THE INFLUENCE OF WAR; THE WAR FOR INFLUENCE

*Duncan Hollis**

ABSTRACT

As part of a symposium on Rosa Brooks's *How Everything Became War and the Military Became Everything*, this essay explores the concept of an influence operation (IO) from the perspective of international law. It examines common elements of an IO and proffers five criteria for differentiating among them, namely by assessing their (i) transparency; (ii) extent of deception; (iii) purpose; (iv) scale; and (v) effects. Using these criteria, I analyze whether and how international law might constrain the conduct of IOs, with particular attention to the duty of non-intervention, sovereignty, and self-determination. I find that, aside from a few cases like IOs that incentivize genocide, the cognitive quality of IOs raises serious questions about the capacity of international law to govern this rapidly developing problem set. Furthermore, I highlight how the difficulty international lawyers face in regulating IOs is equally apparent in assigning responsive authority to militaries or technologists. I conclude with a call for further study of state-sponsored IOs and the potential of hybrid and pluralist responses to regulate this increasingly visible component of international relations.

TABLE OF CONTENTS

I. INTRODUCTION 31
II. DEFINING INFLUENCE OPERATIONS 35
III. DIFFERENTIATING AMONG INFLUENCE OPERATIONS 36
IV. INTERNATIONAL LAW AND INFLUENCE OPERATIONS 39
V. CONCLUSION: WHO SHOULD TAKE RESPONSIBILITY FOR IOS? 43

I. INTRODUCTION

In 1968, my father was a dentist working in rural Vietnam with a physician, a jeep, and a driver. His job? For seven months, he and his colleagues would drive to a different village each morning, set up a tent at the end of town, and offer the villagers free medical and dental care. But, this was not some purely humanitarian mission. My father was a Lieutenant in the U.S. Navy and his work was part of a much larger influence operation—to win the "hearts and minds" of the Vietnamese population to support the United States and its interests in that country. Those efforts, of course, were ultimately unsuccessful.

My father's story came to mind repeatedly as I read Professor Rosa Brooks's *How Everything Became War and the Military Became Everything*.[1] Among its

This essay was first prepared for a book roundtable co-hosted by the Institute for International Law and Public Policy at Temple University Beasley School of Law and the National Constitution

many virtues, Brooks's work reveals just how far the U.S. military has redefined its function beyond Samuel Huntington's famous admonition—"to kill people in the most efficient way possible."[2] From her own work on strategic communications to the military's obsession with counterinsurgency (COIN) and the *Counterinsurgency Field Manual*,[3] Brooks recounts the expansion of the U.S. military's mission from killing to influence. She cites John Nagl and the focus of his "COINdinistas" on legitimacy and political outcomes, explaining how "a thousand COIN-related flowers bloomed" with the U.S. military digging wells, refurbishing schools, and microfinancing projects for rural women.[4] Under the banner of "strategic communication[s]," Brooks highlights her own learning curve with a military incorporating information in its warfare—from anti-extremist slogans on soccer balls, to radio stations with "alternative views," to a "[Department of Defense]-funded 'peace concert.'"[5] Brooks tells us: "You name it, the military was doing it."[6]

For the most part, Brooks appears sympathetic to the military taking on information-related functions in a world where "everything communicates something" and where "[t]anks and fighter jets can't stop disaffected teenagers in Birmingham or Paris or Detroit from being inspired by al Qaeda or ISIS . . . ."[7] She highlights General Stanley McChrystal's call to recognize war as "a struggle for the support of the population," with a mission defined as overcoming "the enemy's influence."[8]

Brooks does acknowledge the military's decidedly "mixed track record" in executing these manifold programs, worrying that "our best instincts . . . lead to our worst failures."[9] Still, her criticisms in the information space are primarily characterized as internal problems. Brooks frames the issue as one where the influence of war has taken previously civilian functions—like public diplomacy—and put them in military hands, which, over time, became the "only game in town."[10] As such, Brooks's concerns with COIN, U.S. strategic communications,

Center on September 15, 2017. The essays from this roundtable have been published as a symposium collection within issue 32.1 of the Temple International & Comparative Law Journal.

* Professor of Law and Associate Dean for Academic Affairs, Temple University Beasley School of Law; Non-Resident Scholar, the Carnegie Endowment for International Peace.

1. ROSA BROOKS, HOW EVERYTHING BECAME WAR AND THE MILITARY BECAME EVERYTHING: TALES FROM THE PENTAGON (2016).

2. *See* Samuel P. Huntington, *New Contingencies, Old Roles*, JOINT FORCES Q. 38, 43 (Autumn 1993).

3. BROOKS, *supra* note 1, at 83; *see generally* DEP'T OF ARMY, FM3-24, COUNTERINSURGENCY (2006).

4. BROOKS, *supra* note 1, at 94.

5. *Id.* at 89.

6. *Id.* at 95.

7. *Id.* at 88, 329.

8. *Id.* at 94 (citing Int'l Sec. Assistance Force, *Tactical Directive* (July 6, 2009)).

9. *Id.* at 96–97.

10. BROOKS, *supra* note 1, at 316.

and other forms of information warfare are decidedly different than the external threats that she associates with U.S. humanitarian interventions and targeted killings. In those cases, she emphasizes how U.S. operations—and the legal justifications offered for them—risk setting precedents that other leaders, such as Russian President Putin, can deploy from interventions in Ukraine to targeted killings in London restaurants.[11]

Hindsight suggests, however, that Brooks should have done more to explore the risk of precedent-setting in the information space. The 2016 presidential election demonstrates that influence is a two-way street, with operations capable of affecting the U.S. population as much as—if not more than—those that the U.S. military employs to influence foreign populations. Just as we ask if U.S. uses of lethal force set operational and legal precedents for other states, can the same be said for U.S. influence operations? Did U.S. information operations create space for Russia to interfere in our own election process?

