Twitter’s legal counsel and CEO, Jack Dorsey, who resolved to “hide Mr. Trump’s tweet behind a warning label that said the message violated its policy against glorifying violence.”\textsuperscript{29}

\textit{The New York Times}

\footnotesize{\textsuperscript{21} 47 U.S.C. § 230. “No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.”
\textsuperscript{23} Ibid.
\textsuperscript{24} Ibid.
\textsuperscript{25} Chertoff, “Fake News.”
\textsuperscript{26} Ibid.
\textsuperscript{27} “Violent Threats Policy,” Twitter Help Center, https://help.twitter.com/en/rules-and-policies/vio-lent-threats-glorification. “Under this policy, you can’t state an intention to inflict violence on a specific person or group of people. We define intent to include statements like ‘I will’, ‘I’m going to’, or ‘I plan to’, as well as conditional statements like ‘If you do X, I will.’”
\textsuperscript{29} Kate Conger, “A Look Inside Twitter’s Move to Flag Trump,” \textit{New York Times}, May 31, 2020.}
reported that this action marked the first instance in which a public official's tweet has been marked with the glorifying violence warning.\textsuperscript{30} Several days later, a tweet by Representative Matt Gaetz (R-FL) about the protests and Antifa prompted Twitter to hide the message behind the same warning label.\textsuperscript{31} Overall, President Trump’s EO is a signal to lawmakers to clarify the scope of immunity granted to platforms under section 230 of the Communication Decency Act and inhibit “stifling free and open debate” online.

\textit{Regulating Online Paid Political Advertisements}

The following case about Maryland’s legislature and its efforts to regulate paid online political advertisements is particularly instructive for policymakers. In April 2018, the Maryland General Assembly passed the Online Electioneering Transparency and Accountability Act to address foreign interference in U.S. elections. This act sought to compel social media companies and news sites to publish the identities of ad buyers and the amount paid within 48 hours of purchase and to publish this information in a “clearly identifiable location” for at least one year from the date of purchase.\textsuperscript{32} The purpose of the Online Electioneering Transparency and Accountability Act was to allow the public access to information about any groups or individuals “seeking to influence their vote through ads run on online platforms.”\textsuperscript{33} Following its passage, news outlets such as the Washington Post, Baltimore Sun, and several other newspaper organizations filed suit against Maryland “to avoid complying with the state’s political ad transparency law.”\textsuperscript{34} The Maryland District Court found that the statute was too broadly conceived and written such that it suppressed more forms of free speech by news sites under the First Amendment than it sought to curtail.\textsuperscript{35} Further, the court noted that the act curiously required advertisement buyers to self-identify to publishers, rather than placing the burden on the publisher to limit foreign governments from interfering in political elections by purchasing political ads.\textsuperscript{36} In 2019, \textit{Washington Post v. McManus} went up for appeal before the Fourth Circuit.\textsuperscript{37} The Court of Appeals affirmed in December the lower court’s decision that Maryland’s law was too broadly constructed to pass constitutional scrutiny under the First Amendment and granted the plaintiffs’ motion for an injunction.\textsuperscript{38} For lawmakers, \textit{McManus} is illustrative in highlighting the difficulties in crafting legislation to mitigate the effects of adversarial information activities and manipulation while balancing the protections afforded to certain types of speech. With that, we turn to examining how social media platforms function as a modern public square.

\textsuperscript{30} Ibid.
\textsuperscript{33} Ibid.
\textsuperscript{35} McManus, at *66.
\textsuperscript{36} Ibid.
\textsuperscript{37} “Cases and Actions.” Campaign Legal Center.
\textsuperscript{38} The Washington Post v. McManus, No. 19-1132, 4 (4th Cir. 2019) “While Maryland’s law tries to serve important aims, the state has gone about this task in too circuitous and burdensome a manner to satisfy constitutional scrutiny.”
Social Media Platforms Are the Modern Public Square

The U.S. Supreme Court’s first examination of social media platforms and the right to free speech was in 2017. In Packingham v. North Carolina, the Court determined that a North Carolina statute that forbade sex offenders from accessing social media websites was unlawful.39

Additionally, Justice Anthony M. Kennedy touted the Internet as “the modern public square”40 and the Court reasoned that social media websites were akin to public forums.41 The Court reasoned that social media websites “allow a person with an Internet connection to ‘become a town crier with a voice that resonates farther than it could from any soapbox.’ In sum, to foreclose access to social media altogether is to prevent the user from engaging in the legitimate exercise of First Amendment rights.”42 The central challenge here, as Professor Eric Posner of Chicago University Law School points out, is that the “First Amendment protects propagandists whom U.S. authorities could reach, and national borders protect propagandists whom the First Amendment does not protect.”43 By equating social media sites as the modern public square, the Supreme Court held that social media sites are now “perhaps the most powerful mechanisms available to a private citizen to make his or her voice heard.”44

There are also concerns that any legislative effort to censor social media content could impinge on U.S. citizens’ right of free speech and have a chilling effect on the free exchange of ideas, and even run the risk of violating privacy laws. For instance, pursuant to section 552a(e)(7) of the Privacy Act of 1974, the federal government is prohibited from keeping records on U.S. person’s First Amendment activities.45 Under the Privacy Act of 1974 (hereafter “Privacy Act”), records are defined as a “group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.”46 This First Amendment exception, however, does not apply to “authorized law enforcement activity” and certain types of activities carried out by the Central Intelligence Agency.47 In addition, a right of action for violating the Privacy Act (e.g., a government official’s misuse of information protected under the Privacy Act) does not apply to data collection efforts aimed at people residing outside of the United States.48 The Privacy Act also does not apply to records kept by the private sector, as well as state and local governments.49 Under these exceptions, classifying social media websites as public forums presents interesting challenges for curtailing information operations because non-state actors generally own and operate social media platforms. Social media websites provide

---

41. Ibid.
42. Ibid. (citing Reno v. American Civil Liberties Union, 521 U.S. 844, 870 (1997)).
46. Ibid.
47. Ibid., § 552a(e)7.
48. Ibid., § 552a(g).
49. Ibid.
services to users under accepted terms of service which denote what types of expression and content are impermissible.\footnote{50}

For example, in 2019, Facebook Inc. announced that it would implement a new, independent content board to arbitrate which posts should be removed or not.\footnote{51} According to Facebook, the review board’s decisions on posts will be open to an appeals process.\footnote{52} In May 2020, Facebook announced the members of the review board, who will be granted the power to “make final and binding decisions on whether specific content should be allowed or removed from Facebook and Instagram.” While this is a first step in content moderation, there still remains strong skepticism about the value of an oversight board. As *WIRED* points out, the board “will hear only individual appeals about specific content that the company has removed from the service—and only a fraction of those appeals. The board can’t say anything about the toxic content that Facebook allows and promotes on the site.”\footnote{53} Furthermore, the board does not have the authority to change Facebook’s advertising and surveillance practices to counter disinformation campaigns.\footnote{54}

While foreign disinformation campaigns will be addressed in Part III, it is important to briefly note that the Department of Defense (DoD) does not engage in domestic information operations and is prohibited from engaging in domestic “publicity or propaganda” operations under title 10 of the United States Code section 2241.\footnote{55} Those terms, however, are not defined under title 10.\footnote{56} Further, the Congressional Research Service (CRS) noted that it is “unclear how IW/IO relate to this so-called military propaganda ban.”\footnote{57} To that end, DoD Directive 3600.01 on information operations expressly prohibits the DoD from engaging in domestic information operation activities and reads: “DoD IO activities will not be directed at or intended to manipulate audiences, public actions, or opinions in the United States and will be conducted in accordance with all applicable U.S. statutes, codes, and laws.”\footnote{58} Having outlined key components of the United States’ domestic legal framework, the following section examines how other states are exploring legislative solutions.

