I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY

On the Organization of the U.S. Government for Responding to Adversarial Information Warfare and Influence Operations

HERBERT LIN*

CONTENTS

* I am grateful to Sonja Swanbeck for research assistance on Section III-C of this paper. In addition, an early draft of this paper was helpfully critiqued by Matthew Waxman, Kurt Sanger, Jack Goldsmith, Jon Hermann, Anne Applebaum, Braden Allenby, Robert Jervis, Rosanna Guandango, and Peter Shane.

I. ON THE IMPORTANCE OF INFORMATION WARFARE AND INFLUENCE OPERATIONS

Russian interference in the U.S. presidential election of 2016 impressed upon many Americans the significance and potential impact of information warfare and influence operations on the political fate of a nation. This paper defines information warfare and influence operations (IW/IO) as the deliberate use of information (whether true or false) by one party on an adversary to confuse, mislead, and ultimately to influence the choices and decisions that the adversary makes. [1] IW/IO is a hostile non-kinetic activity, or at least an activity that is conducted between two parties whose interests are not well-aligned. At the same time, IW/IO is not warfare in the Clausewitzian sense (nor in any sense presently recognized under the laws of war or armed conflict); it is better characterized as hostile or adversarial psychological manipulation. IW/IO has connotations of soft power (more properly, a mix of soft power and sharp power[2]): propaganda, persuasion, culture, social forces, confusion, deception. The patron saint of IW/IO is Sun Tzu, who wrote that, "The supreme art of war is to subdue the enemy without fighting."

---

[1] This description of information warfare and influence operations is taken from Herbert Lin and Jaclyn Kerr, "On Cyber-Enabled Information/Influence Warfare and Manipulation", August 8, 2017, forthcoming *Oxford Handbook of Cybersecurity*, 2018. Available at SSRN: Herbert Lin & Jaclyn Kerr, *On Cyber Enabled Information/Influence Warfare and Manipulation*, OXFORD HANDBOOK OF CYBERSECURITY 1, 4 (2018), https://ssrn.com/abstract=3015680 [https://perma.cc/R738-LZP7].

[2] *See* JOSEPH S. NYE JR., SOFT POWER: THE MEANS TO SUCCESS IN WORLD POLITICS, x (2004). *See also*, Christopher Walker & Jessica Ludwig, *The Meaning of Sharp Power: How Authoritarian States Project Influence*, FOREIGN AFFAIRS (Nov. 16, 2017), https://www.foreign affairs.com/articles/china/2017-11-16/meaning-sharp-power [https://perma.cc/RU8E-AVP3].

Regarding Russian activities in the 2016 election the Office of the Director of National Intelligence (ODNI) released a report in January 2017 stating that:[3]

> Moscow's influence campaign followed a Russian messaging strategy that blends covert intelligence operations—such as cyber activity—with overt efforts by Russian Government agencies, state-funded media, third-party intermediaries, and paid social media users or "trolls."

The ODNI report further noted that, "The Russians used cyber operations against both political parties, including hacking into servers used by the Democratic National Committee (DNC) and releasing stolen data [from the DNC and senior Clinton campaign personnel] to WikiLeaks and other media outlets. Russia also collected on certain Republican party-affiliated targets, but did not release any Republican-related data,"[4] and no evidence or fruits of such labors have as of yet come to public light.

The full extent of Russia's overt efforts as described by the ODNI are still unknown at this writing (and may never be fully known).[5] However, a number of aspects are known with high confidence. For example:

- The Internet Research Agency (a Russian "troll factory") exposed 126 million people to troll content through Facebook.[6]

---

[3] OFFICE OF DIR. OF NAT'L INTELLIGENCE, ICA 2-17-01D ASSESSING RUSSIAN ACTIVITIES AND INTENTIONS IN RECENT US ELECTIONS (2017), https://www.dni.gov/files/documents/ICA_2017_01.pdf.

[4] *Russian Interference in The 2016 United States Election: Before the Subcomm. on Crime and Terrorism of the S. Comm. on the Judiciary*, 115th Cong. 3 (2017) (statement of James R. Clapper, former Director of National Intelligence.) https://www.judiciary.senate.gov/imo/media/doc/05-08-17%20Clapper%20Testimony.pdf [https://perma.cc/N86P-2HJS].

[5] It should be recognized that these "overt" efforts were covert in at least one sense—the Russian actors concealed their identities in conducting their activities on social media.

[6] *Hearing on "Extremist Content and Russian Disinformation Online: Working with Tech to Find Solutions" Before the United States S. Comm. on the Judiciary Subcomm. on Crime and Terrorism*, 115th Cong. 1, 6 (2017) (written statement of Colin Stretch, General Counsel, Facebook), https://www.judiciary.senate.gov/imo/media/doc/10-31-17%20Stretch%20Testimony.pdf [https://perma.cc/GHN9-N824].

- Twitter identified 36,746 Russian automated accounts tweeting election-related content as Russian-linked, generating 1.4 million election-related tweets, many amplified through liking and retweeting.[7]
- Google identified about 1,100 videos with 43 hours of YouTube content tied to the Russian campaign, of which a few dozen had in excess of 5,000 views each.[8]
- Prior to the 2016 U.S. election, Cambridge Analytica improperly received the Facebook information of up to 87 million Facebook users, mostly in the United States.[9] According to Reuters, the former chief executive of Cambridge Analytica claimed that this firm had played a decisive role in U.S. President Donald Trump's 2016 election victory.[10]

Whether these effects had an impact on the outcome of the election is not known; although one study suggests that they may have been sufficient to flip the outcome from an expected Clinton victory to an unexpected Trump victory.[11] These findings have not been replicated in any other study to the best of this author's knowledge.

---

[7] *Hearing on "Extremist Content and Russian Disinformation Online: Working with Tech to Find Solutions" Before the United States S. Comm. on the Judiciary Subcomm. on Crime and Terrorism*, 115th Cong. (2017) (statement of Sean J. Edgett, Acting General Counsel, Twitter).

[8] *Hearing on "Extremist Content and Russian Disinformation Online: Working with Tech to Find Solutions" Before the United States S. Comm. on the Judiciary Subcomm. on Crime and Terrorism*, 115th Cong. (2017) (statement of Richard Salgado, Senior Counsel, Law Enforcement and Information Security, Google).

[9] Mike Schroepfer, *An Update on Our Plans to Restrict Data Access on Facebook*, FACEBOOK (Apr. 4, 2018), https://newsroom.fb.com/news/2018/04/restricting-data-access/ [https://perma.cc/5VYB-SDGK].

[10] Eric Auchard & David Ingram, *Cambridge Analytica CEO Claims Influence on US Election, Facebook Questioned*, REUTERS (Mar. 20, 2018), https://www.reuters.com/article/us-facebook-cambridge-analytica/cambridge-analytica-ceo-claims-influence-on-u-s-election-facebook-questioned-idUSKBN1GW1SG [https://perma.cc/PPY4-BE8R].

[11] Richard Gunther, Paul A. Beck, & Erik C. Nisbet, *Fake News May Have Contributed to Trump's 2016 Victory* (Mar. 8, 2018), https://assets.documentcloud.org/documents/4429952/Fake-News-May-Have-Contributed-to-Trump-s-2016.pdf [https://perma.cc/Q6DX-SBRT]. An earlier version of this report was published February 15, 2018 in *The Conversation*. Richard Gunther, Erik C. Nisbet, & Paul Beck, *Trump may owe his 2016 victory to 'fake news,' new study suggests*, THE CONVERSATION (Feb. 15, 2018), http://theconversation.com/study-suggests-trump-may-owe-his-2016-victory-to-fake-news-91538 [https://perma.cc/2XMY-WGEN].

II. CYBER WAR, INFORMATION WARFARE, AND INFLUENCE OPERATIONS

Many political commentators, Democrats and Republicans alike, have pointed to the Russian interference with the 2016 election as cyber warfare. For example, Senator Dianne Feinstein has said: "What we're talking about is a cataclysmic change. What we're talking about is the beginning of cyber warfare."[12] Similarly, former Vice President Dick Cheney stated:[13]

> Putin's conduct . . . has to do with cyber warfare, cyberattack on the United States—the fact that he used his capabilities in the cyber area to try to influence our election. . . Putin and his government, his organization, interfere[d] in major ways with our basic fundamental democratic processes. In some quarters, that would be considered an act of war.

The conclusion that Russian interference in the 2016 election is an act of cyberwar is understandable, but it is deeply misleading and even dangerous.[14]

To the extent that Russian meddling in the 2016 election involved malicious cyber activities, strengthening the electoral infrastructure of the United States would be part of a plausible response strategy. Indeed, on March 22, 2018 a bipartisan group of six senators introduced the "Secure Elections Act," which is intended to

---

[12] *Open Hearing: Social Media Influence in the 2016 U.S. Election Before the S. Select Comm. on Intelligence*, 115th Cong. 61 (2017) (statement of Sen. Dianne Feinstein, Member, S. Select Comm. on Intelligence).

[13] Kristine Phillips, *Cheney Delivers a Statement on Russian Meddling: "It's an 'Act of War',"* WASH. POST. (Mar. 28, 2017), https://www.washingtonpost.com/news/the-fix/wp/2017/03/28/cheney-is-the-latest-republican-to-call-russias-alleged-meddling-in-u-s-elections-an-act-of-war/?utm_term=.4352b7aae811 [https://perma.cc/4KMU-3LS7].

[14] The very term "act of war," let alone "act of cyberwar," is problematic from an international legal standpoint, as the term "act of war" has been replaced by terms used in the UN Charter, namely "armed attack" and "use of force." The Charter does not define these terms with any specificity, and since the Charter was written in 1945, long before cyber conflict was ever imagined as an issue of international relations, it is most unclear how "armed attack" and "use of force" apply to cyber war. Perhaps more importantly, how any nation under any particular circumstances interprets "armed attack" or "use of force" is first and foremost a political decision. Different governments in different nations under different circumstances will interpret it differently.

"streamline cybersecurity information-sharing between federal intelligence entities and state election agencies; provide security clearances to state election officials;" and provide support for state election cybersecurity infrastructure.[15] The authors of this legislation, and press stories around it, characterize it as a bill to improve the cybersecurity of the U.S. election infrastructure.

The Secure Elections Act addresses the covert Russian cyber activity to which the ODNI report referred and falls within the general scope of what the U.S. government defines as cybersecurity, an official definition of which is contained in NSPD-54:[16]

> [P]revention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and non-repudiation.