Putin coyly denies such involvement. But reports from the media and the U.S. intelligence community are confident that Russia—and more specifically Russia's military agency, the GRU—interfered in the U.S. election process.[12] Russia may not have successfully hacked the voting machines themselves.[13] It did, however, deploy a wide-ranging and multi-faceted operation, including hacking the Democratic National Committee servers, obtaining the e-mails of senior Democratic officials like John Podesta, and releasing the data obtained in strategically-timed tranches via WikiLeaks and DC Leaks.[14] It also pushed disinformation and "fake news" on social media sites like Facebook and Twitter.[15] Russia's goals in doing this included (i) undermining public faith in U.S. democratic electoral processes, (ii) denigrating Secretary Clinton, and (iii) supporting President Trump's candidacy.[16] Whether these efforts affected the

11. *See id.* at 244, 273. Such problems have persisted—if not increased—since Brooks first published her book. *E.g.*, Ellen Barry and Richard Pérez-Peña, *Britain Blames Moscow for Poisoning of Former Russian Spy*, N.Y. TIMES (March 12, 2018).

12. *See, e.g.*, Greg Miller and Adam Entous, *Declassified report says Putin 'ordered' effort to undermine faith in U.S. election and help Trump*, WASH. POST (Jan. 6, 2017), https://www.washingtonpost.com/world/national-security/intelligence-chiefs-expected-in-new-york-to-brief-trump-on-russian-hacking/2017/01/06/5f591416-d41a-11e6-9cb0-54ab630851e8_story.html.

13. Pam Fessler, *10 Months after Election Day, Feds Tell States More about Russian Hacking*, NPR (Sept. 27, 2017), https://www.npr.org/2017/09/22/552956517/ten-months-after-election-day-feds-tell-states-more-about-russian-hacking.

14. Raphael Satter, *Inside story: How Russians hacked the Democrats' emails*, A.P. (Nov. 4, 2017), https://www.apnews.com/dea73efc01594839957c3c9a6c962b8a.

15. *E.g.*, *id.*; Scott Shane, *The Fake Americans Russia Created to Influence the Election*, N.Y. TIMES (Sept. 7, 2017), https://www.nytimes.com/2017/09/07/us/politics/russia-facebook-twitter-election.html.

16. *E.g.*, Adam Entous et al., *Secret CIA Assessment Says Russia Was Trying to Help Trump Win White House*, WASH. POST (Dec. 9, 2016), https://www.washingtonpost.com/world/national-security/obama-orders-review-of-russian-hacking-during-presidential-campaign/2016/12/09/31d6b300-be2a-11e6-94ac-

election's outcome is hotly debated, with insufficient empirical evidence to conclusively decide the matter.

Secrecy, moreover, stymies any rigorous effort to tie Russian acts to earlier U.S. precedents. Without knowing the full scope and extent of U.S. information operations (military or otherwise), it becomes hard to make the case for correlation, let alone causation. Indeed, it is possible that Russia, China, and others are pursuing information operations because of U.S. military dominance in the kinetic space, rather than any precedents the United States may offer in the information arena.[17] Russia, moreover, is also likely drawing on the precedents of its predecessor; the Soviet Union had a long history of developing and deploying influence operations of its own.[18]

Still, Brooks's challenge to interrogate the "space between" war and peace offers an alternative lens for exploring influence operations, not just as an internal, civilian-military issue, but as a rising national security threat.[19] My two stories about influence operations (IOs) have plenty of space between them: (i) a classic "military" IO conducted in wartime that is (happily for my father and me) legally uncontroversial; and (ii) an IO involving two nations nominally at peace, which has generated a rash of claims that the activities did (or should) violate international law. Looking at that space between allows us to explore modern IOs along at least three dimensions.

- First, what links IOs like those in my father's story to the 2016 election? What are the common criteria of an influence operation? How do we define this concept?
- Second, what is the reason for the different reactions to these two IOs? Why does the more modern variant generate more discomfort and concern?
- Third, where does international law enter the equation? Does the law as it exists today prohibit or otherwise regulate IOs, and on what grounds does it do so?

Taken together, these inquiries lead me to conclude with a final question about the way forward. Which actors—international lawyers, military tacticians, technologists—are best suited to respond to the threat of IOs and what tools should they use to do so? Time and space constraints obviously preclude a full review of these topics. Still, I offer some preliminary reactions to lay the groundwork for

3d324840106c_story.html.

17. As Brooks notes, Valery Gerasimov, Russia's Deputy Defense Minister and Chief of the General Staff of Armed Forces, wrote in 2013 that Russian military tactics were shifting to where "[l]ong-distance, contactless actions against the enemy [were] becoming the main means of achieving combat and operational goals." BROOKS, *supra* note 1, at 333; *see also* Molly K. McKew, *The Gerasimov Doctrine: It's Russia's new chaos theory of political warfare. And it's probably being used on you,* POLITICO MAGAZINE (September/October 2017).

18. FREDERICK CHARLES BARGHOOM, SOVIET FOREIGN PROPAGANDA (1964, republished Princeton Univ. Press, 2015).

19. *See* BROOKS, *supra* note 1, at 353.

further research and discourse.