\footnote{52} Ibid.
\footnote{54} Ibid.
\footnote{55} 10 U.S.C. § 2241.
\footnote{56} Ibid.
Part II: How Are Other Liberal Democracies Addressing False Information?

This section provides comparative snapshots of how international institutions and states like the United Kingdom, New Zealand, Australia, Canada, France, and Germany are grappling with balancing freedom of opinion and expression and countering fraudulent information. While each state has taken a distinct path in exploring potential solutions, as a shared baseline, the 2017 Joint Declaration on Freedom of Expression and “Fake News”, Disinformation, and Propaganda affirms that all states are obligated to sustain an “enabling environment for freedom of expression” and identifies broad strands of public policy to this end.\(^{59}\) Further, freedom of opinion and expression is protected under Article 19 of the Universal Declaration of Human Rights, which reads: “Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.”\(^{60}\)

The European Commission and European Union

Focusing first on the European Commission, the commission established a high-level group of experts in 2018 to provide insight on policy recommendations to counter disinformation campaigns.\(^{61}\) The report defined disinformation as “all forms of false, inaccurate, or misleading information designed to be presented, and promoted to intentionally cause public harm or for profit.”\(^{62}\) It did not include, however, “issues arising from the creation and dissemination online of illegal content (notably defamation, hate speech, incitement to violence), which are subject to regulatory remedies under EU or national laws. Nor . . . satire and parody.”\(^{63}\) In their final report, the experts recommended


\(^{60}\) Universal Declaration of Human Rights, art. 19.


\(^{62}\) Ibid.

\(^{63}\) Ibid.
that the Commission support transparency of online news, media, and information literacy, journalistic growth, and protect the plurality of views in the “European news media ecosystem.” They cautioned, however, that any regulation must comply with Article 11 of the Charter of Fundamental Rights of the European Union. On that point, the experts emphasized that “any limitation on freedom of expression must be prescribed by law, proportional, and necessary either to meet general interest objectives recognized by the Union or to protect the rights and freedoms of others.”

The European Union also outlined an Action Plan against Disinformation, which is based on four pillars:

(i) improving the capabilities of Union institutions to detect, analyse and expose disinformation;

(ii) strengthening coordinated and joint responses to disinformation;

(iii) mobilising private sector to tackle disinformation;

(iv) raising awareness and improving societal resilience.

Presently, in the midst of the 2020 Covid-19 pandemic, the UN has called for action against the “infodemic” of misinformation. The surge in false information regarding the virus has further highlighted the need for content moderation as nations struggle to keep the public well-informed of public safety and health information during this worldwide crisis.

**Australia**

The 2019 Christchurch shooting in New Zealand galvanized Australian lawmakers to enact a law to punish social media platforms if they do not “remove violent material swiftly.” The Criminal Code was amended by the Sharing of Abhorrent Material Act passed on April 2019, according to which any form of media showing “terrorism, murder, attempted murder, torture, rape and kidnapping, whether set within or outside Australia, is considered ‘abhorrent violent conduct’ and must be removed from social media platforms” or else criminal penalties will be imposed.

The law does not specify how long social media platforms have to satisfy the temporal requirement when removing material. This ambiguity prompted the United Nations...
Human Rights Council to express concern over the possibility that the bill could have a detrimental chilling effect on freedom of expression. A letter penned by the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression and the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism expressed their concerns about the bill’s interference with Australia’s obligations under international human rights law. It called for the Australian government to “withdraw the Law and to provide additional time for legislative and public consideration of the issues contained in the Law, and evaluate the Law to ensure its consistency with international human rights standards.”

**Canada**

Since the 2017 mosque shooting in Quebec City, Canadian lawmakers have been discussing how to hold social media companies accountable for “fake news.” In February 2018, Canadian Prime Minister Trudeau issued a warning to Facebook “that it needed to fix its ‘fake news’ issues or face stricter federal regulations.” Disseminating false news content, known to be false and that might “cause injury or mischief to a public interest” is prohibited under section 181 of Canada’s Criminal Code, however, this section has been called the “zombie provision” because it was declared unconstitutional by the Supreme Court of Canada but never formally repealed.

The 2018 Bill C-76 contains a provision on “misleading publications” during election periods, making an explicit exception for parody or satire. This bill aimed at increasing the transparency of social media platforms’ advertising policies and tackling disinformation during the electoral process. In April 2019, a Canadian official acknowledged that self-regulation of social media platforms was not satisfactory and that the government was “actively considering” regulating tech giants. Although no specific domestic legislation to counter the spread of false information or hate speech has been proposed in Canada yet, the Trudeau administration launched its Digital Charter last year. One of its ten principles pushed for digital platforms to be free from hate, violent extremism, or criminal content. During the launch, the Canadian prime minister considered that social media platforms “have to step up

---

74. Ibid.
76. Ibid.
77. Ibid.
82. Ibid.
in a major way to counter disinformation. And if they don’t, we will hold them to account and there will be meaningful financial consequences.”

New Zealand

Prompted by the March 2019 mosque shooting in Christchurch City, New Zealand began a reevaluation of both gun laws and the regulation of content moderation by social media platforms. The terrorist attack by a white nationalist against two mosques was live-streamed on Facebook for 17 minutes and viewed around 4,000 times before being removed. Although the initial focus and priority by the Jacinda Arden administration was on the reevaluation of gun laws, the prime minister criticized the role of social media platforms regarding content moderation and stated that “a global approach that involves other governments, tech companies and civil society leaders” was needed to prevent extremist content online. This sentiment took further form in May 2019, when jointly with French President Emmanuel Macron, Prime Minister Arden founded the Christchurch Call. The mission of the Call, which now has the support of 59 countries and online service providers, is “to eliminate terrorist and violent extremist content online.” This nonbinding agreement outlines different stakeholder commitments to increase their efforts as they relate to countering online extremism. At the time of this writing, New Zealand’s government has not introduced a domestic proposal for curtailing false information or violent content posted on social media platforms. The 2019 Cyber Security Strategy recognizes the disruptive role of new technologies and the threat of disinformation. However, the strategy does not provide any further context on how New Zealand views and characterizes information operations. In January 2020, when announcing that the elections would be held on September 19, Prime Minister Arden announced that in order to increase election transparency and avoid “negative fake news style” campaigns, she was committed to fight the spread of misinformation and therefore would sign her party up to the Facebook Ad Library Report. This tool allows voters to see how parties spend money on Facebook advertising.
France

Prior to the relevance that “fake news” and its effects garnered in the United States in the wake of the 2016 presidential election, France already had legislation criminalizing it. The 1881 freedom of the press law made it illegal to “disturb public peace through the publication, dissemination, or reproduction of fake news in bad faith.” In 2018, President Macron announced his intention to push for legislation to fight the spread of disinformation on social media during election periods. Considering “fake news” to be a threat to liberal democracies, the French President presented a law allowing authorities vast removal and blocking powers over social media content during electoral campaigns—in the three months prior to any vote. So as to respond to some pushback on the extent of the authorities granted, the bill was subject to amendments to reflect its fight against the “manipulation of information” rather than fake news. The bill was eventually approved on November 20, 2018, and validated one month later by the Constitutional Council. An interesting consequence of this legislation was Twitter’s decision to not run the government’s campaign encouraging the vote in May 2019 European Parliament elections.

