THE NEW FIGHTING WORDS?: HOW U.S. LAW HAMPERS THE FIGHT AGAINST INFORMATION WARFARE

Jill Goldenziel, Associate Professor of International Law and International Relations, Marine Corps University-Command and Staff College
Manal Cheema, J.D. Candidate, University of Virginia Law School

ABSTRACT:

The United States prides itself on freedom of speech and information. However, enemy states have weaponized these prized freedoms against the United States. The First Amendment, the Privacy Act, and other U.S. laws designed to protect Americans' civil liberties paradoxically constrain the U.S.'s ability to combat information warfare by its enemies. This Article argues that the United States must reform laws and doctrine protecting freedom of speech, information, and privacy in order to protect the U.S. democratic process and national security. By exploring the example of the Russian threat to the U.S. electoral process, which is the most widely-known example of information warfare against the United States, this Article will illustrate how enemy states wield the United States' own laws against it. It will also explain how justifiable concerns with infringement on civil liberties have hampered the United States' response. The Article concludes by making recommendations on how future legislation and policies should balance First Amendment and privacy rights with national security interests.

EXECUTIVE SUMMARY:

The First Amendment has become a weapon of war. The United States prides itself on freedom of speech and information. However, Russia has weaponized these prized freedoms against us. Russia has unleashed a sophisticated and ongoing information warfare campaign against the integrity of the U.S. electoral process. Before the 2016 presidential election, Russia used online sources disguised as news outlets to produce and distribute fake news, targeting voters in swing states. Russia is already trying to influence the 2020 Presidential election. According to the U.S. Department of Justice ("DOJ"), foreign-influenced operations like the one Russia is currently waging against the United States include covert actions are intended to "sow division in our society, undermine confidence in democratic institutions, and otherwise affect political sentiment and public discourse to achieve strategic geopolitical objectives."[1]

The 2017 U.S. National Security Strategy repeatedly notes that the U.S. response to enemy information warfare has been "tepid and fragmented." One reason is that U.S. laws and jurisprudence protecting free speech and privacy were not designed for the technological realities of today. The United States' own laws tie its hands in its fight against information warfare. For this reason, the Department of Defense ("DOD") identified developing, updating, and deconflicting laws regulating information operations as a top priority in its 2016 Strategy for Operations in the Information Environment.[2]

An example from 2016 acutely illustrates how U.S. laws constrain its fight against information warfare. In 2016, the State Department ("DOS") proposed to identify social media influencers who were spreading Kremlin messages and target them with counterarguments.[3] However, the Privacy Act of 1974 restricts the collection of data related to the ways Americans exercise their First Amendment rights. The program could not guarantee that it would not inadvertently collect American citizens' data as part of the effort, and it did not fall under the Act's law enforcement exceptions. State Department lawyers quashed the program, reasoning that tweets, retweets, and comments implicate the collection of data related to the ways Americans exercise their First Amendment rights. Ironically, according to State Department lawyers, the First Amendment prohibited a program that would encourage free political debate by adding political speech to the marketplace of ideas. By this interpretation, the First Amendment could not be used to defend itself.

This Article argues that the United States must reform laws, doctrine, and policies to protect national security and the democratic process. It explains how laws such as the First Amendment and Privacy Act pose substantial obstacles to fighting the 2016 Russian disinformation campaign and information warfare more broadly. It then proposes reforms of law and policy to improve national security while ensuring protection for American civil liberties.

In sum, the article argues that:

---

[1] U.S. Dep't of Just., REPORT OF THE ATTORNEY GENERAL'S CYBER DIGITAL TASK FORCE 1 (July 2, 2018) [hereinafter Cyber Digital Task Force Report].

[2] Dep't of Def., STRATEGY FOR OPERATIONS IN THE INFORMATION ENVIRONMENT 13 (June 2016), https://dod.defense.gov/Portals/1/Documents/pubs/DoD-Strategy-for-Operations-in-the-IE-Signed-20160613.pdf.