II. DEFINING INFLUENCE OPERATIONS

To begin, what is an influence operation? A 2009 RAND study offers a broad definition:

> Influence operations are the coordinated, integrated, and synchronized application of national diplomatic, informational, military, economic, and other capabilities in peacetime, crisis, conflict, and postconflict to foster attitudes, behaviors, or decisions by foreign target audiences that further U.S. interests and objectives.[20]

From this definition, we can identify IOs by three shared elements. First, all IOs involve the deployment of some resources, be they material (like dentists and doctors), economic (like sanctions or aid packages), or informational (like e-mails or social media postings).

Second, IOs deploy resources for cognitive effects. And this is important. As Herbert Lin and Jackie Kerr explain, influence operations operate across three dimensions:[21]

- a physical dimension comprised of people, places and things;
- an informational or virtual dimension, where data is collected, processed, stored, and disseminated; and
- a cognitive or emotional dimension that reflects the minds and emotions of those who transmit, receive and respond to the physical acts and information encountered in the other two dimensions.

Ultimately, IOs aim to operate on—and produce consequences in—the cognitive dimension. At first glance, therefore, IOs aspire to target an entirely different level than kinetic military operations (which target the physical dimension) and cyber operations (which target the confidentiality, integrity, and availability of data and information networks). On closer analysis, however, it is worth recalling Clausewitz's idea that "war is merely the continuation of policy [and political intercourse] by other means."[22] IOs may be crafted to target one or both of the other dimensions with an expectation of knock-on effects in the cognitive space. Kinetic operations can thus qualify as IOs if they seek to generate not just physical effects but cognitive ones; the same is true for cyber operations.

The third criteria for an IO is that the resources are deployed for cognitive purposes to impact a targeted audience—a state's leadership, opinion-leaders, or

20. ERIC V. LARSON ET AL., RAND CORP., FOUNDATIONS OF EFFECTIVE INFLUENCE OPERATIONS: A FRAMEWORK FOR ENHANCING ARMY CAPABILITIES 2 (2009), https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG654.pdf.

21. Herbert Lin & Jackie Kerr, *On Cyber-Enabled Information/Influence Warfare and Manipulation*, *in* THE OXFORD HANDBOOK OF CYBERSECURITY 1, 5 (forthcoming 2018).

22. CARL VON CLAUSEWITZ, ON WAR 87 (Michael Howard & Peter Paret eds. & trans., 1976).

mass publics—to change or reinforce attitudes and behaviors in ways that align with the IO authors' interests. Thus, a successful IO will lead its targeted audience to adopt the goals that the IO author wishes them to adopt openly and willingly. As Lin and Kerr note, IOs are not about coercing targets into capitulation or wearing them down, but rather convincing them to adopt—seemingly on their own—some attitude, view, or behavior that the IO's authors favor.[23] Thus, an effective IO avoids even the appearance of conflict between actor and audience.

III. DIFFERENTIATING AMONG INFLUENCE OPERATIONS

With this definition of IOs in mind—a deployment of resources for cognitive ends that foster or change a targeted audience's behavior—we can turn to the second question: What is the problem with IOs? After all, so many of our daily interactions qualify as IOs. Our families and friends regularly deploy resources to get us to adopt or change our views, social norms, or political beliefs. Companies expend significant resources on marketing to convince us to buy their products and services. And states deploy diplomacy, speeches, and other forms of strategic communication to affect the behavior of adversaries and allies. As Sun Tzu long ago noted, even militaries prioritize IOs over conflict; he suggested that the most effective warfighting "is to subdue the enemy's army without fighting at all."[24] Simply put, IOs are a regular—if often unacknowledged—feature of human relations.

And yet, clearly, *some* IOs pose serious problems. A few are already undoubtedly illegal. Recall the Radio Télévision des Mille Collines (RTLM) radio broadcasts in Rwanda that encouraged racial violence including the famous broadcast message: "You have missed some of the enemies. You must go back there and finish them off. The graves are not yet full!"[25] The International Criminal Tribunal for Rwanda ended up convicting three of RTLM's executives for genocide, incitement to commit genocide, conspiracy to commit genocide, and crimes against humanity.[26]

Where do we draw the line between genocidal IOs and those that are normal parts of human interaction? I propose five candidates for discriminating among IOs: (i) transparency, (ii) deception, (iii) purpose, (iv) scale, and (v) effects. For starters, there is a *transparency* question. Some IOs are like my father's mission—so called "white" operations where the State is open and transparent about its authorship or responsibility for the resources deployed.[27] "Gray" operations, in contrast, are ambiguous in their origins; there may be no attribution or the IO may appear to originate from a private source (under the theory that audiences may be

23. Lin & Kerr, *supra* note 21, at 5.

24. SUN TZU, THE ART OF WARFARE 79 (Roger T. Ames trans., 1993).

25. BILL BERKELEY, THE GRAVES ARE NOT YET FULL: RACE, TRIBE AND POWER IN THE HEART OF AFRICA 20 (2001).

26. *See* Prosecutor v. Nahimana, Case No. ICTR-99-52-T, Judgment and Sentence, ¶¶ 1092–94 (Dec. 3, 2003).

27. Lin & Kerr, *supra* note 21, at 7.

more receptive to an idea if its true source is hidden).[28] Then, there are "black" operations in which the author false flags the IO's source, most often to a hostile adversarial state, group, or individual.[29] The question is whether such differences—alone, or in combination with other factors—should help us delineate acceptable from unacceptable IOs? Might "white" IOs be per se more acceptable than "black" ones?