President Macron’s interest in curtailing the spread of false information expanded from elections to hate speech. The French President began advocating for domestic legislation to combat the spread of hate speech online in 2019 and later cofounded the Christchurch Call with New Zealand’s Jacinda Arden, as described previously. On May 13, 2020, the lower house of parliament passed a bill setting time limits for platform operators to remove racist or sexist posts, child pornography, and terrorist content. Failure to comply could lead to fines up to 1.25 million euros. There are concerns about the infringement on freedom of expression by social media platforms, as there are no fines for removing content later deemed acceptable. This paired with hefty fines for failure to remove content could be a problematic incentive for social media platforms to over-remove.

**Germany**

In October 2017, Germany’s NetzDG law—“the most ambitious effort by a Western democracy to control what appears on social media”\(^{106}\)—came into force. It sought to enforce online Germany’s position on hate speech by giving sites a 24-hour deadline to remove banned content or face fines of up to 50 million euros.\(^{107}\) Strict legislation did lead to a change in social media platforms’ attitude towards their responsibility in content moderation. It was reported that Facebook increased its number of German-language moderators to 1,200, making it a sixth of its global moderation team.\(^{108}\) A few months after taking in January 2018, however, the NetzDG was set to be revised due to its strict provisions leading to too much content being removed or blocked.\(^{109}\) After criticism of its chilling effect on free speech,\(^{110}\) “Lawmakers from Chancellor Angela Merkel’s conservative Christian Democrats and the left-leaning Social Democrats . . . are formulating changes to NetzDG.”\(^{111}\) Some of the modifications to the law would include the ability to petition to have content incorrectly removed be restored and also establishing an independent review body for petitions.\(^{112}\) In February 2020, the German cabinet approved legislation that would require social media platforms to not only remove content, but also report criminal posts to the Office of the Federal Criminal Police.\(^{113}\) Content featuring racial incitement, terrorism, or child pornography must be reported along with “the last IP address and port number most recently assigned to the user profile.”\(^{114}\) Once again, critics have voiced their concerns for the potential of misuse in removing content by fee-weary companies, and the endangerment of freedom of expression.\(^{115}\) Additionally, there are concerns that authoritarian governments will model their domestic legislation after it to censor political dissent speech.\(^{116}\)

**United Kingdom**

In April 2019, the UK government published its Online Harms White Paper, a joint proposal from the Department for Digital, Culture, Media, and Sport and the Home Office.\(^{117}\) Then-prime minister Theresa May Tweeted that “Online companies must start taking responsibility for their platforms, and help restore public trust in this

---

109. Ibid.
110. Ibid.
111. Ibid.
114. Ibid.
116. Ibid.
117. Ibid.
Accordingly, the proposed laws recommend imposing a new statutory duty of care on social media platforms, thereby legally requiring them to protect their users. Holding individual executives personally liable for harmful content for noncompliance with the new regulations is also explored in the document.

The White Paper articulates how cyberspace is an alluring medium to wage information operations against nations:

> There is also a real danger that hostile actors use online disinformation to undermine our democratic values and principles. Social media platforms use algorithms which can lead to ‘echo chambers’ or ‘filter bubbles’, where a user is presented with only one type of content instead of seeing a range of voices and opinions. This can promote disinformation by ensuring that users do not see rebuttals or other sources that may disagree and can also mean that users perceive a story to be far more widely believed than it really is.

With the results of the White Paper consultation published in February 2020, the development and implementation of these recommendations are still ongoing. The UK report recommends using a reasonableness test for imposing a standard of care. While it is unclear what the rubric for reasonableness might be, companies will be required to “take reasonable steps to keep users safe, and prevent other persons coming to harm as a direct consequence of activity on their services. This broader application of the duty, beyond simply users of a particular service, recognizes that in some cases the victims of harmful activity—victims of the sharing of non-consensual images, for example—may not themselves be users of the service where the harmful activity took place.” Still, it is unclear how a uniform reasonableness standard could be equitably implemented here.

Although the duty of care approach holds its appeal, calls for a more human rights centric framework have been made. Identification of the types of content that should be prioritized for removal is part of the broader agenda of work as states move to regulate content moderation of social media platforms.

A special unit was set up by the UK government in March 2020 to counter fake news on the coronavirus. The group of experts is to work in tandem with social media companies to prevent the spread of false information regarding the virus. According to Culture

---

118. Theresa May, Twitter post, April 8, 2019, 4:13 a.m., https://twitter.com/10downingstreet/status/11151657709915483648.
121. Ibid.
123. Ibid., 42.
125. Ibid.
127. Ibid.
Secretary Dowden, “defending the country” from misinformation and digital interference was a “top priority.”\textsuperscript{128} Lastly, in terms of bilateral agreements for facilitating law enforcement investigations, the United States and the United Kingdom entered into the first CLOUD Act agreement in October 2019.\textsuperscript{129} This bilateral agreement allows for criminal investigation cooperation between the two nations, facilitating the process through which law enforcement agencies can request electronic data from companies based in the other jurisdiction.\textsuperscript{130}

Building from this comparative overview, our focus shifts in the subsequent to providing an introductory primer on information warfare from the strategic doctrinal perspective of the Armed Forces of the Russian Federation and information operations according to the U.S. Department of Defense.

\begin{flushright}


\textsuperscript{130} Ibid.
\end{flushright}
Part III: A Primer for Policymakers on Information Warfare

What Is Information Warfare?

Information warfare, as defined here, is the military art of using information to deliberately mislead an adversary and influence their decisionmaking for a strategic purpose. At its core, understanding information warfare is much like studying an impressionist painting.\(^{131}\) Now, granted, the creative muse in Impressionism yields exquisite optical experiences to admire, whereas, in information warfare, there is a malicious intent to deceive an opponent.\(^{132}\) Both are alike, however, in their use of techniques to create impressions of modern life. Interestingly, the term “Impressionism” was originally intended to serve as an insult for painters whose work had an “unfinished, sketch-like appearance.”\(^{133}\)

The French art critic Edmond Duranty, however, praised the Impressionism art movement for conveying the “reality of the street”—our daily lives—in a novel way that viewers could identify with and recognize.\(^{134}\) Impressionism uses short brush strokes to present an illusion of the real-form object or person, as opposed to creating a fully detailed, finished work. Like the layers of artifice that are blended in information warfare to exploit the viewer’s perception of “the reality of the street,” the Impressionists’ style of painting is an aesthetically pleasing amalgamation of vibrant colors and forms to create an optical impression of reality, whether it be of a person, object, or landscape setting\(^{135}\) (see fig. 1). To view the painting properly, we need to step back from the center image to allow the optical illusion to come into focus before our eyes, recognizing that our view will never be crystal clear because that is not the “style” of this information art.\(^{136}\)


\(^{132}\) Ibid.