But the ODNI report also referred to overt Russian activities—messaging activities that can fairly be characterized as information warfare and influence operations directed against the United States. Even if the DNC and John Podesta (and others) had maintained perfect cybersecurity against intrusions, the overt Russian activities to affect political discourse during the election would have proceeded unimpeded (though the absence of the email releases might have diminished their effectiveness).

It is for this reason that a focus on election cybersecurity as it is defined by the U.S. government (and used to define responsibilities, authorities, budgets, and the like) is misleading and dangerous—it does not speak to the toxic nature of political discourse in an Internet-enabled information environment that Russia can manipulate in ways that may be entirely legal.

---

[15] Press Release, Sen. James Lankford et al., Senators Introduce Revised Secure Elections Act with Burr, Warner's Support (Mar. 22, 2018), https://www.lankford.senate.gov/news/press-releases/senators-introduce-revised-secure-elections-act-with-burr-warners-support [https://perma.cc/5RHS-MMMB].

[16] National Security Presidential Directive 54, *Cybersecurity Policy* (Jan. 8, 2008), https://fas.org/irp/offdocs/nspd/nspd-54.pdf [https://perma.cc/Q45Q-HD8H].

When adversaries wage cyberwar, they take advantage of design, implementation, or configuration flaws in the information technology systems and networks they target. For example, they exploit zero-day vulnerabilities in a system,[17] they successfully guess weak passwords, or they enter an Internet-connected system through a port that was inadvertently left open. Better cybersecurity would help to reduce an adversary's ability to wage cyberwar.

By contrast, when adversaries wage cyber-enabled information warfare or conduct influence operations, they take advantage of the features that information technology systems and networks are designed to offer. The Russians used social media exactly as they were designed to be used—Facebook, for example, to direct selected advertisements and other content to very narrowly defined audiences and Twitter to exploit automated accounts to amplify selected messages.

Recalling the definition of information warfare and influence operations above (i.e., the deliberate use of information to confuse, mislead, and affect the choices and decisions that the adversary makes), it is clear that better cybersecurity would not help reduce an adversary's ability to wage information warfare or conduct influence operations.

III. WHY DOES CYBER-ENABLED IW/IO WORK?

The effectiveness of cyber-enabled IW/IO depends on two distinct factors—characteristics of human cognition and emotion and the affordances granted by modern information technology.

A. *On the Psychology of IW/IO*

Information warfare and influence operations have a very long pedigree, and effective practitioners have often exploited principles of

[17] A vulnerability is a design or implementation flaw in a system that may have been introduced accidentally (in which case it is usually called a "bug") or deliberately (e.g., by an untrustworthy insider). A system with a vulnerability can be penetrated by an adversary who knows of it. When an adversary uses a vulnerability that is unknown to others to effect penetration, it is termed a "zero-day" vulnerability, since the victim will have had zero days to repair it.

human cognition in their tradecraft. For example, on propaganda, Hitler wrote that:[18]

> [I]ts purpose must be . . . to attract the attention of the masses and not by any means to dispense individual instructions to those who already have an educated opinion on things or who wish to form such an opinion on grounds of objective study -- because that is not the purpose of propaganda, it must appeal to the feelings of the public rather than to their reasoning powers . . .
>
> The art of propaganda consists precisely in being able to awaken the imagination of the public through an appeal to their feelings, in finding the appropriate psychological form that will arrest the attention and appeal to the hearts of the national masses . . . The receptive powers of the masses are very restricted, and their understanding is feeble . . .
>
> The aim of propaganda is not to try to pass judgment on conflicting rights, giving each its due, but exclusively to emphasize the right which we are asserting. Propaganda must not investigate the truth objectively and, in so far as it is favourable to the other side, present it according to the theoretical rules of justice; yet it must present only that aspect of the truth which is favourable to its own side.

Today's cognitive and social psychology formalizes what Hitler knew intuitively. Specifically, heuristic dual-system cognitive theory—the same psychology that underlies the transformation of neoclassical economics to behavioral economics posits that human beings have two systems for cognitive processing—an intuitive system (often designated as System 1) and an analytical system (often designated as System 2).[19] System 1 is designed to operate rapidly—the default

---

[18] Adolf Hitler, *Mein Kampf*, 155-158 (1925), http://www.greatwar.nl/books/meinkampf/meinkampf.pdf [https://perma.cc/3YPX-4NNW].

[19] For a primer on System 1 and System 2 thinking, see DANIEL KAHNEMAN, THINKING, FAST AND SLOW (Farrar, Straus & Giroux, 2011); Richard Petty & John Cacioppo, *The Elaboration Likelihood Model of Persuasion*, 19 ADVANCES IN EXPERIMENTAL SOCIAL

system of thought, it acts reflexively, and so does process all available information. It is thus more prone to error (also called bias).[20] System 2 operates more slowly—it is rule-based, abstract, and linked to language and conscious thought. Because it operates more slowly, it is better able to consider more of the available information, therefore, making it less prone to error.[21] People engaging in System 1 information processing respond more emotionally and less rationally or critically than System 2 information processing, but they also respond more quickly as well.[22]

Most individuals are capable of both System 1 and System 2 thinking.[23] The important operative question to ask, therefore, is what kinds of circumstances drive an individual to System 1 or System 2 thinking?[24]

Substantial evidence indicates that an individual is far less critical of information that is favorable to his or her position than of information that is not favorable.[25] In other words, individuals are more likely to engage in System 1 thinking when favorable information is involved.[26] For example, people are well known to exhibit confirmation bias in their information seeking and processing behavior.[27] They preferentially seek out information that is consistent

---

PSYCHOLOGY 123, 125 (1986) (For other variants of dual-system cognitive theory); Shelly Chaiken, *The Heuristic Model of Persuasion*, *in* 5 SOCIAL INFLUENCE: THE ONTARIO SYMPOSIUM 3-6 (Mark P. Zanna et al. eds., Psychology Press 1987); For a contrary view on dual-system cognitive theory, see Arie W. Kruglanski & Erik P. Thompson, *Persuasion by a Single Route: A View from the Unimodel*, PSYCHOLOGY INQUIRY, Nov. 9, 2009, at 83-84, 88.

[20] *Id.*

[21] *Id.*

[22] *Id.*

[23] *Id.*

[24] *Id.*

[25] Charles S. Taber & Milton Lodge, *Motivated Skepticism in the Evaluation of Political Beliefs*, 50 AM. J. OF POL. SCI. 755, 755-56 (2006).

[26] *Id.*

[27] For example, in a meta-analysis of 91 studies, Hart et al. considered two motivations for how an individual might select information to consume—the desire to gain an accurate understanding of reality and the desire to feel validated in his or her beliefs. These two motivations conflict when an accurate understanding of reality does not validate one's beliefs, and such a situation motivates the question of which of these motivations is more

with their beliefs and they are highly critical of (or ignore) information that contradicts their beliefs.[28]

Maintenance of an individual's social identity also has an important influence on his or her selection of System 1 or System 2. The evidence suggests that individuals tend to adopt the views of the peer groups that are most salient to them, even if the "objective" or "factual" information available to them contradicts those views.[29] Therefore, uncritical System 1 thinking is more often active in processing information consonant with the beliefs and attitudes of those groups, and critical and skeptical System 2 thinking is more often active in processing information that is dissonant. These effects (that individuals tend to accept salient group norms) are even more pronounced in an anonymous environment (such as that which characterizes much online interaction).[30]

Lastly, there is evidence that emotions and motivations affect cognition. For example, Bodenhausen et al found that subjects who were angry tended to rely more heavily on simple heuristic cues (suggestive of System 1 thinking) than those who were not angry, though they were careful not to speculate on the reason for this

---

powerful. Hart et al. concluded that both motivations drive human information-seeking behavior, thus moderating each other to a certain extent, but that on balance, humans do exhibit a tendency towards the validation of their beliefs. William Hart et al., *Feeling Validated Versus Being Correct: A Meta-Analysis of Selective Exposure to Information*, 135 AM. PSYCHOL. ASS'N. 555, 556-559 (2009).

[28] For example, in a meta-analysis of 91 studies, Hart et al considered two motivations for how an individual might select information to consume—the desire to gain an accurate understanding of reality and the desire to feel validated in his or her beliefs. These two motivations conflict when an accurate understanding of reality does not validate one's beliefs, and such a situation motivates the question of which of these motivations is more powerful. Hart et al conclude that both motivations drive human information-seeking behavior, thus moderating each other to a certain extent, but that on balance, humans do exhibit a tendency towards the validation of their beliefs. See William Hart et al, "Feeling Validated Versus Being Correct: A Meta-Analysis of Selective Exposure to Information," *Psychological Bulletin* 135(4):555-588, 2009, http://psycnet.apa.org/record/2009-09537-004 [https://perma.cc/PD2E-CUGB].

[29] The classic experiments along these lines ("conformity experiments") were performed by Solomon E. Asch in the early 1950's. See, for example, SOLOMON E. ASCH, EFFECTS OF GROUP PRESSURE UPON THE MODIFICATION AND DISTORTION OF JUDGMENTS, *in* GROUPS, LEADERSHIP, AND MEN 226 (Harold Guetzkow, 1951).

[30] Tom Postmes et al., *Social Influence in Computer-Mediated Communication: The Effects of Anonymity on Group Behavior*, 27 PERSONALITY & SOC. PSYCHOL. BULL. 1243, 1252 (2001).

tendency.[31] Kunda and Sinclair found that individuals were more likely to stereotype people (a form of System 1 thinking) when that stereotype was consistent with their desired impression of those people; conversely, when the stereotype was inconsistent with their desired impression, individuals tended to inhibit the use of this stereotype.[32] Goel and Vartanian found that negative emotions (such as those induced by the receipt of information incongruent with a person's prior beliefs) can improve the ability of a person to reason logically, thus enabling him or her to negate or discount that information.[33]

B. *Impact of Today's Cyber-Enabled Capabilities on IW/IO*

The psychological tendencies in human beings described above have been present for millennia. But today's information-age technologies give IW and IO practitioners capabilities that could not have been imagined in the wildest dreams of master propagandists such as Stalin and Hitler. Specifically, modern information technologies and the Internet provide high connectivity, low latency, high degrees of anonymity, customized information searches, insensitivity to distance and national borders, democratized access to publishing capabilities, and inexpensive production and consumption of information content. These aspects of modern information technologies enable foreign practitioners of IW and IO to use automated Twitter accounts to amplify one-sided messages, to communicate with large populations at low cost without accountability, to pay foreign trolls to masquerade as Americans, to tailor inflammatory and inauthentic political messages in a manner highly customized to narrow audiences, and to leak confidential emails purloined from the accounts of political parties and personnel.[34]

---

[31] Galen Bodenhausen et al, *Negative Affect and Social Judgment: The Differential Impact of Anger and Sadness*, 24 EUR. J. OF SOC. 45, 58-59 (1994).