Beyond transparency, we could differentiate IOs based on the presence of *deception*. IOs can, for example, leak accurate information—WikiLeaks released Podesta's actual e-mails—while other IOs incorporate disinformation or offer "fake news." In 2014, for example, there was an attempt to convince a Louisiana town that it had been the victim of an ISIS bombing by using all sorts of false information—YouTube videos, cloned websites, "eyewitness" Twitter accounts, etc.[30] Brooks explains the history of the now shuttered Office of Strategic Influence by emphasizing the controversy over its reported plans to plant false news stories in foreign press offices.[31] The veracity of the informational resources deployed might thus be another ground for differentiating among IOs.

Third, there is a question of *purpose*: What is the IO trying to do? IOs can be general, specific, or chaotic. Some IO campaigns—like the use of propaganda—target public attitudes and dispositions *generally*; they attempt to shift sentiments rather than particular positions. Other, more precise IOs seek to generate *specific* behavioral outcomes—whether it is genocide, taking to the streets, or casting a particular vote. Finally, some IOs simply sow chaos and confusion under the premise that doing so lowers an adversary's situational awareness and creates uncertainty among the targeted audience.[32] There is, moreover, strong support for the idea that—beyond the promotion of genocide—other IOs may have unacceptable aims, such as those encouraging civil war or civil strife. A purpose-based criterion thus invites questions of what purposes warrant segregation. Is it just IOs that seek violent outcomes? What about those designed to impact elections? What about IOs that target a shift in a specific legislative outcome or foreign policy? In other words, when should we delineate an IO as inappropriate based on what it appears designed to do?

Fourth, there are issues of *scale*. IOs are, like espionage, among the world's oldest professions. There was a time when IOs were relatively costly, requiring substantial resources to generate modest effects. But, the information age has significantly scaled up what can be done. We live in a highly interconnected world. Information, including personal data, is either widely available or insecure enough to be accessible with persistence. IOs can quickly deploy informational resources

28. *Id.*

29. *Id.*

30. *See* Adrian Chen, *The Agency*, N.Y. TIMES (June 2, 2015), https://www.nytimes.com/2015/06/07/magazine/the-agency.html (describing the fake media campaign that convinced townspeople of an attack that never happened).

31. BROOKS, *supra* note 1, at 87.

32. Lin & Kerr, *supra* note 21, at 6.

at low costs, via a range of distribution points, and with the possibility of avoiding established intermediaries like media outlets. Thus, we might ask the sorts of questions that arose with the rise of commercial cyber espionage, inquiring when the systemic impacts of IOs will reach a point such that a previously unregulated phenomenon requires regulation. And, although it took several years of U.S. campaigning, the United States and China did agree in 2015 to forgo cyber espionage for commercial advantages, a commitment that the entire G-20 later endorsed.[33]

Last but not least, there is the possibility of differentiating among IOs based on their actual *effects*. There is something ironic in how the IOs that generate the most concern are those most likely to be effective in their cognitive impacts. Compare, for example, two hypothetical IOs. The first one tries to convince people that Donald Trump is the greatest U.S. President, with little success beyond his political base, while the second hypnotizes a population into voting to re-elect Donald Trump. Which one is a greater national security concern? I believe it would clearly be the latter. Of course, we do not (yet?) live in a world where mass hypnosis is possible. Still, my point is to use these hypotheticals to highlight how the greater the guarantee that an IO will involve a measurable loss of human agency or free will is, then the more problematic the IO becomes.

Today's social sciences offer us a range of cognitive and emotional biases that can be leveraged to influence individuals, leaders, groups, and networks. We all, for example, have a confirmation bias where we seek and interpret information in ways consistent with our attitudes and decisions, steering away from inconsistent information.[34] Or, consider the loss-aversion bias, through which people are more likely to be reckless in recouping losses than in seeking gains.[35] Thus, if we believe conditions are bad or deteriorating, we can be primed to act more recklessly.[36]

Of course, this science is not perfect; some long-touted experiments have

33. *See Fact Sheet: President Xi Jinping's State Visit to the United States*, WHITE HOUSE OFF. OF THE PRESS SEC'Y (Sept. 25, 2015), https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states (President Obama and President Xi announced a "common understanding" where both governments agreed that neither "will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing commercial advantages to companies or commercial sectors."); G20 Antalya Summit 2015, Antalya, Turk., Nov. 15–16, 2015, *G-20 Leaders' Communiqué* 26 (2015) ("[N]o country should conduct or support ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors.").

34. *See generally* Kate Sweeny et al, *Information Avoidance: Who, What, When, and Why*, 14 REV. OF GENERAL PSYCHOLOGY 340 (2010); Raymond S. Nickerson, *Confirmation Bias: A Ubiquitous Phenomenon in Many Guises*, 2 REV. OF GENERAL PSYCHOLOGY 175 (1998).

35. *See generally* Daniel Kahneman, Jack L. Knetsch, and Richard H. Thaler, *Anomalies: The Endowment Effect, Loss Aversion, and Status Quo Bias*, 5 J. OF ECON. PERSPECTIVES 193 (1991).