\(^{134}\) Ibid.


\(^{136}\) Malekos Smith “Artistic Impression of Information Warfare.”
Approaches to Hostile Information Campaigns: China, Russia, and the United States

A precise understanding of information warfare concepts and terminology is necessary to guide precision of thought in mitigating such threats. To that end, George Orwell wrote that whenever he would sit down to write a book, his philosophy was: “I write it because there is some lie that I want to expose, some fact to which I want to draw attention, and my initial concern is to get a hearing.”¹³⁸ In that same spirit, this report seeks to untangle common misperceptions about information warfare and encourage policymakers to be particularly attentive to the language used in developing a national strategy and addressing the public on these threats. Whereas U.S. military doctrine currently treats information operations and cyberspace operations as distinct zones organized under different Department of Defense directives, other near-peer competitors such as China and Russia do not.¹³⁹ Rather, it is regarded as part and parcel of combined arms warfare. This report chiefly focuses on Russia’s approach to information warfare but will very briefly highlight China’s increased exploration of this area in the wake of the Covid-19 pandemic.

**China and Informationized Wars**

In addition to China’s efforts to advance its commercial and technological interests, China has also developed “soft” techniques to influence public perception of the Chinese Communist Party (CCP) globally. According to Foreign Affairs, Beijing’s influence initiatives feature “both co-optation and manipulation, and they are targeted at the media, academia, and the policy community.”\(^{140}\) As part of its strategy to project national strength, Beijing plans to “permeate institutions in democratic states that might draw attention or raise obstacles to CCP interests, creating disincentives for any such resistance.”\(^{141}\) Further, under its evolving national defense doctrine, China announced in 2004 that “informationization has become the key factor in enhancing the warfighting capability of the armed forces.”\(^{142}\)

Why is it significant that China’s military conceptualizes the information environment as a strategic amalgamation? As Richard J. Harknett elucidates in *International Security*:

> If one examines the writings of Russian Gen. Valery Gerasimov and the Chinese People’s Liberation Army’s notions of informationized war, it becomes clear that certain actors see cyberspace as a strategically salient vector for achieving their goals below the traditional deterrence/war threshold. We must examine the dynamics of the cyber domain if we are to provide policies to secure it.\(^{143}\)

The ability to leverage these platforms in concert is a means to the strategic end of dominating great power competition. According to People’s Liberation Army Senior Colonel Xu Weidi, “cyber politics in international relations do not transcend the scope of power politics” and “the relationship between China and the United States in cyberspace is naturally manifested first as a competitive relationship.”\(^{144}\) Further elaborating on the interconnectedness of informationized war, Major General Hao Yeli, the former deputy director of the Fourth Department of the People’s Liberation Army’s General Staff Headquarters, explains that “in the cyber-electromagnetic space, war and peace are no longer distinct, and the front and rear are no longer [divided].”\(^{145}\)

In terms of China’s informationized war actions in the wake of Covid-19, in March 2020, Chinese agents sought to create panic in the United States by sending out fake text messages and social media announcements that the president had imposed a national

---

141. Ibid.
145. Ibid.
lockdown and deployed military troops to prevent looting. Apart from targeting the United States with influence operations, China also engaged in election interference and voter manipulation in Taiwan’s January 2020 general elections by using artificial intelligence and machine learning tools. According to a report by Recorded Future:

Chinese and Taiwanese content farms have become one of the biggest sources for misleading, intentionally biased, and false content in Taiwan. According to the database of Taiwanese fact-checking website MyGoPen (which translates to “don’t lie” in Taiwanese), at least 60% of false or misleading information forwarded to the site are from foreign sources, the majority of which are from mainland China.

Overall, the CCP conceptualizes the information environment as a strategic amalgamation to influence great power competition.

**Russia and Information Warfare**

The Armed Forces of the Russian Federation also conceptualizes cybernetic and information warfare as part of combined arms warfare, also known as New-Generation Warfare or Network-Centric Warfare. As Russian military theorists A.V. Raskin and V.S. Pelyak wrote in Military Thought, the official military publication of the Russian Armed Forces, “success in warfare is achieved not through numerical and firepower superiority of forces but through [1] information potential superiority [information warfare] and [2] the employment of warfighting entities with a fundamentally new network structure.”

Adding granularity to this comparative examination, the following section provides an overview of Russia’s information warfighting doctrine and then introduces the U.S. military’s approach to information operations. The analysis is neither intended to frighten nor inflame passions, rather, it is written from the clinical standpoint of a physician who wishes to understand the malaise of a patient in order to treat it.

Information warfare refers to a broad spectrum of activities constituting both active measures and passive measures like disinformation (дезинформация), imitation (имитация), surprise (внезапность), creativity (творчество), kidnapping, psychological reflexive control, and subversion, just to name several. Subversion, as defined by Professor Thomas Rid of Johns Hopkins University, appears in two main forms: “it may be intended as a non-violent prelude to insurrection and revolution, or it may evolve into a campaign with a non-revolutionary dynamic, be it violent or non-violent.”

---

150. Ibid.
Is There a Common Thread to All These Techniques?

The answer to that particular “riddle wrapped in a mystery inside an enigma” is called *maskirovka* (маскировка). *Maskirovka* is Russia’s strategic warfighting ideology of camouflage, concealment, and deception. This strategic doctrine dates back to 1904 with the founding of Russia’s first military *maskirovka* school. Although the school was dissolved in 1929, Russian military studies expert Timothy Thomas explains that “the Higher School of Maskirovka, provided the bases for maskirovka concepts and created manuals for future generations.”

Literally translated, *maskirovka* means “disguise” or camouflage; however, there is no direct equivalent to the concept in English. Further, Roger Beaumont cautions that although this concept pertains to “concealment and deception” tactics, it is “not identical with the western concept term of camouflage.” The central purpose of *maskirovka*, as Soviet Colonel V. Shchedrov wrote, “is to convince the enemy of the presence of troops and objectives in places where in fact they are not.”

Figure 2. Understanding the Components of Maskirovka

"The eye, which is called the window of the soul, is the chief means whereby the understanding may most fully and abundantly appreciate the infinite works of nature[.]” On Painting, The Notebook of Leonardo Da Vinci, (Random House, 1957), p. 35.

_MASKIROVKA_

While *maskirovka* could be likened to the Clausewitzian concept of the “fog of war,” it would perhaps be more accurate to conceptualize it as the lifeblood that sustains the Russian body politic in performing both military and non-military functions (e.g., intelligence gathering, conducting foreign diplomacy and trade, and carrying out humanitarian missions). The *Soviet Military Encyclopedia* defined *maskirovka* as an “aggregate of measures to deceive the adversary regarding the presence and disposition of troops (forces), military vehicles and installations (targets), their status and condition, combat readiness and actions, as well as command authority plans; category of operational (combat) support.”