[32] Ziva Kunda & Lisa Sinclair, *Motivated Reasoning with Stereotypes: Activation, Application, and Inhibition*, 10 PSYCHOL. INQUIRY 12, 20-21 (1999).

[33] *See* Vinod Goel & Oshin Vartanian, *Negative Emotions Can Attenuate the Influence of Beliefs on Logical Reasoning*, 25 COGNITION & EMOTION 121, 127 (2011).

[34] Herbert Lin, "Cyber Assaults on Democracy's 'Brain-Space' are Here to Stay", THE CIPHER BRIEF (Sept. 17, 2017), https://www.thecipherbrief.com/cyber-assaults-democracys-brain-space-stay [https://perma.cc/HG9H-X22U].

Perhaps most importantly, information age technologies and the internet have increased the volume and velocity of information in the public sphere by orders of magnitude in the last few decades (remember that the World Wide Web was invented in 1995, less than a quarter century ago) while the natural cognitive processing capabilities of human beings have not changed at all.

Faced with a deluge of information and a chaotic information environment, people take measures to reduce their information overload. System 1 information processing is ideally suited for doing exactly that, and adversaries conduct cyber-enabled IW/IO to push people into that mode of thinking—a mode that is less rational, less critical, and more emotionally driven.[35] Applying these cognitive tendencies to the cultural and political climate of today, adversaries such as Russia seek to increase polarization and divisiveness in democratic nations, amplifying existing anger and resentment to the point where rational discourse is nearly impossible.

To date, the mechanisms of cyber-enabled IW/IO have been relatively simple. What might we see in the future?

C. *Future Cyber-Enabled Capabilities for IW/IO*

The future is likely to bring a new level of technological sophistication to the instruments of cyber-enabled IW/IO. Some of the possibilities include the following.

1. *Faked Documents*

To date, leaked documents have for the most part been authentic. But it does not take much imagination to consider artfully forged emails that are released along with purloined emails, with content in these forged emails intended to mislead and/or create artificial scandal. These forged emails will be difficult to distinguish from authentic emails that are released simultaneously.

Indeed, there is today at least one documented instance of such machinations. In May 2017, the Citizen's Lab at the University of Toronto released a report about documents stolen from a prominent journalist and critic of the Russian government that were manipulated

---

[35] Herbert Lin & Jacyln Kerr, *On Cyber-Enabled Information/Influence Warfare and Manipulation*, OXFORD HANDBOOK ON CYBERSECURITY (forthcoming 2019).

and then released as a "leak" to discredit domestic and foreign critics of that government.[36]

2. *Name-matched Use of Personal Information Obtained From Multiple Sources*

In 2018, the improper access of Facebook data by Cambridge Analytica made front-page headlines around the world. Although this incident involved the data from tens of millions of American Facebook users, it involves only one data source—Facebook. But there have been many data breaches over the past several years (e.g., Equifax, Anthem, the U.S. government Office of Personnel Management) that have resulted in the compromise of personal information. As capacious and detailed as Facebook is as a repository of personal information, adding even more information from other sources to the Facebook data trove can only be more worrisome. Combining information from multiple sources (multiple social media sources and multiple data brokers, for example) can result in profiles of individuals that are even more detailed than what was possible with Facebook data alone, and one can easily imagine that in the future specific individuals would be the recipients of specially targeted political messaging, a term that includes both explicit advocacy of candidates and hot-button issues that may affect a campaign.

3. *Exploitation of Emotional State*

Near-real-time use of social media and other clues can help to pinpoint the moments in time when specific individuals are most susceptible to particular kinds of messaging. Demonstrating the feasibility of such targeting, a Facebook document leaked in May 2017 suggested that Facebook was capable of identifying teenagers at moments when they needed a boost in confidence, such as when they were feeling "stressed, "a failure", "worthless," "insecure," "defeated," "anxious," "silly," "useless," "stupid," or "overwhelmed."[37] Responding

[36] Adam Hulcoop *et al*, *Tainted Leaks Disinformation and Phishing with a Russian Nexus*, THE CITIZEN LAB (May 25, 2017), https://citizenlab.ca/2017/05/tainted-leaks-disinformation-phish [https://perma.cc/ER37-R7ZL].

[37] Sam Machkovech, *Report: Facebook helped advertisers target teens who feel "worthless" [Updated]*, ARS TECHNICA (last visited May 1, 2017), https://arstechnica.com/information-technology/2017/05/facebook-helped-advertisers-target-teens-who-feel-worthless/ [https://perma.cc/VJU5-23R2].

to stories about this leaked document, Facebook only stated that it was not offering tools to advertisers to target teenagers in such a manner.[38]

Given this backdrop, it is interesting to speculate on the possibility that an adversary might be able to target specific individuals with highly tailored messages at specific times of maximum emotional vulnerability or stress.

4. *AI-driven Chatbots Indistinguishable From Human Beings*

AI-driven chatbots will be capable of engaging in realistic text-based conversation about hot-button issues that work to intensify anger and resentment on a one-on-one basis. These chatbots will not be able successfully emulate all aspects of human communication; however, within the domain of a one-sided and biased political conversation, it will be difficult or impossible to distinguish them from the persons they are trying to emulate. These chatbots are likely to work most effectively against audiences who do not expect to be talking to automated agents and who welcome the messages spreading.

A number of recent developments suggest the feasibility of such chatbots. Human-simulating chatbots designed to persuade would ideally demonstrate command of relevant facts and logic, sound like actual humans, and make emotional connections.

- In July 2018, IBM's AI-driven Project Debater engaged in a live, public debate with a human debater.[39] The specific topics chosen for debate were not known beforehand, though they were selected from a known list of about 100 topics. The Project Debater knowledge base was a library of hundreds of millions of articles from numerous well-known newspapers and magazines.[40] Given the topic, each party delivered a four-minute opening statement, a four-minute rebuttal, and a two-minute summary. The BBC reported that the human audience

---

[38] *Id.*

[39] Arvind Krishna, *AI Learns the Art of Debate*, IBM NEWSROOM: IBM RESEARCH (June 18, 2018), http://newsroom.ibm.com/IBM-research?item=30543 [https://perma.cc/DL9A-32K5].

[40] IBM, *IBM Project Debater FAQ*, IBM RESEARCH: AI RESEARCH, https://www.research.ibm.com/artificial-intelligence/project-debater/faq.html [https://perma.cc/7DGL-6Z9Z].

believed that the human debaters had better delivery and that the machine "offered greater substance in its arguments."[41] In the words of the director of IBM Research, the Project Debater system "absorbs massive and diverse sets of information and perspectives *to help people build persuasive arguments* and make well-informed decisions."[42]

- Chatbots that sound like real human beings have come a long way in the 50 years since the first chatbot, ELIZA, was created by Joseph Weizenbaum in 1966.[43] In March 2016, Microsoft debuted the Tay chatbot, aimed at an audience of 18-24 year-olds. Within a day, Tay had been targeted in a "coordinated attack by a subset of people" that induced Tay to issue a variety of offensive racist and genocidal tweets.[44]
- Microsoft quickly took Tay offline and apologized for the comments, but it is a clear example of how exposure to a particular kind of online environment can train an artificial intelligence to mimic that environment.
- Microsoft's XiaoIce chatbot is capable of "learning" about the person with whom it is interacting and engaging in a natural conversation. Operated primarily for a Chinese audience, XiaoIce had 20 million users in 2015.[45] Senior Microsoft researchers associated with XiaoIce said that the appeal of "social chatbots" lies not only in their ability to respond to users' diverse requests, but also in being able *to establish an emotional connection with users*, the latter of which is done by

---

[41] Dave Lee, *IBM's Machine Argues, Pretty Convincingly, with Humans*, BBC NEWS (June 19, 2018), https://www.bbc.com/news/technology-44531132 [https://perma.cc/PNW6-Y2W2].

[42] Arvind Krishna, *AI Learns the Art of Debate*, IBM NEWSROOM: IBM RESEARCH (June 18, 2018), http://newsroom.ibm.com/IBM-research?item=30543 [https://perma.cc/4N3H-3TC4].

[43] Joseph Weizenbaum, *ELIZA - A Computer Program for the Study of Natural Language Communication between Man and Machine*, 9 COMM. OF THE ACM 36, 36 (1966).

[44] Sophie Kleeman, *Here Are the Microsoft Twitter Bot's Craziest Racist Rants*, GIZMODO (March 24, 2016) https://gizmodo.com/here-are-the-microsoft-twitter-bot-s-craziest-racist-ra-1766820160 [https://perma.cc/M3AM-N6XS].

[45] John Markoff & Paul Mozur, *For Sympathetic Ear, More Chinese Turn to Smartphone Program*, N.Y. TIMES (July 31, 2015), https://www.nytimes.com/2015/08/04/science/for-sympathetic-ear-more-chinese-turn-to-smartphone-program.html [https://perma.cc/YR9N-D9GV].

> "*satisfying users' need for communication, affection, as well as social belonging*."[46] Further, these researchers report that XiaoIce does in fact enable such connection for many of its users.

Taken together, these developments suggest the eventual feasibility of politically persuasive chatbots that are more or less indistinguishable from a human being to the untrained eye—and "eventually" may not be very long from now.

5. *Realistic Video and Audio Forgeries*

From rudimentary scam robocalls that collect people's voices saying the word "yes" in order to confirm fraudulent purchases to sophisticated video editing programs, technology is enabling highly realistic forgery of speech and video (also known as deepfakes).[47]

For example, Adobe's Voco program (at this writing, still in beta testing and not yet on the market) has been described by one of its developers as Photoshop for voice.[48] Where previous audio editing technologies are limited to audio cutting, copying, and pasting, Voco allows editors to add words that don't appear in the original audio file in the same voice as the original narration with only about 20 minutes of recorded speech for analysis. Voco was demonstrated at Adobe's MAX Conference in 2016. Using a voice sample from comedian Keegan-Michael Key to change a sample audio of him saying, "I kissed my dogs and my wife" to a realistic sample of him saying, "I kissed Jordan three times."[49] Today, Voco's capabilities are limited in that it

---

[46] Heung-Yeung Shum, Xiaodong He & Di Li, *From Eliza to XiaoIce: Challenges and Opportunities with Social Chatbots*, 19 FRONTIERS OF INFO. TECH. & ELECTRONIC ENGINEERING 10, 10-13 (2018).