36. *See generally id.*; Daniel Kahneman & Amos Tversky, *Prospect Theory: An Analysis of Decision under Risk*, 47 ECONOMETRICA 263 (1979).

proven hard to replicate, while other established measures will not work on any portion of the population that is more resistant to influence.[37] Measuring effectiveness is equally difficult. Absent some futuristic mind control technique, it will be difficult to demonstrate that an IO "caused" any particular outcome even if it is clear that the IO had some visible role in the processes that led up to that outcome.

To be clear, in flagging these IO characteristics of *transparency*, *deception*, *purpose*, *scale*, and *effects*, I am not saying they must be used to delineate among IOs. Nor am I suggesting that they are the only criteria for doing so. My goal is more modest: to illustrate the range of IOs possible today, and to generate a discussion of which variables may isolate those aspects of IOs of greatest concern, especially as a matter of national security.

IV. INTERNATIONAL LAW AND INFLUENCE OPERATIONS

For international lawyers, of course, opinions on IOs may vary by my third framing question: their legality. At present, there is no international law on IOs specifically. Thus, to regulate IOs we are obliged to look to existing international laws and identify ways in which they overlap with, or otherwise analogize to, existing IOs. I have already mentioned how international criminal law may do so, particularly the law on genocide. Similarly, IOs that involve a threat to use force, or even an actual use of force, are likely banned under the *jus ad bellum*, including Article 2(4) of the U.N. Charter.[38]

But what about IOs that do not implicate violence directly? Are there already international legal regimes that carve off and ban certain IOs from those that are regarded as a normal part of international discourse? I am not confident that existing international law does so. Certainly, we can marshal arguments that international law restricts certain non-violent IOs. But for a more firm conclusion, we need to see either more consensus around particular interpretations of the existing law or the development of new law, whether by treaty or customary practice.

The most widely invoked legal principle in the IO context is the duty of non-intervention. It has a long, well-established pedigree, from U.N. General Assembly resolutions like the Declaration on the Principles of International Law concerning

37. *E.g.*, Open Science Collaboration, *Estimating the Reproducibility of Psychological Science*, 349 SCIENCE 943 (28 Aug. 2015); Lin & Kerr, *supra* note 21, at 7–8 ("there will always be people in a target population that are immune to its effects—this is most true in populations that have strong institutions and traditions dedicated to the rule of law and relatively sane trustworthy (i.e., not corrupt) political leaders.").

38. U.N. Charter, art. 2(4) ("All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."). There, are, of course, two exceptions to the prohibition on the use or threat of force: self-defense and activity authorized by the U.N. Security Council under Chapter VII. These exceptions would presumably apply to any covered IOs as well.

Friendly Relations[39] to the ICJ's repeated endorsement in the *Nicaragua* and *Armed Activities* cases.[40] Most recently, Rule 66 of the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (*Tallinn 2.0*) provides that "[a] State may not intervene, including by cyber means, in the internal or external affairs of another State."[41]

The problem lies not in the rule's existence but in its application. Although the prohibition clearly applies to interference with a state's internal or external affairs, the contents of these categories are not well defined. A state's internal affairs implicate the idea of the *domain réservé*. A century ago, there were subjects clearly cabined off from international attention that a state could address as it saw fit. Today, however, both the human rights revolution and globalization have generated international interest in almost every topic. Thus, any *domain réservé* argument is likely to be fairly limited, contested, and dynamic, as the boundaries of what subjects are appropriate for international attention continue to shift.[42]

Nonetheless, the commentary to *Tallinn 2.0* notes agreement among the International Group of Experts who authored it that "the choice of both the political system and its organization" are clearly within a state's *domain réservé*.[43] As such, they are protected from intervention by the rule. But applying the non-intervention doctrine to events like Russia's 2016 IO runs into a separate problem—the absence of coercion. Ever since the *Nicaragua* decision, international lawyers have defined intervention to require coercion; or as the ICJ put it, coercion "defines, and indeed forms the very essence of, prohibited intervention."[44] Thus, acts that do not involve coercion lie outside the reach of the prohibition on intervention.

Defining coercion is difficult. *Tallinn 2.0* takes the view that coercion does not require physical force but involves acts "designed to deprive another State of its freedom of choice, that is, to force that State to act in an involuntary manner or involuntarily refrain from acting in a particular way."[45] Coercion may thus be found in IOs that involve disrupting the physical environment, like the 2015

39. G.A. Res. 2625 (XXV) (Oct. 24, 1970) ("No State or group of States has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any other State.").

40. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J.14 ¶ 205 (June 27); Armed Activities on the Territory of the Congo (Congo v. Uganda), Judgment, 2005 I.C.J. 116 ¶ 164 (Dec. 19).

41. INT'L GRPS. OF EXPERTS AT THE INVITATION OF THE NATO COOP. CYBER DEF. CTR. OF EXCELLENCE, TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 312 (Michael N. Schmitt ed., 2017) [hereinafter TALLINN 2.0].

42. *See, e.g.*, Duncan B. Hollis, *An Inter-Subjective Treaty Power*, 90 NOTRE DAME L. REV. 1415, 1457–62 (2015) (recounting dynamic U.S. experience where previously domestic topics—e.g., human rights and private law—became appropriate subjects for international regulation, while others, like Native American relations, shifted from the international agenda to a domestic one).