[3] Adam Entous, Ellen Nakashima, & Greg Jaffe, *Kremlin Trolls Burned Across the Internet as Washington Debated Options*, WASH. POST (Dec. 25, 2017), https://www.washingtonpost.com/world/national-security/kremlin-trolls-burned-across-the-internet-as-washington-debated-options/2017/12/23/e7b9dc92-e403-11e7-ab50-621fe0588340_story.html.

- First Amendment doctrine, the Privacy Act, and related laws constrain the United States' ability to fight information warfare.
- The Supreme Court's interpretation of the First Amendment is inadequate for the realities of political discourse on the Internet and social media.
    - Supreme Court doctrine mistakenly equates social media and the Internet with the public square, ignoring the distinct characteristics of social media that distort free speech and allow foreign adversaries to exploit the U.S.'s free information environment.
    - Supreme Court doctrine is premised on the idea of counterspeech, that true speech should be used to counter false speech, which will compete in a free marketplace of ideas until truth prevails. Significant evidence calls the effectiveness of counterspeech into doubt, particularly in the social media context.
    - Supreme Court jurisprudence mistakenly treats social media like traditional media.
    - First Amendment doctrine protects false speech, likely including enemy disinformation.
    - Most enemy information warfare and propaganda efforts would not qualify as incitement under Supreme Court precedent.
- The Privacy Act and other Cold War-era surveillance laws do not allow collection of data relating to U.S. persons' First Amendment activities. These acts include an exception for law enforcement but not national security, impeding a whole-of-government approach to combatting information warfare.
- Potential remedies to these problems include:
    - Reforming Supreme Court doctrine to treat online platforms and social media companies as distinct entities based on their unique functions.
    - Reforming Supreme Court doctrine to recognize that preserving the integrity of the electoral process is a national security interest and First Amendment right that should be balanced with other civil liberties concerns.
    - Enacting laws that allow prosecution of people who make reckless false speech with the intent to distort the results of the electoral process or suppress the vote.
    - Reforming surveillance laws to allow for a narrowly tailored national security exception with appropriate safeguards for civil liberties.
    - Investing in research to determine the conditions under which counterspeech is likely to be effective and developing programs accordingly.
    - Regulating online platforms and social media outlets in accordance with Constitutional principles
    - Asking online platforms and social media outlets to self-regulate to eliminate disinformation campaigns.
    - Registering and regulating bots.
    - Regulating online paid political ads.
    - Aggressively enforcing the Foreign Agent Registration Act to better monitor foreign actors seeking to intervene in the electoral process.

This Article will discuss how the United States can combat information warfare through a whole-of-government approach, with a primary focus on civilian government agencies. A thorough discussion of U.S. military operations involving information warfare involves additional legal authorities, including classified information, and lies beyond the scope of this paper.

However, the framework in this Article will have utility for fighting information warfare in military operations, since information operations and surveillance activities by the military must also comply with Constitutional principles. In engaging with social media, all government agencies would employ the very tools that allow free access to information to combat misinformation and propaganda campaigns. Military operations must conform to the Constitution and many other applicable laws and policies of the United States. Even though military operations are within the purview of the Executive Branch, their constitutional validity may rest on Congressional approval or limitations. The court of public opinion, which is increasingly important in military operations, is also concerned with constitutional liberties. Furthermore, military cyber operations may produce collateral effects that may affect U.S. nationals and may involve the functioning of online platforms, especially if they are subject to a cyber intrusion. Perhaps most importantly, military operations increasingly rely on a whole-of-government approach, in which the military works closely with other government agencies to coordinate a unified fight against an enemy. Thus, the analysis above will be useful to DOD in planning future military efforts to fight information warfare. To achieve mission success, all national security actors must learn to move quickly—and legally—on the new social media battleground.

Misinformation threatens the existence of a well-informed public, and therefore, democracy itself. As Justice Robert Jackson aptly noted, the Constitution should not be a suicide pact. Likewise, the United States should not fall on the First Amendment's double-edged sword. The time has come for the U.S. to reform its laws to better fight foreign information operations while protecting civil liberties and the electoral process. Nothing less than the meaning of the First Amendment, American civil liberties, and the foundations of American democracy are at stake.