[47] Annalyn Kurtz *Regulators Are Warning People Not to Fall for This Sneaky Phone Scam*, FORTUNE MAGAZINE (Mar. 28, 2017), http://fortune.com/2017/03/28/yes-scam-phone-call/ [https://perma.cc/57UX-68KY].

[48] Matthew Gault, *After 20 Minutes of Listening, New Adobe Tool Can Make You Say Anything*," VICE: MOTHERBOARD (Nov. 5, 2016), https://motherboard.vice.com/en_us/article/jpgkxp/after-20-minutes-of-listening-new-adobe-tool-can-make-you-say-anything [https://perma.cc/9H6Y-WGX9].

[49] Peter Dockrill, *Adobe's New 'Photoshop For Voice' App Lets You Put Words in People's Mouths*, SCI. ALERT (Nov. 11, 2016), https://www.sciencealert.com/adobe-s-new-photoshop-for-voice-app-lets-you-put-words-in-people-s-mouths [https://perma.cc/W926-698Q].

can only be used to manipulate a word or short phrase rather than a longer sample, which for Voco tend to sound less natural.

WaveNet, developed by Google's DeepMind, performs a similar function to that of the Voco project, but is designed to generate authentic-sounding speech samples of longer length. Wavenet depends on a neural network to generate raw audio waveforms, which are then linked to produce new speech. Wavenet's generated speech samples have been tested in at least one instance as being more natural than other voice generators. Wavenet can be trained on one speaker's voice to create a voice mimic, on multiple speakers' voices to create a generic voice, or on classical music samples to create realistic-sounding new music samples. Interestingly, when trained on multiple speakers, the program performed better at modelling a single speaker's voice than when it was trained on just one voice. [50] The main limitation of the technology is that it cannot read a straight text input yet, but instead requires text that is pre-translated into computer readable phonetic spelling.[51]

Researchers have also been able to create digital replicas of faces that defeat relatively sophisticated facial recognition software. At a security conference in 2016, computer vision specialists from the University of North Carolina constructed 3D facial models based on publicly available Facebook photos and displayed them with mobile VR technology to defeat five out of five popular facial recognition systems that were tested (KeyLemon, Mobius, TrueKey, BioID, and 1D).[52]

---

[50] Aaron van den Oord *et al.*, *WaveNet: A Generative Model for Raw Audio*, GOOGLE DEEPMIND (Sep. 19, 2016), https://regmedia.co.uk/2016/09/09/wavenet.pdf [https://perma.cc/APA7-KZBE].

[51] Devin Coldewey, *Google's WaveNet Uses Neural Nets to Generate Eerily Convincing Speech and Music,* TECHCRUNCH (Sept. 2016), https://techcrunch.com/2016/09/09/googles-wavenet-uses-neural-nets-to-generate-eerily-convincing-speech-and-music/ [https://perma.cc/8LAY-MLK7].

[52] Lily Hay Newman, *Hackers Trick Facial-Recognition Logins with Photos from Facebook (What Else?)*, WIRED (Aug. 19, 2016), https://www.wired.com/2016/08/hackers-trick-facial-recognition-logins-photos-facebook-thanks-zuck/[https://perma.cc/ES8Y-9EDV] (citing Yi Xu, True Price, Jan Michael Frahm, and Fabian Monrose, *Virtual U: Defeating Face Liveness Detection by Building Virtual Models from your Public Photos* (2016), https://www.usenix.org/system/files/conference/usenixsecurity16/sec16_paper_xu.pdf [https://perma.cc/7VQA-6QYH]).

These advances have been combined to create realistic video forgeries. Researchers at Washington University used footage and corresponding audio of President Obama to synthesize high-quality video of him speaking things he never actually said with realistic lip and head movements.[53] Researchers from the University of Erlangen-Nuremberg, the Max-Planck Institute for Informatics, and Stanford University improved on these methods to create a program that allows an individual to "control" the expressions of the target actor being mimicked (the researchers used footage of a variety of politicians/actors) with realistic facial transfer, in real time, and with smooth transition between expressions.[54]

In an information environment in which the authenticity of a video or audio "recording" cannot be verified, the prospects for manipulating public perceptions are concerning. In response to such concerns, some researchers in this field—aware of these dangers—are trying to find ways to mark such objects as inauthentic. For example, Zeyu Jin, one of the Voco developers at Adobe, indicated that they are also researching watermarking techniques to provide such an indication, noting that "As we're getting the results much better, making it so people can't distinguish between the fake and the real one, we're working harder trying to make it detectable."[55] Balakrishnan et al have shown that it is possible to detect a human

---

[53] Supasorn Suwajanakorn, Steven Seitz, & Ira Kemelmacher-Schilzerman, *Synthesizing Obama: Learning Lip Sync from Audio*, 36 ACM TRANS. GRAPH 95:1, 95:3 (July 2017) http://grail.cs.washington.edu/projects/AudioToObama/siggraph17_obama.pdf [https://perma.cc/297F-EEEE]; An independently produced deepfake video of President Obama can be viewed online at James Vincent, *Watch Jordan Peele Use AI to Make Barrack Obama Deliver a PSA About Fake News*, (Apr. 7, 2018), https://www.theverge.com/tldr/2018/4/17/17247334/ai-fake-news-video-barack-obama-jordan-peele-buzzfeed [https://perma.cc/89UY-GFFB].

[54] Justus Thies et al, *Face2Face: Real-time Face Capture and Reenactment of RGB Videos*, UNIVERSITY OF ERLANGEN-NUREMBERG 1, 1-2 (2016) http://www.graphics.stanford.edu/~niessner/papers/2016/1facetoface/thies2016face.pdf [https://perma.cc/S662-UQ3E].

[55] Matthew Gault, *After 20 Minutes of Listening, New Adobe Tool Can Make You Say Anything*, MOTHERBOARD (Nov. 5, 2016), https://motherboard.vice.com/en_us/article/jpgkxp/after-20-minutes-of-listening-new-adobe-tool-can-make-you-say-anything [https://perma.cc/SA5A-TVYM].

pulse from a video clip of a real person,[56] and in some faked video, a human pulse will not be present.

So the arms race between creators and detectors of fake videos will continue—the next iteration of technologies to create fake video clips of humans may simulate pulses in its images. But the fundamental dynamic is likely to be one of reaction—creators of fakes will have the advantage over detectors of fakes for some period of time, during which users of fakes will have the advantage.

Perhaps a larger point is that an indicator or warning that a clip is fake may not actually be useful. For example, in early March 2017, Facebook began to display a tag on news items identified by a substantial number of users as "fake"; the tag indicated that the item contained disputed content.[57] In late March 2017, the Guardian reported on many complaints about the tag from parties that forwarded a particular news item about the repeatedly debunked Irish slave trade.[58] In November 2017, *Fortune* reported that a number of third-party fact checkers for Facebook were concerned that their work was doing little to curb fake news on the platform.[59] A 2017 report from Stanford found that about 70 percent of Facebook users were unaware of Facebook's new tool for reporting false news, and 90 percent had not used the tool,[60] even though the tool had been available and publicized to some extent for several months. If these reports are true, they suggest that for some substantial fraction of

---

[56] Guha Balakrishnan, Fredo Durand, & John Guttag, *Detecting Pulse from Head Motions in Video,* IEEE COMPUTER SOCIETY, 3430, 3436 (2013), https://ieeexplore.ieee.org/document/6619284/ [https://perma.cc/6VUB-HWR].

[57] Hudson Hongo, *Facebook Finally Rolls Out 'Disputed News' Tag Everyone Will* Dispute, GIZMODO (March 3, 2017), https://gizmodo.com/facebook-finally-rolls-out-disputed-news-tag-everyone-w-1792959827 [https://perma.cc/LY64-GR88].

[58] Elle Hunt, *'Disputed by Multiple Fact-checkers': Facebook rolls out new alert to combat fake* news, THE GUARDIAN (Mar. 21, 2017, 8:37 PM), https://www.theguardian.com/technology/2017/mar/22/facebook-fact-checking-tool-fake-news [http://perma.cc/4JHV-5XVC].

[59] Tom Huddleston Jr., *Facebook's Fact-Checkers Complain That 'Fake Information Is Still Going* Viral', FORTUNE (Nov. 14, 2017), http://fortune.com/2017/11/14/facebook-fact-checking-fake-news/ [http://perma.cc/77LU-VR9B].

[60] Russell Feingold et al., *Fake News and Misinformation: The Roles of the Nation's Digital Newsstands, Facebook, Google, Twitter, and Reddit*, STANFORD LAW SCHOOL LAW & POLICY LAB 45 (2017), https://law.stanford.edu/publications/fake-news-and-misinformation-the-roles-of-the-nations-digital-newsstands-facebook-google-twitter-and-reddit/ [https://perma.cc/2UTY-J2D6].

viewers, it simply does not matter if the content of the news posting is disputed.

Falsified video and audio present an even harder problem to solve. Textual inputs are processed in the first instance by System 2, which is itself oriented towards the symbolic and logical. Video and audio inputs are processed by System 1—and are hence even more likely to stimulate strong emotion regardless of whether warnings about authenticity are present. Indeed, it is well known that exposure to time-ordered sequences of images and sounds can provoke strong emotional reactions in certain people—otherwise known as moviegoers.

Filmmaker Alfred Hitchcock is quoted as saying to scriptwriter Ernest Lehman that:

> [T]he audience is like a giant organ that you and I are playing. At one moment we play this note on them and get this reaction, and then we play that chord and they react that way. And someday we won't even have to make a movie – there'll be electrodes planted in their brains, as we'll just press different buttons and they'll go 'oooh' and 'aaah' and we'll frighten them and make them laugh. Won't that be wonderful?[61]

One could not ask for a better description of the filmmaker's intent.

Neurological evidence supports the claim that some movies are quite capable of evoking strong emotional reactions in many people.[62]

---

[61] PAUL ELLIOTT, HITCHCOCK AND THE CINEMA OF SENSATIONS: EMBODIED FILM THEORY AND CINEMATIC RECEPTION 99 (2011).