43. TALLINN 2.0, *supra* note 411, at 315 (Commentary to Rule 66, ¶ 10).

44. Nicar. v. U.S., 1986 I.C.J. at 107–08, ¶ 205.

45. TALLINN 2.0, *supra* note 41, at 317 (footnote omitted).

BlackEnergy Operation that took down parts of the Ukrainian power grid.[46] Or it could implicate IOs that only disrupt the virtual environment, such as a distributed denial of service attack targeting a state's banks. But the very nature of IOs—the goal of having a target adopt or change certain behaviors *willingly*—implies an absence of coercion, making the prohibition inconsistent with the IO concept's core idea. It would seem, for example, that there was no coercion in the DNC hack that formed part of Russia's 2016 IO; rather, that IO constituted a case of espionage.[47] Perhaps the timed data dumps on WikiLeaks and elsewhere involved coercion, but it is not clear what the threatened consequences were, let alone who its targets were. Russian social media efforts are even harder to label as coercion since, at best, all they did was impact people's opinions, which may or may not have impacted some number of subsequent votes.[48]

Beyond non-intervention, international law might treat IOs as a breach of sovereignty. Here, however, we have an existential debate about the nature of sovereignty. *Tallinn 2.0* treats sovereignty as an enforceable rule that states can violate.[49] Others, including the chief lawyer to U.S. Cyber Command, suggest that it is a fundamental principle that only operates in the background to inform other rules of international law.[50]

46. *See* Andy Greenberg, *How an Entire Nation Became Russia's Test Lab for Cyberwar*, WIRED (June 20, 2017, 6:00 AM), https://www.wired.com/story/russian-hackers-attack-ukraine/ (detailing the evolution of BlackEnergy malware planted by hackers into Ukrainian and American energy firms).

47. International law's relationship to espionage is murky at best, either treating it as an extra-legal phenomenon or excepting it from other international rules even as new calls emerge for its regulation. *E.g.*, Ashley Deeks, *An International Legal Framework for Surveillance*, 55 VA. J. INT'L L. 291 (2015).

48. Beyond coercion lie further complications involving questions of intent and non-state actors. *Tallinn 2.0* suggests that the IO's authors must intend to coerce behavior. TALLINN 2.0, *supra* note 41, at 321. In contrast, Sean Watts suggests an objective standard, where "[i]t is the fact of coercion with respect to an internal or external affair that establishes a prohibited intervention." Sean Watts, *Low-Intensity Cyber Operations and the Principle of Non-Intervention*, in CYBER WAR: LAW AND ETHICS FOR VIRTUAL CONFLICTS 268 (Jens David Ohlin et al. eds., 2015). Beyond intent, there is also a problem with states employing non-state actors for IOs. TIM MAURER, CYBER MERCENARIES: THE STATE, HACKERS, AND POWER (2018). Recall the now-familiar debates over proxy actors and whether attributing responsibility should turn on a state's overall or effective control. *See, e.g.*, Derek Jinks, *State Responsibility for the Acts of Private Armed Groups*, 4 CHICAGO J. INT'L L. 83, 88–9 (2003). When it comes to IOs, however, states may operate strategically to encourage non-state actors to act in ways that fall outside both effective and overall control. As such, international law might not reach such non-state actor behavior. Or, alternatively, it is possible international law could adopt some version of the "unwilling or unable" test encountered in the use-of-force context, especially after 9/11. *See, e.g.*, Elena Chachko & Ashley Deeks, *Who is on Board with "Unwilling or Unable"?* LAWFARE (Oct. 10, 2016, 1:55 PM), https://www.lawfareblog.com/who-board-unwilling-or-unable.

49. TALLINN 2.0, *supra* note 41, at 17 (Rule 4: "A State must not conduct cyber operations that violate the sovereignty of another State.").

50. *See, e.g.*, Gary Corn & Robert Taylor, *Sovereignty in the Age of Cyber*, 111 AJIL UNBOUND 207 (2017); Gary Corn, *Tallinn Manual 2.0 – Advancing the Conversation*, JUST SECURITY (Feb. 15, 2017)), https://www.justsecurity.org/37812/tallinn-manual-2-0-advancing-

Even accepting sovereignty as a rule, there are open questions about what a breach of sovereignty entails. Existing precedents largely center on states engaging in operations with physical effects in the state whose sovereignty is breached (e.g., exercising enforcement jurisdiction by arresting a defendant in another state's territory, or flying an aircraft across another state's territorial border).[51] As such, events like the Shamoon virus, which destroyed much of Saudi Aramco's computer hardware, might, by analogy, constitute a violation of sovereignty.[52]

But there is little precedent for treating the purely cognitive effects to which IOs ultimately aspire as breaching sovereignty. *Tallinn 2.0* assesses sovereignty violations based on the degree of infringement upon the target state's territorial integrity or the interference with or usurpation of inherently governmental functions.[53] So, if an IO targets voting machinery to undermine public confidence in the vote totals—whether or not the IO actually disrupts the functionality of those machines—it might follow that such an operation comprises a state's sovereignty. But what about "fake news" campaigns affecting how the people using those machines vote? Absent concrete territorial impacts or interference in the government's functions, it is hard to make the case that sovereignty currently forbids such IOs.

In addition to non-intervention and sovereignty, we might ask about human rights regulating IOs. Could, for example, the right to privacy codified in Article 17 of the International Covenant on Civil and Political Rights (ICCPR) regulate hacks of personal data like John Podesta's e-mails?[54] It is not clear, however, that Article 17 and other ICCPR provisions govern Russia's IOs in the United States. Human rights law, including protections of the right to privacy, restricts a state's behavior within its own territory or in jurisdictions under its control.[55] Whether a state must abide by human rights commitments abroad—in, say, an IO targeting a foreign population—is contested. The U.N. Human Rights Committee has endorsed extending the ICCPR to govern extraterritorial government

conversation/.