Modern-day *maskirovka* also operates as an aggregate of measures to deceive the opponent and strategically influence their perception of the information environment in cyberspace, electronic warfare, kinetic operations, and global news media outlets. *Maskirovka* is

---

employed in combined arms-warfare—also described as New Generation Warfare—\textsuperscript{163} to alter the optics of a situation and help camouflage the state’s military and political objectives from opponents. Lastly, \textit{maskirovka} exists in both active and passive forms—“the former being methods of shielding and masking, the latter, the movement of forces and inobtrusive [sic] use of methods to deceive.”\textsuperscript{164} Denial of perception is at its core. Thus, \textit{maskirovka} is as much of a philosophy as it is a blending of stratagems to disorient and impede an opponent’s capabilities to accurately observe the “battlespace,” whether that’s in a traditional warfighting domain such as land, or sea, or simply the battle for public opinion.

\textbf{Disinformation (Дезинформация)}

In the \textit{New York Times}’ 2018 documentary on disinformation, active measures were defined in three categories: forgeries, disinformation, and kidnapping.\textsuperscript{165} The documentary described disinformation as being a concerted effort to manipulate public opinion for strategic gains. Unfortunately, this framework is misleading as it oversimplifies the concept of active measures and glosses over the nuances of Soviet military strategy and thinking. Even one of the training manuals on maskirovka, which was released publicly in the 1990s, warns that “it is essential to avoid underestimating the enemy, for a sure way of being deceived is to consider oneself more clever than others.”\textsuperscript{166}

According to an article by Thomas Boghardt from the Central Intelligence Agency’s online Public Library, active measures include, but are not limited to:

- Manipulation and media control, written and oral disinformation, use of foreign communist parties and front organizations, clandestine radio broadcasting, manipulation of the economy, kidnappings, paramilitary operations, and support of guerrilla groups and terrorist organizations. Under Joseph Stalin, active measures also included political assassinations. The basic goal of Soviet active measures was to weaken the USSR’s opponents—first and foremost the “main enemy” (glavny protivnik), the United States—and to create a favorable environment for advancing Moscow’s views and international objectives worldwide.\textsuperscript{167}

Further, Boghardt writes that \textit{dezinformatsiya} refers to activities to propagate “false or misleading information that Soviet bloc active measures specialists sought to leak into the foreign media.”\textsuperscript{168} He highlights the difference between the East and West in conceptualizing this concept. For example, for Westerners, “disinformation was a politically motivated lie, but Soviet bloc propagandists believed their disinformation campaigns merely highlighted greater truths by exposing the real nature of capitalism.” Thus, disinformation is neither a synonym for misinformation nor a stand-alone

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{163} Raskin and Pelyak, “On Network-Centric Warfare,” 87-88.
\item \textsuperscript{164} Beaumont, \textit{Maskirovka}, 7.
\item \textsuperscript{166} Jalali et al., “Maskirovka Outline.”
\item \textsuperscript{168} Ibid.
\end{itemize}
\end{footnotesize}
doctrine. Rather, it is a form of active measures—a deception technique employed in information warfare.

**What Are Active Measures?**

Active measures are a category of aggressive operation activities employed to conceal and protect the state’s strategic intentions from being discovered by an opponent. The Russian military and intelligence services have applied these concepts towards civilian and military audiences alike. According to Timothy Thomas, the purpose of disinformation is to “manipulate perceptions and information and misinform people or groups of people.” Moreover, disinformation is one technique employed in active measures that serve the Russian Armed Forces’ information warfare strategy. The 1990 Maskirovka Outline For POI published by the Xenophon Group describes other tactics like imitation and creativity as the process of learning your opponent’s “filter”—and then exploiting it to further the mission objectives.

Another tactic, called “reflexive control,” is a psychological warfare technique that was developed by the Soviet military to influence enemy commanders in their decisionmaking processes. The concept is simple: Based on your adversary’s unique proclivities and implicit biases, the aim is to construct a tantalizingly misleading “Information Doppelgänger” that will deceive them and hamper their efforts to discover your true strategic objectives. Thus, false information is thoughtfully constructed based on the adversary’s personal “skill and experience,” the operator’s estimation of the “effectiveness of the device utilized,” and surrounding political and social factors. Lastly, misinformation is not a recognized construct because the strategy employed in disinformation plays with shades of truth and falsity, much like how impressionist painting plays with light, shading and perspective, to create a moving optical illusion of reality.

The CRS defines misinformation as “the spreading of unintentionally false information. Examples include Internet trolls who spread unfounded conspiracy theories or web hoaxes through social media, believing them to be true.” The CRS distinguishes misinformation from disinformation by stating that “Unlike misinformation, disinformation is intentionally false. Examples include planting false news stories in the media and tampering with private and/or classified communications before their widespread release.” The CRS report makes clear that there are different types of

---

170. Thomas, *Russia’s Reflexive Control Theory*. “Some disinformation procedures are obvious, some are unconvincing, and others work through delayed perceptions, rumors, repetition, or arguments. Specific persons or particular social groups can serve as disinformation targets.”
172. Jalali et al., “Maskirovka Outline.”
177. Ibid.
information threats. For example, while the term “disinformation campaign” is used as a substitute term for information operations, “disinformation or deception is only one of the informational tools that comprise an IW [information warfare] strategy; factual information can also be used to achieve strategic goals and in some cases more effectively than deceptive means,” like leaking an adversary’s classified material to the public.

Again, understanding the essence of information warfare tactics and strategy is like looking at an impressionist painting. To properly view it, we need to step back to allow the four corners of the painting and the surrounding imagery to come into focus before our eyes, as illustrated in Figure 2.

The United States and Information Operations

The U.S. government has not formally defined information warfare but instead uses the term information operations. Pursuant to Department of Defense Joint-Publication 3-13 (DoD JP 3-13), Information Operations, the U.S. military defines information operations as: “The integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decisionmaking of adversaries and potential adversaries while protecting our own.”

These operations serve a variety of purposes such as preserving the element of surprise in a military operation to gain an advantage or protecting information about one’s forces and capabilities. Pursuant to DoD JP 3-13, there are five central pillars to information operations: (1) computer network operations, which are guided under DoD JP 3-12, Cyberspace Operations; (2) psychological operations; (3) electronic warfare; (4) operations security; and (5) military deception. In July 2018, the chairman of the Joint Chiefs of Staff announced that information was now a distinct form of warfare and the seventh Joint Function of the armed forces. To formally signal this doctrinal shift, the Chairman approved an out-of-cycle release of the Joint Concept for Operations in the Information Environment. Notably, the Joint Concept avoids the term information operations entirely and instead references the information environment as an aggregate of “numerous social, cultural, cognitive, technical, and physical attributes that act upon and impact knowledge, understanding, beliefs, world views, and, ultimately, actions of an individual, group, system, community, or organization. The [information environment] also includes technical systems and their use of data.” The following section examines Russia’s social media campaign targeting the 2016 U.S. presidential election.