[62] Specifically, inter-subject correlation (ISC) analysis depends on the use of functional magnetic resonance imaging (fMRI) to identify regions of the brain that are activated over the time period during which a subject views a film, thus yielding a specific sequence of brain regions "lighting up" as a function of time that is personal to the particular subject involved. A second subject viewing the same film will have another sequence that is personal to the second subject, and so on. When the sequences for different individuals are similar (i.e., highly correlated), the film is said to have high ISC because the film evokes activity in mostly the same areas of the brain in different individuals. Films with low ISC evoke idiosyncratic responses that vary significantly with the individual. It is an empirical result that some motion pictures have high ISC and others have low ISC (a canonical example might be a video taken of a street corner over a long period of time with no changes in perspective or magnification). In other words, films with high ISC can reliably evoke particular sequences of brain response. Activity in certain areas of the brain is known to correlate with various kinds of brain function, including different emotions, and thus it is reasonable to suppose that when the appropriate brain regions light up, the

A viewer knows he or she is watching a film with paid actors following a script written by human beings that generally includes many things that did not happen in reality, and still the viewer cries at various poignant moments during the film's showing. Another example is a well done horror film—no amount of prior intellectual or cognitive knowledge about the nature of the film will eliminate the emotional power of the horror scenes.

Today, filmmakers have a wide variety of tools at their disposal to practice their craft, including compelling screenplays, powerful music, appropriate lighting and scene editing, close-ups, and so on, but their cinematic choices are made intuitively. Neurocinematics offers the possibility that decisions made to induce specific emotions in the viewer could be made on a much more reliable and repeatable basis—quite a boon for future IW/IO operators. Coupling neurocinematically informed filmmaking with falsified video and audio footage suggests that future deep-fake videos will make today's propaganda seem quite amateurish by comparison.

IV. ORGANIZING THE U.S. GOVERNMENT TO DEAL WITH INFORMATION WARFARE AND INFLUENCE OPERATIONS

The preceding Section III is profoundly important in understanding how the U.S. government is (or as will be seen, is not) organized to defend against cyber-enabled information warfare and influence operations. In particular, the concerns raised in Section III all relate to different kinds of speech, a term that is quite broad in the context of U.S. law, the Constitution, and the structure of U.S. governmental institutions.

A. *On the First Amendment—Some Constitutional Constraints on Government Action*

Under current First Amendment jurisprudence and decades of precedent,[63] it is virtually certain that any government regulation

viewer's emotions are being engaged. For more discussion on ISC, *see* Uri Hasson *et al.*, *Neurocinematics: The Neuroscience of Film*, 2.1 PROJECTIONS 1 (2008), http://www.cns.nyu.edu/~nava/MyPubs/Hasson-etal_NeuroCinematics2008.pdf [https://perma.cc/8GAK-4MVK].

[63] *See* United States v. Alvarez, 567 U.S. 709, 719 (2012) ("the Court has never endorsed the categorical rule . . . that false statements receive no First Amendment protection"); Meese v. Keene, 481 U.S. 465, 466, 480-83 (1987) (the Court is critical of a "paternalistic

directed at intentionally false, misleading, or polarizing speech would have to be drafted quite narrowly and with exceptional precision to avoid running afoul of the First Amendment. The Supreme Court will uphold content-based speech restrictions only if narrowly tailored to combat what the Court deems to be a compelling government interest. The relevant legal hurdles are likely all the more insuperable because much of the communication that forms the basis of cyber-enabled information warfare and influence operations is political speech--a form of expression that elicits the Supreme Court's greatest solicitude.

Given that the concerns raised in Section III relate to different kinds of speech, they necessarily implicate the U.S. Constitution and especially the First Amendment, which places strong restrictions on the authority of government to restrict the content of speech. Any content-based government restrictions on speech are subject to a standard of strict scrutiny and are allowable only in support of compelling governmental interests and then only with the narrowest means possible so that only "bad" speech is restricted and "bad" is narrowly defined. Furthermore, a long history of Supreme Court decisions has held that political speech is among the most protected of all categories of speech.

One metaphor frequently used to describe the operation of the First Amendment is the marketplace of ideas. This metaphor posits that the value of a specific idea is determined in competition with other ideas rather than by the judgment of an external authority (such as government), and the judgments that people make in weighing these various ideas against each other determine which ones survive. Truth emerges through public debate and discourse of ideas, uninhibited by governmental interference.

The "marketplace of ideas" metaphor, however, is potentially misleading in today's information environment and the presence of cyber-enabled IW/IO.[64] In the marketplace of ideas, good ideas push out bad ideas. The philosophy underlying the First Amendment was

---

assumption that the public will misunderstand" the use of the term "political propaganda" and therefore will "misuse [that] information").

[64] Tim Wu has also explored this question, arguing that "it is no longer speech itself that is scarce, but the attention of listeners," an assertion that, if true, undercuts the basis on which the First Amendment was originally written and adopted. *See* Tim Wu, *Is the First Amendment Obsolete?*, KNIGHT FIRST AMENDMENT INSTITUTE, COLUMBIA UNIVERSITY, (Sept. 2017), https://knightcolumbia.org/content/tim-wu-first-amendment-obsolete [https://perma.cc/34LK-8TXE].

developed by John Stuart Mill[65] at a time in human history when information available to the public was sparser by many orders of magnitude than it is today. The metaphor also implicitly assumes that information consumers have access to all of the ideas and information that must be compared, although it stretches the imagination to believe that is true in today's marketplace of ideas.

But — continuing the metaphor — markets sometimes experience market failure for various reasons, at which point governments often step in to remediate those failures. Furthermore, the discussion in Section III suggests that the metaphor does not apply in today's information environment and in the presence of cyber-enabled IW/IO.[66] Thus, the important question that arises is this: to the extent that there is market failure today in the marketplace of ideas, how should the U.S. government respond?

A fundamental question of today is whether the cyber-enabled proliferation of false, misleading, and inauthentic statements designed to manipulate and distort the political process is so pervasive and so destructive that the nation should consider ways to prohibit such speech—while at the same time minimizing the dangers of either government abuse or undue restrictions on the marketplace of ideas. Even more problematic from a First Amendment standpoint are statements that are literally true but nevertheless misleading.[67]

And what of divisive ideas and opinions? To the extent that the political ideas and thoughts spread through cyber-enabled IW/IO are regarded as speech (and how could they not be?), any governmental restraints on that speech would be even more inherently suspect.

The First Amendment has also been used to ensure the rights of Americans to receive information from a diversity of sources, and in

---

[65] JOHN STUART MILL, ON LIBERTY 86 (David Bromwich & George Kateb, Vail-Ballou Press 2003) (1859).

[66] For more on this issue, *see* Wu, *supra*, note 65 (arguing that "it is no longer speech itself that is scarce, but the attention of listeners," an assertion that, if true, undercuts the basis on which the First Amendment was originally written and adopted).

[67] The following old story illustrates that sometimes the best way to lie is to tell the truth. A merchant ship docks in a new harbor. On the first night, the first mate goes ashore and returns drunk. The next morning, the captain enters into the ship's log: "The first mate returned drunk last night." The first mate pleads with the captain: "Captain, please don't let that stay in the log. This could keep me from getting a promotion." The captain says: "It is true that you returned drunk last night, and if it is true it has to go in the log. That's the rule." The next night, the captain goes ashore and returns sober. The first mate enters into the log: "The captain returned sober last night."

particular from foreign sources. For example, in considering the Postal Service and Federal Employees Salary Act of 1962 (which required the Postmaster General to collect and deliver unsealed communist propaganda only upon the recipient's request), the U.S. Supreme Court held unanimously that "[t]he regime of this Act is at war with the 'uninhibited, robust, and wide-open' debate and discussion that are contemplated by the First Amendment."[68] Of particular note is the concurring opinion of Justice Brennan in this case in which he writes that, "[T]he dissemination of ideas can accomplish nothing if otherwise willing addressees are not free to receive and consider them. It would be a barren marketplace of ideas that had only sellers and no buyers."[69] The U.S. Supreme Court has also held (again, unanimously) that, "[T]he Constitution protects the right to receive information and ideas, regardless of their social worth, and to be generally free from governmental intrusions into one's privacy and control of one's thoughts."[70]

In light of these precedents, it is interesting to contemplate its applicability to U.S. government efforts to suppress foreign actors from introducing information in American public discourse. For example, if a substantial number of American citizens want to receive ads and videos from Russian troll farms, could the U.S. government constitutionally take action to against those troll farms to prevent them from sending such material into the United States? Even today, Defense Department planners are required to take extra care in operations that might result in misinforming the American public.

The discussion of Sections I-III strongly suggests that cyber-enabled IW/IO, as it has been practiced recently against the United States, is specifically intended to cause market failure in the U.S. marketplace of ideas. At the same time, the discussion of this section (Section IV-A) makes it clear that the First Amendment places significant limitations on direct U.S. government action to impede the flow of information from practitioners of cyber-enabled IW/IO to the United States.

Therefore, for the sake of analysis, this paper hypothesizes that there exist some indirect and thus constitutionally permissible

---

[68] Lamont v. Postmaster Gen. of U.S., 381 U.S. 301, 307 (1965) (quoting in part N.Y. Times Co. v. Sullivan, 376 U.S. 254, 270 (1964)).

[69] *Id.* at 308 (Brennan, J., concurring).

[70] Stanley v. Georgia, 394 U.S. 557, 557 (1969).

strategies for combating IW/IO--strategies focusing, for example, on preventing unlawful foreign intervention in U.S. elections or in equipping U.S. audiences to be more cognizant of IW strategies and resistant to their influence. Assuming such strategies exist, it remains to be considered whether government has the expertise, knowledge, technical capabilities, and resources to act effectively and wisely in designing and implementing those strategies.

B. *U.S. Government Departments and Agencies with Some Possible Role in Addressing Adversary Information Warfare and Influence Operations*

Given a host of other precedents regarding government regulation on the content of political speech, it is highly unlikely (arguably near-impossible) that any governmental restrictions on the content of political speech would stand up to scrutiny. Nevertheless, for the sake of argument, imagine that constitutional objections could be addressed successfully. In this hypothetical world, the government would be free to act—but would it have the expertise, knowledge, technical capabilities, and resources to act effectively and wisely?

The U.S. Government consists of fifteen departments (i.e., the executive departments of the executive branch) and a large number of agencies not affiliated with any department, each of which has different authorities for action and different expertise to support the exercise of those authorities.[71] What follows below is a listing of U.S.