51. *See, e.g.*, Michael N. Schmitt & Liis Vihul, *Respect for Sovereignty in Cyberspace*, 95 Texas L. Rev. 1639, 1644, 1649 (2017) (citing law enforcement and aircraft overflight as examples of sovereignty violations outside the cyber context); *Corfu Channel* case (United Kingdom v. Albania), 1949 I.C.J. 4, 36 (Dec. 15).

52. *See* TALLINN 2.0, *supra* note 41, at 20–21 (Commentary to Rule 4, ¶ 13); *see also* Nicole Perlroth, *In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back*, N.Y. TIMES (Oct. 23, 2012), http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html (discussing the 2012 cyberattack on Saudi Aramco's computer networks and systems).

53. TALLINN 2.0, *supra* note 41, at 20.

54. International Covenant on Civil and Political Rights, art. 17, ¶ 1, Dec. 16, 1966, 999 U.N.T.S. 171 ("No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence . . . .").

55. *See id.* art. 2 ("Each State Party . . . undertakes to respect and to ensure to all individuals within its territory and subject to its jurisdiction the rights recognized in the present Covenant . . . .").

surveillance.[56] But states like the United States reject that reading.[57] Thus, it is not clear how much, if at all, human rights law may restrain modern IOs like the Russian activities in the 2016 election.

Finally, I should note the innovative claim by Jens Ohlin that IOs could violate the principle of self-determination—the right of a peoples to determine for themselves their political destiny.[58] Ohlin suggests using the self-determination principle to treat as illegal any IO that interferes with an ongoing electoral process.[59] But Ohlin notes that his argument faces some challenges. The history of self-determination has focused on peoples' rights in creating states, not in discourse about electing governments. Moreover, applying the right to self-determination in the IO context presupposes a capacity to identify with sufficient specificity the impact of an IO like "fake news" on a voting public. But, as noted above, this may be difficult to do empirically. Perhaps most importantly, IOs have a long—and, some would say, successful—history of interfering with foreign national elections without self-determination complaints.[60] Dov Levin has done some impressive work that identifies 117 incidents of interference in national elections by either the United States or the Soviet Union/Russia between 1946 and 2000.[61] That practice poses a challenge to arguments about the state of customary international law with respect to IOs like those that occurred in the United States in 2016.

Looking across international law as it exists today, therefore, I am less than sanguine about its capacity to regulate IOs like Russia's 2016 campaign. Existing international law likely prohibits IOs that involve violence or violent consequences in the physical space. IOs that have certain virtual effects may also violate international law whether as an intervention or as a violation of sovereignty. At the same time, there appears to be a range of IOs that states may deploy with only cognitive effects, for which international law has little to say at present.

56. *See* Ryan Goodman, *UN Human Rights Committee Says ICCPR Applies to Extraterritorial Surveillance: But Is That So Novel?*, JUST SECURITY (Mar. 27, 2014), https://www.justsecurity.org/8620/human-rights-committee-iccpr-applies-extraterritorial-surveillance-novel/.

57. *See* Ashley Deeks, *Does the ICCPR Establish an Extraterritorial Right to Privacy?*, LAWFARE (Nov. 14, 2013, 12:00 PM), https://www.lawfareblog.com/does-iccpr-establish-extraterritorial-right-privacy ("[T]he United States has long argued that the ICCPR does not apply extra-territorially, because the U.S. government reads the scope requirement as limiting the treaty to activity within U.S. territory.").

58. Jens David Ohlin, *Did Russian Cyber Interference in the 2016 Election Violate International Law?*, 95 TEX. L. REV. 1579, 1595–96 (2017).

59. *Id.* at 1594–98.

60. *See id.* at 1596 (explaining why international lawyers have been reticent to apply "the language of self-determination" to Russia's involvement in the 2016 U.S. election).

61. Dov H. Levin, *Partisan Electoral Interventions by the Great Powers: Introducing the PEIG Dataset*, CONFLICT MGMT. & PEACE SCI. (2016), at 7.

V. CONCLUSION: WHO SHOULD TAKE RESPONSIBILITY FOR IOS?

I have used this essay to try to lay out a working definition of IOs. In addition, I have offered some bases for distinguishing among IOs in an effort to identify certain elements that could make IOs unacceptable from a national security perspective. International law offers some ways to regulate certain IOs, particularly those that lead to violence. But, for many other IOs—including Russian interference in the 2016 U.S. election campaign—existing international law is not well suited to the task at hand. This then leads to my concluding inquiry: How do we deal with the threats IOs pose? Which actors should use what tools to regulate modern IOs?

Is this an area where we need new international law? For more than a decade, I have argued for new international laws to regulate cyber operations.[62] I have long thought that problems of uncertainty, complexity, and insufficiency favor new rules for cyberspace. And I still believe that international law needs to do more to regulate the information domain, including cyber operations that qualify as IOs.

Yet I do not believe the same proscription holds for influence operations writ large. Simply put, I am not sure that international law is suited to regulation at a cognitive level. Certainly, international law can and has regulated at the physical level. That is what the *jus ad bellum* and the *jus in bello* do, whether it is Hague Law or Geneva Law.[63] Similarly, efforts like *Tallinn 2.0* suggest international law may regulate information operations (although there is a significant increase in the degree of difficulty in doing so). I am doubtful, however, as to whether international law will be able to regulate activities primarily defined by their connection to the cognitive dimension. There is so much uncertainty about evidence, causation, and motivations, that any new law is likely to prove ineffective from the outset.