The 2016 U.S. Presidential Election

As former director of the Central Intelligence Agency Michael V. Hayden wrote in his memoir, The Assault on Intelligence, “the central fact to be faced and understood here is that the
Russians have gotten very good indeed at invading and often dominating the American information space.” An examination of recent events is a testament to this: Beginning in February 2018, the U.S. Justice Department issued an indictment against 13 Russian nationals and 3 Russian companies for engaging in “information warfare,” with the intent to “interfere with U.S. political and electoral processes, including the 2016 U.S. presidential election.” Thereafter, in July 2018, 12 Russian intelligence officers were indicted by a grand jury in the District of Columbia on conspiracy charges to “hack into the computers of U.S. persons and entities involved in the 2016 presidential election, steal documents from those computers, and stage releases of the stolen documents to interfere with the 2016 presidential election.” On September 28, 2018, the Justice Department filed an indictment against a Russian national for engaging in information warfare against the United States to influence the midterm elections via “fictitious U.S. personas on social media platforms and other Internet-based media.”

One month later, the Department indicted seven Russian intelligence officers for waging a “disinformation campaign” against the United States.

Generally speaking, Russian cyber operations can be divided into two main categories: “[1] the collection of information and [2] intrusions designed to hold the target at risk,” writes Dr. Ben Buchanan and Dr. Michael Sulmeyer.

According to Tactics and Tropes of the Internet Research Agency, New Knowledge's report to the U.S. Senate Select Committee on Intelligence, Russia's interference took the following forms: (1) attempting to access online voting systems; (2) hacking into the Democratic National Committee’s networks and releasing information about the Clinton campaign through online fake identities and Wikileaks; and (3) conducting an elaborate information warfare campaign to exploit social tensions in the U.S. to influence voters. Further, according to Oxford University’s Computational Propaganda Research Project, more than 30 million U.S. social media users, “shared the IRA’s Facebook and Instagram posts with their friends and family, liking, reacting to, and commenting on them along the way” between 2015 and 2017 alone.

The Department of Justice's report by Special Counsel Robert S. Mueller, The Investigation into Russian Interference in the 2016 Presidential Election (hereafter, the Mueller Report),

---

193. Ibid.
also highlighted how the Russian state-sponsored Internet Research Agency served as the central conduit for disseminating propaganda. The Mueller Report was prepared for and submitted to the U.S. Attorney General for the purposes of investigating Russian interference in the 2016 U.S. election and the links between the Russian government and individuals involved with the Trump campaign.\textsuperscript{196} In a press conference at the Department of Justice on May 30, 2019, Special Counsel Mueller acknowledged that “there were multiple, systematic efforts to interfere in our election and that allegation deserves the attention of every American.”\textsuperscript{197} The Mueller Report describes how Russian intelligence officers serving under the Russian military engaged in continuous, systematic efforts to influence the U.S. political system.\textsuperscript{198} In addition, it outlines Russia’s use of social media to influence U.S. voters in the 2016 election and interfere with the political system. Despite this evidence, Russia denies interfering in the election.\textsuperscript{199}

\textit{Looking to the Future}

The Defense Advanced Research Projects Agency is developing software to help detect deepfakes (i.e., generative artificial intelligence) and other false media content to protect the integrity of elections.\textsuperscript{200} The aim of the project is to produce special custom software to detect fake content “hidden among more than 500,000 stories, photos, video and audio clips. If successful, the system after four years of trials may expand to detect malicious intent and prevent viral fake news from polarizing society.”\textsuperscript{201} The \textit{New York Times} reports that “almost all of the Russian disinformation efforts, according to current and former officials, are aimed at sowing dissent, polarizing the political parties and setting the stage for the 2020 presidential election.”\textsuperscript{202}

Apart from developing artificial intelligence tools and Congress’s ongoing efforts to draft legislation to protect election systems, the U.S. Army is also reevaluating its approach to training and preparing soldiers for conflict in the information environment. As an initial signal of the coming doctrinal changes, U.S. Army Cyber Commander Lt. Gen. Stephen Fogarty announced in 2019 that he wanted to rename Army Cyber Command to “Army Information Warfare Command.”\textsuperscript{203}

In sum, a precise understanding of information warfare concepts and terminology is necessary to guide precision of thought in mitigating these threats.

\textsuperscript{196} Ibid.
\textsuperscript{198} See Mueller Report.
\textsuperscript{201} Ibid.
Part IV: Building National Perseverance in the Information Environment

As a thematic scaffolding, this paper extends da Vinci’s juxtaposition of fire as a revealer of truth to offer a multipronged framework to support national perseverance against persistent information threats—the da Vinci F.I.R.E. Model for National Perseverance in the Information Environment: (F)ocusing on Smart Power in Great Power Competition, (I)nformation Sharing, (R)esiliency, and (E)ducation.

On truth, da Vinci wrote:

Fire destroys falsehood,—that is to say, sophistry,—and rehabilitates truth, scattering the darkness. Fire must be represented as the consumer of all sophistry and the revealer of truth, because it is light and scatters darkness which conceals all essences. Fire destroys all sophistry, that is to say, deceit, — and perseveres truth alone, which is gold. Truth cannot be concealed in the end, dissimulation is of no avail. There is nothing hidden under the sun. Fire must represent truth because it destroys all sophistry and lies, and the mask is for sophistry and lies, which conceal truth.204

Focus on Smart Power in Great Power Competition

International relations theorist Joseph S. Nye developed the concept of smart power because he wished to negate the opinion that soft power alone yields effective foreign policy.205 At its core, power is the ability to influence others to achieve a desired outcome. Hard power entails using methods of coercion and incentives (i.e., sticks and carrots), whereas soft power involves using persuasion to motivate others to do what you want them to do.206 Smart power is combining hard and soft power to achieve a strategic objective.207

The strategic value of applying smart power in modern foreign affairs, Nye explains, is that “the ability to get the outcomes we want will rest upon a new narrative of smart power. Americans will need to stop asking questions about who is number one, and entertaining narratives about dominance, and start asking questions about how the various tools of power can be combined into smart strategies for power with, rather than merely over other nations.”

According to United States Secretary of Defense Mark Esper, we are transitioning to a period of great power competition. One dimension of great power competition involves shaping and influencing strategic narratives as part of information warfare. In Secretary Esper’s 2019 address at the Air Force Association’s Air, Space and Cyber Conference, he cautioned that while “the United States military was focused on on-going activities in the Middle East, our strategic competitors were actively modernizing their militaries, growing their power and expanding their influence.”

On this point, Nye explains that “information affects power, and governments of all kinds will find their control eroding during the twenty-first century as information technology gradually spreads and costs continue to decrease.” The tools of national power that can be leveraged in designing smart power strategies include diplomacy, information, military, and economic. The axiom that information is power, coupled with Nye’s premise that power is context driven, underscores the point that the manner in which information is contextualized is a strategic concern in great power competition. Furthermore, as information communication technologies become increasingly embedded in our day-to-day lives, it has led to a diffusion of state power. This report recommends policymakers consider how smart power can be leveraged to address foreign information threats that undermine state sovereignty.