---

[71] The names and missions of U.S. government executive branch departments can be found at USA.gov; as of this writing, fifteen departments are listed. *Executive Departments*, USA.GOV, (last visited Nov. 16, 2018) https://www.usa.gov/executive-departments [https://perma.cc/S4CT-QC3S]. As for U.S. government agencies not affiliated with any department, the term "independent agency" is not sufficiently well-defined for analytical purposes. The Administrative Conference of the United States notes that there is no widely accepted definition of that term, noting that some scholars use the term to mean "any agency created outside the EOP [Executive Office of the President] or executive departments," while other scholars use the term to denote agencies whose leaders can only be removed "for cause," "inefficiency, neglect of duty, or malfeasance in office," or similar language. DAVID E. LEWIS & JENNIFER L. SELIN, ADMIN. CONFERENCE OF THE U.S., SOURCEBOOK OF UNITED STATES EXECUTIVE AGENCIES 48-49 (1st ed. 2012), https://www.acus.gov/sites/default/files/documents/Sourcebook%202012%20FINAL_May%202013.pdf [https://perma.cc/HKE8-2K9S]. As the ACUS notes, "independence in this context means independence from political interference, particularly removal by the President." *Id.* This paper has used an operational definition of the universe of agencies to be considered—the entities listed in the 2012 ACUS report as "independent agencies" as well as those listed on USA.gov as "independent agencies." *Id.* at 52-54, 56, *Independent Agencies*, USA.GOV, (last visited Nov. 16, 2018) https://www.usa.gov/independent-agencies [https://perma.cc/8AVC-HPZK].

government departments and agencies whose mission and roles, in this author's assessment, have some possible relevance to addressing information warfare and/or influence operations conducted against the United States. (*Italicized material below refers to the part of the department or agency's authorities/mission/expertise that may be relevant*.)

- The Department of Defense. The Department of Defense has a well-articulated doctrine and framework for psychological operations—*how to use psychological operations against adversaries and how to respond to psychological operations conducted by adversaries*.[72] (The Department of Defense has flipped repeatedly between "psychological operations" and "military information support operations" as the appropriate title for activities covered under this rubric.)
- The Department of Education. Under the rubric of the Department of Education's mission to promote student achievement and preparation for global competitiveness by fostering educational excellence, *the Department of Education has from time to time supported efforts to promote critical thinking in schools*.[73]
- The Department of Justice. The Department of Justice prosecutes criminal activity. In February 2018, the Department of Justice indicted 13 Russian nationals and three Russian companies in connection with alleged interference with the 2016 campaign.[74] Specifically, *the indictment charged the defendants with one count of conspiracy "to defraud the United States by impairing, obstructing, and defeating the lawful functions of the Federal Election Commission, the U.S. Department of Justice, and the U.S. Department of State in administering federal requirements for disclosure of foreign*

---

[72] Joint Chiefs of Staff, *Joint Publication 3-13: Psychological Operations*, FED'N OF AM. SCIENTISTS (2010) https://fas.org/irp/doddir/dod/jp3-13-2.pdf [https://perma.cc/RRY9-S5B7].

[73] *See* P. Karen Murphy *et al.*, *Quality Talk: Developing Students' Discourse to Promote Critical-Analytic Thinking, Epistemic Cognition, and High-Level Comprehension,* INST. OF EDUC. SCI. (2013).

[74] Indictment ¶¶ 2-3, United States v. Internet Research Agency, No. 1:18-cr-00032-DLF (D.D.C. Feb. 26, 2018) https://www.justice.gov/file/1035477/download [https://perma.cc/Q7Y8-28D2].

involvement in certain domestic activities" and one count of conspiracy to commit wire fraud and bank fraud by violating 18 USC Sections 1343 and 1344.[75]

- The Department of State. Within the Department of State, the Under Secretary for Public Diplomacy and Public Affairs has the mission of supporting the achievement of U.S. foreign policy goals and objectives, advancing national interests, and enhancing national security by informing and influencing foreign publics and by expanding and strengthening the relationship between the people and Government of the United States and citizens of the rest of the world. The Under Secretary for Public Diplomacy and Public Affairs oversees the Bureau of Public Affairs(PA), the Bureau of International Information Programs (IIP), and the Global Engagement Center (GEC),[76] each of which with some expertise in some aspect of information warfare or influence operations.
    - The IIP supports people-to-people conversations with foreign publics on U.S. policy priorities, *developing multimedia communications products for both traditional communications and new media channels* and managing an overseas network of bricks-and-mortar American Spaces.[77]
    - PA engages in *strategic and tactical communications planning to advance America's foreign policy interests, uses social media and other modern technologies to engage the public*, and oversees the State Department's six *international Regional Media Hubs, which are overseas platforms for engagement of foreign audiences via the internet and broadcast and print media*.[78]
    - The GEC's role is to *"lead, synchronize, and coordinate efforts of the Federal Government to recognize, understand, expose, and counter foreign state and non-*

---

[75] *Id.*

[76] *Under Secretary for Pub. Dipl. and Pub. Aff.*, STATE.GOV, (last visited Oct. 4, 2018), https://www.state.gov/r/index.htm [https://perma.cc/C5R8-J3U3].

[77] *Bureau of Int'l Info. Programs*, STATE.GOV. (last visited Oct. 4, 2018), https://www.state.gov/r/iip/ [https://perma.cc/MC8L-AGHG].

[78] *Bureau of Pub. Aff.*, STATE.GOV. (last visited Oct. 4, 2018), https://www.state.gov/r/pa/ [https://perma.cc/JT3G-BFLC].

> *state propaganda and disinformation efforts aimed at undermining United States national security interests*."[79] In this role, it seeks to increase the reach and effectiveness of U.S. government communications, to identify efficiencies and opportunities in the messaging and partnership space, to drive a wedge between audiences that are most vulnerable to harmful propaganda and hostile nations, groups, and terrorists seeking to influence them, and to inject factual content about terrorist organizations into the information space to counter recruitment and radicalization to violence.

- The Broadcasting Board of Governors (BBG). The BBG's mission is *to inform, engage, and connect people around the world in support of freedom and democracy*.[80] The BBG oversees a number of international broadcast networks, including Voice of America; Radio Free Europe / Radio Liberty; Office of Cuba Broadcasting (including Radio and Television Martí and martinoticias.com); Radio Free Asia; and Middle East Broadcasting Networks (including Alhurra Television, Radio Sawa and MBN Digital). These networks strive to provide programming that provides accurate, objective, and comprehensive news, especially in regions in which freedom of the press is limited, nonexistent, or not fully established.
- The Central Intelligence Agency (CIA). In 1976, the Senate Select Committee to Study Governmental Operations With Respect To Intelligence Activities reported that "The CIA currently maintains *a network of several hundred foreign individuals around the world who provide intelligence for the CIA and at times attempt to influence opinion through the use of covert propaganda*. These individuals provide the CIA with direct access to a large number of newspapers and periodicals, scores of press services and news agencies, radio and television stations, commercial book publishers, and other foreign media outlets."[81] If similar activities continue today, they are likely

---

[79] *Global Engagement Center*, STATE.GOV (last visited Oct. 3, 2018), https://www.state.gov/r/gec/index.htm [https://perma.cc/PXK4-T2JE].

[80] *Who We Are: Mission*, BBG.GOV. (last visited October 3, 2018), https://www.bbg.gov/who-we-are/mission/ [https://perma.cc/SHJ5-PCEH].

[81] S. REP. NO. 94-755, at 455 (1976).

performed under authorities granted to the President under 50 USC § 3093 (Presidential approval and reporting of covert actions).

- The Federal Communications Commission (FCC): The role of the FCC is to promote connectivity and ensure a robust and competitive market in communications services such as cable, radio, television, satellite and wire. The FCC is not permitted to promulgate regulations that infringe upon constitutionally protected free speech, even if such speech may be offensive to some parts of the public. On the other hand, *when certain kinds of speech are not fully protected (e.g., when speech can constitutionally be restricted or banned, as in the cases of indecent/profane or obscene material respectively), the FCC can and does enforce regulations to implement such restrictions or prohibitions.* [82]
- The Federal Election Commission (FEC). The FEC enforces federal campaign finance laws, which covers public disclosure of funds raised and spent to influence federal elections and restrictions on contributions and expenditures made to influence federal elections.[83] *For example, 52 USC § 30121 makes it illegal for a foreign national, directly or indirectly, to make a contribution or donation of money or other thing of value in connection with a Federal election.*
- The Federal Trade Commission (FTC). The FTC works *to prevent fraudulent, deceptive, and unfair business practices, and provide information to help consumers spot, stop, and avoid scams and fraud.*[84]
- The Agency for International Development (USAID). USAID *promotes and demonstrates democratic values abroad*, and advances a free, peaceful, and prosperous world by providing international development and disaster assistance through partnerships and investments that save lives, reduce poverty,

---

[82] *The FCC and Freedom of Speech*, FCC.GOV. (last visited Oct. 3, 2018), https://www.fcc.gov/consumers/guides/fcc-and-freedom-speech [https://perma.cc/8XSN-LH58].

[83] *Mission and History*, FEC.GOV. (last visited Oct. 4, 2018), https://www.fec.gov/about/mission-and-history/ [https://perma.cc/68YS-JFYU] .

[84] *Federal Trade Commission*, USA.GOV, (last visited Oct. 4, 2018), https://www.usa.gov/federal-agencies/federal-trade-commission [https://perma.cc/G8L7-LCWJ].

strengthen democratic governance, and help people emerge from humanitarian crises and progress beyond assistance.

- The Election Assistance Commission (EAC).[85] The Help America Vote Act of 2002 requires states to implement procedures for provisional voting, for providing voting information, for updating and upgrading voting equipment, implementing and maintaining statewide voter registration databases, for implementing voter identification procedures, and for managing procedures for administrative complaint. The EAC assists states in meeting these requirements, and under this rubric, it *maintains guidelines for electronic voting systems, operates the federal government's voting system certification program,* and administers a national clearinghouse on elections that includes shared practices, information for voters and other resources to improve elections.
- The National Science Foundation (NSF).[86] NSF is a federal agency created "to promote the progress of science; to advance the national health, prosperity, and welfare; *to secure the national defense…*" Through grants and contracts, NSF supports basic research in all fields of fundamental science and engineering, except for medical sciences.[87]
- The National Endowment for the Humanities (NEH).[88] NEH promotes excellence in the humanities and *conveying the lessons of history to all Americans by awarding grants in the humanities*, which include, but are not limited to, the study and interpretation of "language, both modern and classical; linguistics; literature; history; jurisprudence; philosophy; archaeology; comparative religion; ethics; the history, criticism and theory of the arts; those aspects of social sciences which have humanistic content and employ humanistic methods; and the study and application of the humanities to the human

---

[85] *Help America Vote Act*, U.S. ELECTION ASSISTANCE COMM'N. (last visited Oct. 4, 2018), https://www.eac.gov/about/help-america-vote-act [https://perma.cc/99PM-Y728].

[86] *About the National Science Foundation*, NSF.GOV. (last visited Oct. 4, 2018), https://www.nsf.gov/about [https://perma.cc/L4JU-Z9Y6].

