TEXAS NATIONAL SECURITY REVIEW

POLICY ROUNDTABLE:

Cyber Conflict as an Intelligence Contest

September 17, 2020

In this policy roundtable, part of our special issue on cyber competition, the panelists explore whether cyber conflict might better be understood as a form of intelligence competition.

Table of Contents

1. "Introduction: Is Cyber Conflict an Intelligence Contest?" By Robert Chesney and Max Smeets
2. "What is an Intelligence Contest?" By Joshua Rovner
3. "The Character of Cyber Conflict" By Michael Warner
4. "Military Organizations, Intelligence Operations, and Information Technology" By Jon R. Lindsay
5. "Cyber Persistence, Intelligence Contests, and Strategic Competition" By Michael P. Fischerkeller and Richard J. Harknett
6. "Cyber Conflict as an Intelligence Competition in an Era of Open Innovation" By Nina Kollars

Introduction: Is Cyber Conflict an Intelligence Contest?

Robert Chesney and Max Smeets

Cyber war is out. But what is in?

Scholars now generally recognize the limits of cyber war as a useful concept and/or framework for interpreting the strategic activity taking place in and through cyberspace. But what *is* an accurate way to describe the activity we have been observing over the past few decades, carried out by a broad array of actors? Should we bucket this activity in lots of different categories? Or is there a coherent logic at play which can be captured using an alternative framework?[1]

This roundtable fits within a more recent trend of scholarship — a new wave, one could say — that seeks to grasp the nature of strategic cyber activity. The purpose of this literature is not merely to explain the limits of the cyber war narrative and related concepts, such as deterrence.[2] Instead, it aims to discern the value of *alternative* logics

[1] For the "bucket" approach see, for example, Thomas Rid*, Cyber War Will Not Take Place* (New York, NY: Oxford University Press, 2013).

[2] For works doing exactly this, see, Martin Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND Corporation, 2009), https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf; Adam P. Liff, "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War," *Journal of Strategic Studies* 35, no. 3 (2012): 401–28, https://doi.org/10.1080/01402390.2012.663252; Martin C. Libicki, "Cyberspace is Not a Warfighting Domain," *I/S A Journal of Law and Policy for the Information Society* 8, no. 2 (2012): 325–40, https://kb.osu.edu/bitstream/handle/1811/73111/1/ISJLP_V8N2_321.pdf; Timothy J. Junio, "How Probable is Cyber War? Bringing IR Theory Back In to the Cyber Conflict Debate," *Journal of Strategic Studies* 36, no. 1

and frameworks to explain cyber behavior.[3] We formulated the following question to guide the discussion: Is cyber conflict an intelligence contest?

We have five papers from six authors: Joshua Rovner, associate professor at American University; Michael Warner, former CIA historian and current NSA and U.S. Cyber Command historian; Jon Lindsay, assistant professor at the University of Toronto;

(2013): 125–33, https://doi.org/10.1080/01402390.2012.739561; Erik Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," *International Security* 38, no. 2 (2013): 41–73, http://muse.jhu.edu/journals/ins/summary/v038/38.2.gartzke.html; Brandon Valeriano and Ryan C. Maness, *Cyber War Versus Cyber Realities: Cyber Conflict in the International System* (New York, NY: Oxford University Press, 2015); Michael Fischerkeller and Richard Harknett, "Deterrence is Not a Credible Strategy of Cyberspace," *Orbis* 61, no. 3 (2017): 381–393, https://doi.org/10.1016/j.orbis.2017.05.003; Max Smeets, "The Strategic Promise of Offensive Cyber Operations," *Strategic Studies Quarterly* 12, no. 3 (Fall 2018): 90–113, https://cisac.fsi.stanford.edu/publication/strategic-promise-offensive-cyber-operations.

[3] Different alternatives have so far been proposed. On deception, see, Erik Gartzke and Jon R. Lindsay, "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace," *Security Studies* 24, no. 2 (2015): 316–348, http://dx.doi.org/10.1080/09636412.2015.1038188; On "unpeace" see, Lucas Kello, *The Virtual Weapon and International Order* (New Haven, CT: Yale University Press, 2017); On cyber campaigns, see, Richard J. Harknett and Max Smeets, "Cyber Campaigns and Strategic Outcomes," *Journal of Strategic Studies* (Published on-line March 2020), https://doi.org/10.1080/01402390.2020.1732354; On "shaping operations" see, Ben Buchanan, *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics* (Cambridge, MA: Harvard University Press, 2020); On intelligence, see, Joshua Rovner, "Cyber War as an Intelligence Contest," *War on the Rocks*, Sept. 16, 2019, https://warontherocks.com/2019/09/cyber-war-as-an-intelligence-contest/; David V. Gioe, Michael S. Goodman, and Tim Stevens, "Intelligence in the Cyber Era: Evolution or Revolution?," *Political Science Quarterly* 135, no. 2 (2020): 191–224, https://doi.org/10.1002/polq.13031; Jon R. Lindsay, "Cyber Espionage," in *The Oxford Handbook of Cybersecurity*, ed. Paul Cornish (New York, NY: Oxford University Press, Forthcoming). For a general discussion on the role of framing, see, David J. Betz and Tim Stevens, "Analogical Reasoning and Cyber Security," *Security Dialogue* 44, no. 2 (2013): 147–64, https://www.jstor.org/stable/26302224.