Moreover, there is also a fear that the cure might be worse than the disease. Consider, for example, resistance to Germany's new NetzDG law (the Network Enforcement Act).[64] The NetzDG law is designed to protect discourse and thus sustain democracy by requiring take-downs of "evidently criminal" content.[65] But

62. *See generally, e.g.*, Duncan B. Hollis, *An e-SOS for Cyberspace*, 52 HARV. INT'L L.J. 373 (2011); Duncan B. Hollis, *Why States Need an International Law for Information Operations*, 11 LEWIS & CLARK L. REV. 1023 (2007).

63. *See generally, e.g.*, Tom Ruys, *The Meaning of "Force" and the Boundaries of the Jus Ad Bellum: Are "Minimal" Uses of Force Excluded from UN Charter Article 2 (4)?*, 108 AM. J. INT'L L. 159 (2014); FRITS KALSHOVEN & LIESEBETH ZEGVELD, CONSTRAINTS ON THE WAGING OF WAR: AN INTRODUCTION TO INTERNATIONAL HUMANITARIAN LAW (2011).

64. Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken [Netzwerksdurchsetzungsgesetz] [NetzDG] (Network Enforcement Act or NetzDG), June 30, 2017, DEUTSCHER BUNDESRAT: DRUCKSACHEN [BR-Drs.] 536/17 (Ger.), http://www.bundesrat.de/SharedDocs/drucksachen/2017/0501-0600/536-17.pdf?__blob=publicationFile&v=1 (last visited Feb. 13, 2018).

65. *See, e.g.*, Eileen Donahue, *Protecting Democracy from Online Disinformation Requires Better Algorithms, Not Censorship*, COUNCIL ON FOREIGN REL. (Aug. 21, 2017), https://www.cfr.org/blog/protecting-democracy-online-disinformation-requires-better-algorithms-

the law has already generated controversy over how it empowers actors like Facebook or Twitter, while also raising fears of censorship and chilling effects, which could themselves end up negatively impacting democratic discourse.[66] Thus, we might consider the warning inherent in the old adage, "if you have a hammer, everything looks like a nail." We can—and should—ask whether the arguments for new law by international lawyers are more an instinctive reaction by those who see law everywhere, rather than an appropriate regulatory response to the problem of IOs.

If law and lawyers are not well-suited to regulate IOs, then who is? Rosa Brooks's book suggests an easy answer: the military. Could the U.S. military take primary responsibility for dealing with state-sponsored IOs, whether as part of the new concept of war or some "space between"?[67] Should it do so? I would expect any such military role to generate many of the same challenges Brooks identifies with other ongoing U.S. military efforts. There are obvious civilian-military issues in assigning responsibility to the military for all IOs, while its mixed track record in the COIN context highlights the risks of making it the "only game in town."[68]

There are, of course, other possible actors and tools beyond the military and the lawyers. Technologists, for example, have begun to acknowledge the role their codes and algorithms play in influencing human behavior.[69] Thus, there might be a third way forward when it comes to differentiating among IOs and seeking to stop those that, like Russian activities in 2016, have caused so much concern. Specifically, we might ask those who produce the technology to serve as the primary line of defense. Of course, recent allegations against Facebook in the Cambridge Analytica scandal[70] raise concerns about the capacity—and motivation—of information communication technology companies to handle this task.

At present, therefore, the complexity and diversity of IOs suggest that they should not be seen as the exclusive regulatory province of any single group. Likewise, I doubt that there can be any single regulatory form for dealing with IOs; different tools will be needed for different contexts, whether domestic regulation, international law, social norms, political pressure, or even military operations.

not-censorship.

66. *Id.*

67. *See supra* note 19, and accompanying text.

68. *See supra* note 10, and accompanying text.

69. *See, e.g.*, Facebook, *Hard Questions: What is Facebook Doing to Protect Election Security?*, Facebook News Room (March 29, 2018), https://newsroom.fb.com/news/2018/03/hard-questions-election-security/; Robert M. Bond et al, *A 61-million-person experiment in social influence and political mobilization*, 489 NATURE 295 (Sept. 2012); Martha Finnemore & Duncan B. Hollis, *Constructing Norms for Global Cybersecurity,* 110 AM. J. INT'L L. 425, 460–61, 472 (2016).

70. *See* Philip Bump, *Everything you need to know about the Cambridge Analytica-Facebook debacle,* WASH. POST (March 19, 2018) https://www.washingtonpost.com/news/politics/wp/2018/03/19/everything-you-need-to-know-about-the-cambridge-analytica-facebook-debacle/.

Simply put, the range of IOs that give rise to national security concerns suggests the need for a hybrid response; multiple actors working collaboratively along multiple fronts to deter IOs from occurring or ensuring the resilience of the audience(s) targeted by them.

We are only just beginning to come to terms with the implications of IOs, notwithstanding that such operations have existed for centuries. Like the "war" concept at the heart of Brooks's *How Everything Became War and the Military Became Everything*, IOs appear to be moving from something apart from our everyday existence—isolated missions like my father's seven months in Vietnam—to ongoing, if not constant, campaigns. Russia's involvement in the 2016 U.S. presidential election signals the beginning, if not of a new form of "war," of something in the "space between." Accordingly, we all need to think carefully about the appropriate responses to it, whether in law, tactics, or technology. In short, we need to pay more attention not just to how war influences everything, but also the rising war for influence.