[87] *Id.*

[88] *About the National Endowment for the Humanities*, NEH.GOV. (last visited Jan. 23, 2019), https://www.neh.gov/about [http://perma.cc/76VF-27TK].

environment with particular attention to reflecting our diverse heritage, traditions, and history and to the relevance of the humanities to the current conditions of national life."

- The Institute of Museum and Library Services (IMLS).[89] The IMLS mission supports America's museums, libraries, and related organizations through grantmaking, research, and policy development; these activities *promote literacy* and lifelong learning and increase access to information, ideas, and networks through libraries and museums.

C. *The Bad Fit of U.S. Government Authorities for Addressing Adversary Information Warfare and Influence Operations*

The brief survey of Executive Branch departments and agencies suggests that a variety of U.S. government entities have some expertise that could be relevant to some aspects of the cyber-enabled information warfare/influence operations problem. But, in most cases, the fit between the italicized authorities/mission/expertise and the cyber-enabled IW/IO conducted by adversaries in the United States is not good.

- The entity within the Department of Defense responsible for homeland defense is the U.S. Northern Command (USNORTHCOM), which provides command and control for Department of Defense homeland defense efforts and coordinates defense support of civil authorities. According to USNORTHCOM's web page,[90] USNORTHCOM is responsible for aerospace warning, aerospace control, and maritime warning for the continental United States (and Alaska and Canada as well). Its civil support mission includes domestic disaster relief operations that occur during fires, hurricanes, floods and earthquakes, as well as counter-drug operations and managing the consequences of a terrorist event using weapons of mass destruction. Note the absence of any mention of combatting adversary propaganda—USNORTHCOM's military mission is to protect the homeland against physical

---

[89] *Mission*, IMLS.GOV. (last visited Jan. 23, 2019), https://www.imls.gov/about-us [http://perma.cc/8H8L-E3YQ].

[90] *About US Northern Command*, NORTHCOM.MIL. (last visited Jan. 23, 2019), http://www.northcom.mil/About-USNORTHCOM/ [http://perma.cc/DN2B-JVHR].

attack, and its civil support mission is limited to responding to domestic disasters. More generally, 18 U.S.C. 1385 (also known as the Posse Comitatus Act) restricts the circumstances under which the Department of Defense can take action and the activities it can conduct within the United States.[91]

- Although the Department of Education has supported efforts to promote critical thinking in schools, education in the United States is primarily a state and local responsibility. The federal government is not responsible for developing the required curricula or determining requirements for enrollment and graduation. Thus, to the extent that instilling critical thinking habits enable citizens to better identify disinformation and fake news more effectively,[92] imparting those skills broadly to citizens in the course of their formal educational programs will not be a federal responsibility. Also, calls for the improvement of critical thinking in citizens have been common for at least a half-century,[93] and the same laments about the lack of critical thinking are seen today—a reality suggesting that the promotion of critical thinking skills in the population is at best a problem solved over a time scale measured in decades if not centuries.
- The Justice Department indictments of February 2018 focused on conspiracy related to the nondisclosure of foreign involvement in certain domestic activities regarding U.S.

---

[91] For the view of the Department of Defense on the restrictions imposed by the Posse Comitatus Act, *see* U.S. DEP'T OF DEFENSE, DOD MANUAL 3025.01, VOL. 3, DEFENSE SUPPORT OF CIVIL AUTHORITIES: PRE-PLANNED DOD SUPPORT OF LAW ENFORCEMENT AGENCIES, SPECIAL EVENTS, COMMUNITY ENGAGEMENT, AND OTHER NON-DOD ENTITIES (2016), http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/302501_vol03.pdf [https://perma.cc/P92H-M3HB]. According to this document, the DOD can provide support to civilian law enforcement agencies, to the U.S. Secret Service, and for counter-drug operations, and nothing in principle would rule out the DOD from cooperating with civilian agencies, at their request, when the latter would find it useful to apply DOD knowledge and expertise on psychological operations and how they might be countered.

[92] *See*, International Baccalaureate, *In a Fake News Climate, Critical Thinking Skills Are More Crucial Than Ever*, THE CHRONICLE OF HIGHER EDUCATION (2017), https://www.chronicle.com/paid-article/in-a-fake-news-climate-critic/36 [https://perma.cc/DX62-BL8Y].

[93] Raymond B. Fox, *Difficulties in Developing Skill in Critical Thinking*, 55 J. EDUC. RES. 335, 335 (1962).

elections in 2016.[94] But under U.S. law, individuals, corporations, and unions are allowed to spend unlimited amounts of money on political messaging, as long as they operate independently of specific political campaigns.[95] Thus, it appears that if the activities alleged in the Justice Department indictment had been undertaken by U.S. citizens properly registered as agents of foreign principals—and funded through mechanisms allowed by U.S. law—no U.S. laws would have been violated.

- The State Department's activities to advance U.S. foreign policy interests through people-to-people interactions and various strategic and tactical communications activities target foreign audiences and are not a defense against cyber-enabled IW/IO carried out against U.S. citizens.[96] The activities of the GEC have only recently turned to disinformation efforts conducted by nation-states, and most of these activities focus on audiences outside the United States, relying on "fact-based narratives and analyses to counter adversarial foreign propaganda and disinformation directed at the United States

---

[94] Indictment, *supra* note 74, at ¶¶ 3-5.

[95] On individuals, see Buckley v. Valeo, 424 U.S. 1, 58-59 (1976) ("The First Amendment requires the invalidation of the Act's independent expenditure ceiling, its limitation on a candidate's expenditures from his own personal funds, and its ceilings on over-all campaign expenditures, since those provisions place substantial and direct restrictions on the ability of candidates, citizens, and associations to engage in protected political expression, restrictions that the First Amendment cannot tolerate."). The Act to which *Buckley* refers is the Federal Election Campaign Act of 1971, as amended in 1974, which limited expenditures by individuals or groups "relative to a clearly identified candidate" to $1,000 per candidate per election. Federal Election Campaign Act Amendments of 1974, Pub. L. No. 93-443, §101 (codified as amended at 2 U.S.C. § 431). On corporations, *see* Citizens United v. Federal Election Commission, 558 U.S. 310, 356 (2010) ("[W]ealthy individuals and unincorporated associations can spend unlimited amounts on independent expenditures. Yet certain disfavored associations of citizens—those that have taken on the corporate form—are penalized for engaging in the same political speech. . . When Government seeks to use its full power, including the criminal law, to command where a person may get his or her information or what distrusted source he or she may not hear, it uses censorship to control thought. This is unlawful. The First Amendment confirms the freedom to think for ourselves.").

[96] I note without further comment that as positive and enlightened as these Department activities are from a U.S. perspective, one has to wonder how the governments of those audiences targeted by these activities feel about such communications.

and United States allies and partner nations."[97] However, one important focus of GEC activities calls for proposals to "identify, catalogue and, where feasible, quantify current and emerging trends in adversarial foreign propaganda and disinformation in order to coordinate and shape the development of tactics, techniques, and procedures to expose and refute foreign disinformation."[98] This focus is directly on point but assumes the consumers of foreign disinformation actually care about being properly informed.

- As with the State Department, the Broadcasting Board of Governors operates outside U.S. territory. Its programming activities do not focus on U.S. citizens and cannot be a defense against cyber-enabled IW/IO carried out against U.S. citizens.
- The CIA has substantial expertise in propaganda and psychological operations, and could provide advice to other U.S. government agencies, but it is not permitted to conduct operations in the United States. Moreover, according to 50 U.S.C 3093, covert action undertaken by the U.S. government must not involve any action that would violate the U.S. Constitution.[99] Additionally, it appears that Russian efforts to interfere with the U.S. political system, including the 2016 election, started as early as 2014.[100] If true, this suggests a possible intelligence failure—that the CIA, and the U.S. intelligence community more broadly, either did not know about the election threat the Russians posed for two years, or it did know and failed to disseminate information about that threat throughout the U.S. government.
- The ability of the FCC to restrict certain kinds of speech is limited today to "broadcast media." The Communications Act of 1934 establishes the FCC's authority to manage the use of

---

[97] BUREAU OF PUB. AFFAIRS, U.S. DEP'T OF STATE, *Request for Statements of Interest and Capacity (SOIC) Countering State-Sponsored Propaganda and Disinformation*, GRANT.GOV (Mar. 9, 2018), https://www.grants.gov/web/grants/view-opportunity.html?oppId=301460 [https://perma.cc/KMD7-NKV8].

[98] *Id.*

[99] 50 U.S.C. § 3093 (2015). In practice, this requirement shapes the scope and nature of U.S. propaganda because of concerns that such propaganda might reach and thus improperly influence U.S. persons.

[100] Indictment, *supra* note 74, at ¶ 3.

the relevant portion of the electromagnetic spectrum, which broadcast media—by definition—uses. But the FCC lacks authority to interfere with speech—constitutionally protected or not—in any other kind of media and, in particular, on the Internet. As noted above, political speech receives the highest levels of constitutional protection.

- Federal campaign finance laws, enforced by the FEC, are for the most part intended to increase the transparency of political advertising. For example, on March 26, 2018, the FEC issued a notice of proposed rule-making that would require political advertising on internet-enabled devices and applications to disclose the sources that funded such advertising.[101] The notice also noted the opinion of the U.S. Supreme Court in *Citizens United* that "identification of the source of advertising may be required as a means of disclosure, so that the people will be able to evaluate the arguments to which they are being subjected."[102] However, the proposed rule rests on several assumptions: that issue advertising (i.e., advertising that is not explicitly tied to a specific political campaign or party) is comparatively less important than political advertising, that citizens actually do care about who is funding a political advertisement, and that the identity disclosure requirements cannot easily be circumvented.
- The FTC's authority to prevent fraudulent, deceptive, and unfair business practices, and to provide information to help consumers spot, stop, and avoid scams and fraud have been limited to transactions in which consumers exchange money with a real or alleged goods or service provider. This almost certainly does not extend to election practices in which citizens do not lose money.
- USAID only acts abroad, and thus has no authority or responsibility for domestic action.
- The Election Assistance Commission provides assistance to states for election administration—an activity that includes

---

[101] Internet Communication Disclaimers and Definition of "Public Communication", 83 Fed. Reg. 12864 (proposed Mar. 26, 2018) (to be codified at 11 C.F.R. pt. 100-110) (proposing a disclaimer regarding the identity of the payor or sponsor of "public communications on the internet that contain express advocacy, solicit contributions, or are made by political committees," colloquially referred to as "political advertising").

[102] Citizens United v. Federal Election Com'n, 588 U.S. 310, 368 (2010).

building and securing HAVA-mandated state voter registration databases and certifying the security of computer-based electronic voting machines. But, as noted in Section II, cybersecurity threats (such as these) are distinct from cyber-enabled IW/IO threats.