**Information Sharing**

Mitigating the effects of information operations will require an all-of-government approach with robust communication channels across public and private industry. A necessary first step is laying communication nodes across the intelligence community. As Rid writes in War and Media Operations, “Doctrinal concepts evolve hand in hand with technology, one shaping the other.” In terms of subsequent legislative developments, the U.S. Senate Democrats introduced the Combating Foreign Influence Act in September 2019 as Senate Bill 2493. The bill sought to establish a Malign Foreign Influence Response Center under the Office of the Director of National Intelligence, which would act as the central conduit for the intelligence community and other organizations to share election security data. According to the bill’s sponsor, Senator Amy Klobuchar

---

208. Ibid., xvii.
210. Ibid.
(D-MN): “We currently have numerous agencies and departments independently working to combat foreign influence, and it’s past time that our intelligence community comes together to fight these threats.”\textsuperscript{216} This provision of the Combating Foreign Influence Act was included in the National Defense Authorization Act and signed into law in December 2019.\textsuperscript{217} Establishing this response center to encourage information sharing on election security threats across local, state, and federal jurisdictions is a promising step. Another positive example of information sharing across federal and private industries to combat cyber threats is the Department of Homeland Security's Automated Information Sharing (AIS) database. The AIS database encourages private companies and federal agencies to report cyber threat information securely. According to DHS, by having this channel for the public sector to report cyber incidents “adversaries can only use that attack once, which increases their costs and ultimately reduces the prevalence of cyber attacks.”\textsuperscript{218} Similarly here, having an AIS-type system to examine foreign information operations could yield similar intelligence benefits.

To help support information sharing on election security threats, the former director of national intelligence Dan Coats announced the creation of a new government advisory position—the nation’s first election threats executive in July 2019.\textsuperscript{219} He also ordered each intelligence community agency to appoint an official to lead their election security efforts and serve as a liaison to the election threats executive.\textsuperscript{220} According to The Washington Times, this new intelligence community Election Threats Leadership Board would function as “the principal vehicle for IC-wide coordination and focus on election threats.”\textsuperscript{221} In terms of financially supporting election security initiatives, in 2019, a U.S. Senate panel agreed to allocate $250 million towards helping states improve their election systems and invest in updated voting systems for the 2020 election.\textsuperscript{222} The House of Representatives also passed legislation to award $600 million in grant money to states through the U.S. Election Assistance Commission, which was approved by the Senate Appropriations Committee in 2019.\textsuperscript{223} Overall, Congress has enacted several measures to support joint coordination against foreign influence operations and to bolster election security.

**Resiliency**

Resiliency refers to both hardening technological systems from manipulation and the concept of active defense, or “defend forward,” as promulgated by U.S. Cyber Command.

\begin{footnotes}
\item[216] Ibid.
\item[220] Ibid.
\item[221] Ibid.
\item[223] Ibid.
\end{footnotes}
Speaking to the former, developing artificial intelligence tools and machine learning capabilities is one way to help detect fraudulent content to generate technological resiliency. As mentioned in Part III, DARPA is developing software to help detect deepfakes and other false media content to protect the integrity of elections. Leveraging artificial intelligence tools also carries a degree of risk, however, for those very same tools may also be exploited for nefarious purposes.

For instance, the American Bar Association Journal highlights the nexus between AI and cybersecurity by noting that AI “has long been an important trend in the digital landscape, but it’s quickly expanding its influence into the world of cybersecurity. As it turns out, 62 percent of cybersecurity experts polled at the 2017 Black Hat USA conference predicted criminals would use AI as an offensive tool in the coming years, and they were right.”

On the other hand, companies can also develop malware AI bots in-house to then conduct penetration tests of their own network to learn about other malicious AI bots. One example is IBM’s AI bot DeepLocker. According to IBM’s Security Intelligence:

IBM Research developed DeepLocker to better understand how several existing AI models can be combined with current malware techniques to create a particularly challenging new breed of malware. This class of AI-powered evasive malware conceals its intent until it reaches a specific victim. It unleashes its malicious action as soon as the AI model identifies the target through indicators like facial recognition, geolocation and voice recognition.

Overall, pairing artificial intelligence in cybersecurity and human analysts together can help speed up detection and response time to attacks—which in the long term could save victim entities’ money, data, and resources.

As social media users struggle with recognizing deepfake-generated profile photos, some have started to proactively employ countertechnics. According to UCLA cybersecurity expert, Nicholas Weaver, one countertechnic is copying the profile image and pasting it into Google Images to run a reverse image search. “The search will then indicate which stock photo company the malicious actor was using for the account.” Some hackers, however, are working to undermine this detection method by using machine learning software to create fake photos. Thus, in practice, a bad actor could create AI-generated photos using an amalgamation of other photos so that it would trick the security algorithms used in Google Image Search. As a result, because the profile photo is an amalgamation of many fake photos and is like a generative adversarial network generated image, it is able to deceive Google’s search algorithm. Weaver asserts that this shows that LinkedIn is an open

226. Ibid.
228. Ibid.
229. Ibid.
230. Ibid.
“trove of information” on users that can be exploited by malicious actors.\textsuperscript{231} In addition, The Register reports that foreign intelligence agencies have created deepfake-generated LinkedIn accounts to recruit spies.\textsuperscript{232}

Apart from LinkedIn, the infamous fake “Drunk Pelosi” video is an illustrative example of the dangerous ability for deepfake videos to flourish online. In May 2019, a fake video of U.S. House Speaker Nancy Pelosi emerged on Facebook wherein she appeared drunk. The video showed Speaker Pelosi slurring her words and appearing intoxicated. It received more than 2.5 million views and was tweeted by several U.S. politicians—including President Trump.\textsuperscript{233} Deepfakes are a concern of the U.S. intelligence community and were identified in the 2019 Worldwide Threat Assessment report.\textsuperscript{234} Following this Pelosi video debacle, the U.S. House Permanent Select Committee on Intelligence held its first open hearing on AI to discuss the potential influence of deepfakes and bots on American voters in the 2020 election and how to protect voters. Next, we turn to examining resiliency in the context of military operations.

**RESILIENCY IN MILITARY OPERATIONS**

Apart from technological resiliency, military operational resiliency as an active defense posture is equally vital to counter malicious operations. This is seen in U.S. Cyber Command’s 2018 Cyber Strategy Report, which introduces the strategic concept of “defend forward.”\textsuperscript{235} The Cyber Strategy describes defend forward as “confronting threats before they reach U.S. networks”\textsuperscript{236} and is comprised of two components—the strategic persistent engagement of adversaries and working with allies and partners to promote security.\textsuperscript{237} According to DoD General Counsel Paul C. Ney, Jr., the defend forward strategy “envisions that our military cyber forces will be conducting operations in cyberspace to disrupt and defeat malicious cyber activity that is harmful to U.S. national interests.”\textsuperscript{238} Thus, defend forward prioritizes strategic persistent engagement—versus an episodic “hack-by-hack” type of response to an adversary—and engaging with international partners to promote security.\textsuperscript{239}

An example of collaboration is Cyber Command’s (hereafter CYBERCOM) ongoing information sharing and training efforts with Montenegro, a NATO ally, to promote election security in 2020.\textsuperscript{240} According to CYBERCOM’s executive director, David Luber, the agency is “seeing some very interesting malware and other activities when we

\begin{itemize}
\item \textsuperscript{231} Ibid.
\item \textsuperscript{232} Katyana Quach, “Politically linked deepfake LinkedIn profile sparks spy fears, Apple cooks up AI transfer tech,“ The Register, June 17, 2019, https://www.theregister.co.uk/2019/06/17/roundup_ai/.
\item \textsuperscript{234} Coats, Statement for the Record, 7.
\item \textsuperscript{236} Ibid.
\item \textsuperscript{239} Malekos Smith, “Would da Vinci Support the Pentagon’s New Cyber Strategy?”
\end{itemize}
conduct some of those defend-forward missions . . . Then we take that information and we share that broadly with industry and the rest of the government. Focusing now on persistent engagement, while this refers to continuous engagement with an adversary, such as anticipating the nature of a cyber operation and thwarting malicious activity, what makes it strategic? The answer is friction. Again, the friction concept was developed by Clausewitz in On War. Friction, as promulgated by the nineteenth century Prussian General Carl von Clausewitz, is about generating uncertainty and confusion in the conflict environment, as well as and depleting your adversary’s will to fight. Clausewitz posited:

> Everything is very simple in War, but the simplest thing is difficult. These difficulties accumulate and produce a friction which no man can imagine exactly who has not seen War. Suppose now a traveller, who towards evening expects to accomplish the two stages at the end of his day’s journey, four or five leagues, with post-horses, on the high road—it is nothing. He arrives now at the last station but one, finds no horses, or very bad ones; then a hilly country, bad roads; it is a dark night, and he is glad when, after a great deal of trouble, he reaches the next station, and finds there some miserable accommodation.

From his explanation of friction, we see how its contours extend beyond the battlefield. The essential goal is to create strategic disruptions, delay, and adversity with a combination of high and low visibility at the tactical, operational, and strategic levels of planning.

An example of how the U.S. military is defending forward against this and leveraging friction was in October 2018. The New York Times reported that CYBERCOM had begun its first overseas cyber operation to deter Russian operatives engaged in information warfare efforts against the United States. In addition, on the day of the U.S. 2018 midterm election, CYBERCOM also disrupted the Internet access of the Russian troll farm, the Internet Research Agency. The Washington Post reported that this operation marked the “first muscle-flexing by U.S. Cyber Command, with intelligence from the National Security Agency, under new authorities it was granted by President Trump and Congress last year to bolster offensive capabilities.” Another example was CYBERCOM’s actions in disabling a critical database used by Iran’s paramilitary forces in 2019. This targeting action was done in response to Iran’s actions in launching a surface-to-air missile on an unmanned U.S. Navy MQ-4 surveillance aircraft and waged mine attacks against tankers in the Strait of Hormuz. How has the defend forward strategy been perceived by states

243. Ibid.
246. Ibid.
248. Robert Chesney, “The Legal Context for CYBERCOM’s Reported Operations Against Iran,” Lawfare, June 24,
Like Russia? Interestingly, the May 2020 statement by the Permanent Mission of Russia to the UN on its non-participation in the UN Security Council Arria-Formula meeting on Cyber Stability, Conflict Prevention and Capacity Building reads as a subtly-crafted critique of this strategy of “preventative cyber strikes.” The open statement reads: “It is of grave concern that this ‘elite’ minority is actively pursuing the militarization of cyberspace by pushing forward the concept of ‘preventive military cyber strikes,’ including against critical infrastructure.”

Lastly, to help support a unity of effort in military cyberspace operations and prevent threats to national security systems and the defense industrial base, the National Security Agency director, General Paul M. Nakasone, announced the creation of NSA’s new Cybersecurity Directorate, led by Anne Neuberger, on October 1, 2019. Collectively, these are encouraging steps to developing technological and institutional resiliency; however, investing resources in teaching the public-at-large about these threats is equally significant.

**Education Initiatives to Promote Civic Literacy and Information Security Skills**

In the 1960s, President John F. Kennedy popularized the expression that “a rising tide lifts all boats.” While this concept is timeless, the tide is in need of encouragement when it comes to understanding modern threats to democracy. A rising tide of information security literacy and civic awareness can lift the knowledge baseline for all. As malicious actors exploit information and communications technologies to foment public discord and propagate false information to influence public opinion, democratic institutions face a heightened risk.

Here, the U.S. Department of Education can help make recommendations for education reform to the president in furtherance of the president’s education policies; however, the Department does not have the statutory authority to develop curricula or determine state education standards. The reason being, under the 1979 Department of Education Organization Act, that responsibility is reserved to the states and districts and between public and private organizations. Rather, the Department of Education “identifies the major issues and problems in education and focuses national attention on them.” The Department could focus national attention, for instance, on the need for computer science and information security literacy curriculums, as well as that in traditional fields like rhetoric, by preparing legislative proposals for Congress and the president to consider. As the threat and effects of information warfare become more pronounced in

---


251. Department of Education Organization Act of 1979 § 103[b].

252. Ibid.

cyberspace, society’s collective knowledge must also continuously evolve to stay abreast of cyber-enabled threats to democratic institutions. In summary, it is imperative that the public remains well informed about these deception techniques to help develop effective counter responses.
Conclusion

Light shines through glass, sometimes in a surprising way . . . You haven’t seen the light that way before but it reflects a rainbow. That’s what the law does. The law shows you new beauty. The law shows you new dimensions. The more you think about it, the more you study it, the more dedicated you are to it. But it’s also made of glass, and glass can break. Just like when the rule of law is broken, it requires great effort to fix it and you’re not sure that it will be as beautiful the next time.


This report explored how liberal democracies are grappling with addressing threats in the information environment. In addition, the report surveyed how information operations are influencing modern great power competition by generating civil discord and friction. Lastly, it offered a multi-pronged framework to support national perseverance against information threats. Democratic institutions face a heightened risk from malicious actors’ exploitation of news outlets and online platforms to propagate false information and sow civil strife. It is imperative that the public remains well-informed about these perpetual information threats to reduce their impact. As Justice Kennedy’s words remind us, protecting the rule of law is a delicate matter and will require great diligence and care from lawmakers to nurture democracy.

About the Author

Jessica “Zhanna” Malekos Smith, J.D., is a senior associate with the Center for Strategic and International Studies Technology Policy Program and a professor of cyber warfare studies with the Air War College. A former captain in the Air Force Judge Advocate General’s Corps, she has held fellowships with the Madeleine K. Albright Institute for Global Affairs, the Belfer Center’s Cyber Security Project at the Harvard Kennedy School, Duke University Law School as the Reuben Everett Cyber Scholar, and Stanford University’s U.S.-Russia Forum. Malekos Smith has presented her research at DEF CON, RSA Conference, and ShmooCon and has published op-eds in The Hill and Defense One, among others. She writes in the areas of science and technology, international law, international security and defense, and cybersecurity. She holds a B.A. from Wellesley College; an M.A. and A.K.C. from King’s College London, Department of War Studies; and a J.D. from the University of California, Davis, where she pursued a self-concentration in cyberlaw.