- The National Science Foundation, the National Endowment for the Humanities, and the Institute of Museum and Library Services carry out their missions primarily through grant-making activities. They do not have significant operational responsibilities regardless of the expertise that any of their staff may have as a result of those activities.

More broadly, this brief survey of departmental and agency authorities also suggests two high-level observations. First, the legal authorities of U.S. governmental departments and agencies have yet to catch up to the problem of cyber-enabled IW/IO conducted against the United States. Indeed, U.S. governmental authorities that may be useful, continue to be premised on the existence of a marketplace of ideas that works well to inform a public that routinely and systematically engages in critical thinking and reflection on political matters. Even in an Internet-enabled information environment manipulated by sophisticated nation-state adversaries.

Second and perhaps more importantly, given the diffuse nature of the cyber-enabled IW/IO problem, it is not clear at all how the U.S. government could draw a "bubble chart"—that is, a chart depicting the organizational units sharing a common objective—with unambiguous lines of responsibility and authority. Who or what existing entity could be put "in charge" or respond to cyber-enabled IW/IO? If, as seems likely, no existing entity could do the job, what charge should be given to a new entity to address the problem?

To appreciate the complexity of the problem posed by cyber-enabled IW/IO, it is helpful to consider two other examples. One example is provided in Figure 1, which presents what is colloquially known in the U.S. government as the cybersecurity "bubble chart." It is intended to describe where within the U.S. government responsibility lies for different aspects of cybersecurity. Officials from the Obama Administration say that the chart was revised between 50 and 100 times before a consensus on its content was achieved.

The key feature of the cyber bubble chart is the spaces between the three bubbles, which refer to the Departments of Defense, Homeland Security, and Justice (FBI). With anything more than one bubble, there are necessarily gray areas in between them. These gray areas

show that some responsibilities are unclear and that information flow will be impeded in possible operational scenarios. Put differently, the bubble chart clearly shows three distinct bubbles, with zero overlap between them. A footnote to the bubble chart explains why: "Nothing in this chart alters existing DHS, DOJ, and DOD roles, responsibilities, or authorities." Also, deliberations over the bubble chart for cybersecurity were conducted in the context of an accepted U.S. government definition of cybersecurity articulated in NSPD-54.

If it was difficult to reach consensus on an area as well specified as cybersecurity, imagine the difficulties in determining responsibilities for a threat as diffuse such as that posed by information warfare and influence operations.

A second example is from the early 1950's, when the U.S. government became aware of a national security threat through electromagnetic warfare which was "the contest through preclusive use, jamming, interference and related measures for the control of all or parts of the radio spectrum or the denial of its use by others" and having a "direct bearing on diplomacy, limited or total military operations, economic warfare, psychological warfare and telecommunications policy.[103] According to an archive-based study by Jonathan Winkler,[104] "Attempts to address these problems [i.e., the problems posed by electromagnetic warfare] required a level of interaction between the military, diplomatic, and intelligence communities for which they were not prepared and that only the NSC could oversee. Even then, the matter was so complex that even the senior officials themselves acknowledged that it required presidential intervention and the emplacement of a technical advisor at the president's side."[105]

---

[103] Briefing Notes, "Soviet Capability for Waging Electromagnetic Warfare," February 11, 1953, CIA-RDP80R01443R000100220012-5, CIA CREST database (hereafter CIA CREST), National Archives and Records Administration (hereafter USNA); Appendix 2, NSC 137, cited in Appendix II, Jackson Report (Report of President's Committee on International Information Activities), June 30, 1953, Special Collection, "Intelligence, Policy and Politics: The DCI, the White House, and Congress," doc. 5166d49399326091c6a60500, CIA FOIA Electronic Reading Room, 111-13.

[104] Jonathan Winkler, The Forgotten Menace of Electro-Magnetic Warfare in the Early Cold War, 42(2) DIPLOMATIC HISTORY 254, 254-280 (2018), https://academic.oup.com/dh/article-abstract/42/2/254/3896229 [https://perma.cc/M3GH-8D63].

[105] *Id.* at 278.

Although the Eisenhower administration was able to address the problem in the short run by building additional communications facilities for the Department of Defense, "the complex interconnected issues identified at the time by the participants about synthesizing federal defense requirements with civilian capabilities, making more efficient use of the radio spectrum, and balancing the desire for efficiency against the traditions of antimonopoly and plurality proved insurmountable."[106] Moreover, "It was not possible to agree on whether there should be someone in the cabinet who would handle the problem of electromagnetic warfare and who that person should be. . . . Neither the Truman nor Eisenhower administrations could figure out how best to balance these weights in the absence of clear authority for dealing with the dual-use technology in war, peace, or somewhere in between such as the Cold War."[107]

Winkler further writes that "in 1953, NSC officials lamented that 'the relative importance of this whole field of activity' was not clear. They were unsure 'whether a new agency is required, a new PSB-type Board, a new bureau in an old-line department like Commerce, or a staff in the Executive Office of the President. The Bureau [of the Budget] apparently needs guidance as to whether it might be raising a technical function too high, or not raising an extremely important function high enough.'"[108]

To this author, the organizational parallels between the U.S. government trying to respond to the threat of electromagnetic warfare and trying to respond to cyber-enabled IW/IO are striking.

V. CONCLUSION

In 1927, Justice Louis Brandeis' concurring opinion in *Whitney v. California* stated that: [109]

> [N]o danger flowing from speech can be deemed clear and present, unless the incidence of the evil apprehended is so imminent that it may befall before

---

[106] *Id.*

[107] *Id.* at 279.

[108] *Id.*

[109] Whitney v. California, 274 U.S. 357 (1927).

> there is opportunity for full discussion. 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.

This extended passage is often summarized as "the cure for bad speech is more speech." But, the information environment has changed greatly since 1927. Justice Brandeis' conclusion relies on citizens having the "opportunity for full discussion" and time to "avert the evil by the processes of education."[110] Given the vastly increased volume and velocity of information today, and cyber-enabled information warfare and influence operations exploiting these characteristics of the environment, both opportunity and time are in short supply.

As argued above, the likelihood of governmental action against the cyber-enabled proliferation of false, misleading, or inauthentic statements designed to manipulate and distort the political process is exceedingly low under current interpretations of the First Amendment. But, constitutional interpretations sometimes slowly change in response to changes in circumstance and environment. This author will not go further than to make two points. First, the advent of cyber-enabled speech of various kinds poses a significant and qualitatively different environment that may warrant such change in the future. Second, the wisdom of allowing government agencies to make decisions about what counts as "a false, misleading, or inauthentic statement designed to manipulate and distort the political process" can legitimately be questioned.

It is clearly good that some degree of public attention has been focused on the problems posed by cyber-enabled IW/IO conducted against the United States. But, as serious as foreign election interference is to the nation's future, the real threat to the republic is the tribal and toxic nature of current political discourse. Such tensions have been rising for some time, and yet their enormous amplification through cyber-enabled IW/IO has been shocking to many observers. Moreover, current U.S. law does not forbid any of the activities that may be characterized as cyber-enabled IW/IO. In fact, First Amendment jurisprudence protects many of these activities explicitly.

---

[110] *Id.* at 377.

Given the limitations on the governmental action described above, action to ameliorate the problem by the private sector is a possible alternative. Indeed, the private sector in the United States owns and operates technological infrastructure that provides the cyber-enabling part of cyber-enabled IW/IO. And the First Amendment does not place constraints on private sector action—a point misunderstood by many citizens.

This paper does not address possible private sector actions, except to make the following point: the First Amendment would severely limit the influence that the U.S. government could exercise with respect to entities in the private sector. That is, government law, regulation, or policy to influence private sector actions would also be subject to court challenge if those actions impeded the free expression of ideas and opinions. However, if private sector entities were willing to take such actions on their own (e.g., because they decided to do so as part of a different business model, as a matter of corporate ethics, or as a part of incentives that the U.S. government might offer), they would be entirely free to do so.[111]

In this new environment, perhaps a new social contract is needed between citizens and government regarding the extent and nature of the rights afforded by the First Amendment—which was adopted more than two centuries before the invention of the World Wide Web. Perhaps the private sector will find business models that enable them to profit from more civil and reasoned discourse. Perhaps researchers will find effective ways to depolarize political dialogue. These elements may—or may not—have a place in a serious strategy for how to deal with the problems posed by cyber-enabled IW/IO. Whatever that strategy entails, the design of such a strategy is a necessary prerequisite for any serious discussion of how the U.S. government should be structured to address these problems.

It may be possible to find a national consensus about awareness of the dangers posed by cyber-enabled information warfare and influence operations—obviously a necessary first step. But even with good leadership addressing the issue—focused on the problem, consistent in its approach (whatever it may be), and committed to the idea of reality-based policy discourse—organizing the various assets of the U.S. government and the private sector—a whole-of-nation

---

[111] *Facebook Suspends U.S. Conspiracy Theorist Alex Jones*, REUTERS (July 27, 2018), https://www.reuters.com/article/us-facebook-infowars/facebook-suspends-u-s-conspiracy-theorist-alex-jones-idUSKBN1KH2PN [https://perma.cc/V4WH-E9A8].

response rather than a whole-of-government response—to handle such a diverse threat would be a difficult if not daunting task. If national leaders deny the existence of the problem—or benefit from it—making meaningful progress will be much, much more difficult.

I have argued that the information marketplace metaphor fails in the information environment, and specifically in the face of a foreign cyber-enabled information IW/IO threat that further undermines the operation of that market. Thus, we will need to examine what kind of coordinated national response is possible that would not threaten the values that underlie the First Amendment. We have our work cut out for us.

Table 1. System 1 and System 2 thinking, compared

System 1	System 2
Unconscious Reasoning	Conscious Reasoning
Implicit	Explicit
Automatic	Controlled
Low Effort	High Effort
Large Capacity	Small Capacity
Rapid	Slow
Default Process	Inhibitory
Associative	Rule-Based
Contextualized	Abstract
Domain Specific	Domain General
Evolutionarily Old	Evolutionarily Recent
Nonverbal	Linked to language
Includes recognition, perception, orientation	Includes rule following, comparisons, weighing of options
Modular Cognition	Fluid Intelligence
Independent of working memory	Limited by working memory capacity
Non-Logical	Logical
Parallel	Serial

Source: DANIEL KAHNEMAN, THINKING, FAST AND SLOW (New York: Farrar, Straus & Giroux, 1st ed. 2011).

Figure 1. Bubble Chart for U.S. Government Cybersecurity Roles and Responsibilities