Richard Harknett, professor at the University of Cincinnati, writing together with Michael Fischerkeller, researcher at the Institute for Defense Analyses; and Nina Kollars, associate professor at the Naval War College.

The authors are almost evenly split when pushed to answer the question with a simple "yes" or "no." There are at least four underlying questions the roundtable participants raise and attempt to answer. First, what is the logic of intelligence? Though the intelligence studies literature is vast, a definition remains elusive and has changed over time.[4] The roundtable participants agree that intelligence is more than just information-gathering. They discuss the central role of secrecy and deception. However, there remains disagreement on whether intelligence could be an end of itself, or whether it is always connected to another end (e.g. war or diplomacy).

Second, the participants asked whether scale changes the fundamental logic of intelligence. They all recognize that cyberspace facilitates the ability to operate at a scale not witnessed before. According to Warner, this change in quantity takes on its own quality, fundamentally altering the nature of cyber activities and pushing them past the scope of intelligence activities. Harknett and Fischerkeller agree. For the other roundtable participants, it is not clear how scale fundamentally changes the legitimate ends or

[4] Michael Warner, "Wanted: A Definition of 'Intelligence,'" *CSI Studies* 46, no. 3 (2008): 15–22, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol46no3/article02.html; Mark Phythian, Peter Gill, and Steven Marrin, eds., *Intelligence Theory: Key Questions and Debates* (London: Routledge, 2009); Mark Stout and Michael Warner, "Intelligence Is As Intelligence Does," *Intelligence and National Security* 33, no. 4 (2018): 517–526, https://doi.org/10.1080/02684527.2018.1452593.

appropriate means of cyber activities, or whether it takes on a new quality as a result of this change in scale.

Third, the participants ask: How much do the structural features of cyberspace shape the behavior of actors? Harknett and Fischerkeller argue that cyber activity — specifically, "the dynamics of cyber persistence" — are derived from the fundamental feature of networked computing: interconnectedness. Lindsay draws analogy with evolutionary biology: "Much of cyber security in the wild ... is an example of convergent evolution: Dolphins look like sharks because they are both marine predators, but their common ancestor is exceedingly remote."[5] Similarly, Lindsay notes that in cyber security, "new actors are responding to the same functional imperatives for intelligence and counter-intelligence that have long motivated state agencies." In other words, both Lindsay as well as Harknett and Fischerkeller argue that functional imperatives play a key role in shaping behavior. For Lindsay, this leads to an intelligence contest. For Harknett and Fischerkeller, it leads to persistent engagement.

Fourth, the participants determine which key actors are being enabled by the strategic cyber contest. What is the role of states beyond the great powers? The roundtable essays' principle focus is on the role of state actors. Kollars' essay, however, moves the focus away from state actors towards nonstate actors as the principal focus of discussion. State-based cyber competition is "a tiny parcel of larger competition that often

[5] For an initial discussion on this point also, see, Michael Fischerkeller and Richard J. Harknett, "Deterrence Is Not a Credible Strategy For Cyberspace," *Orbis* 61, no. 3 (2017): 381–393, https://doi.org/10.1016/j.orbis.2017.05.003.

uncomfortably intervenes in state efforts to play their spy games," Kollars notes. Indeed, when it comes to data collection and analysis, the private sector dominates.

The answers set out in this roundtable are important for both understanding the nature of the cyber threat and formulating an accurate policy response. In recent years, we have witnessed an exponential increase in the number of countries establishing military cyber commands. There are now more NATO member states that have established — or seek to establish — a military command with the authority to conduct offensive cyber-effect operations than those that have not.[6] Other countries, such as Peru, Brazil, and Nigeria have recently sought to establish military organizations with a cyber-warfare purview.

We can only interpret this dynamic if we understand the nature of activity enabled through cyberspace. What is the purpose of these organizations if the nature of activity is so closely tied to intelligence agencies?[7] This roundtable debates to what degree these

[6] Max Smeets, "NATO Members' Organizational Path Towards Conducting Offensive Cyber Operations: A Framework for Analysis," *9th International Conference on Cyber Conflict* (NATO CCD COE: 2017), https://ccdcoe.org/uploads/2019/06/Art_09_NATO-Members-Organizational-Path.pdf. For comparative overview of command's organizational structure, see, Piret Pernik, *Preparing for Cyber Conflict – Case Studies of Cyber Command* (Tallinn, Estonia: International Center for Defence and Strategy, December 2018), https://icds.ee/wp-content/uploads/2018/12/ICDS_Report_Preparing_for_Cyber_Conflict_Piret_Pernik_December_2018.pdf.

[7] These issues partially echo an earlier debate on the organizational integration of intelligence agencies and cyber command. See, Michael Sulmeyer, "Much Ado about Nothing? Cyber Command and the NSA," *War on the Rocks*, July 19, 2017, https://warontherocks.com/2017/07/much-ado-about-nothing-cyber-command-and-the-nsa/; Max Smeets, "Integrating Offensive Cyber Capabilities: Meaning, Dilemmas, and Assessment," *Defence Studies* 18, no. 4 (2018): 395–410, https://doi.org/10.1080/14702436.2018.1508349; Robert Chesney, "Should NSA and CYBERCOM Split? The Legal and Policy Hurdles as They Developed Over the Past Year,"

organizational dynamics are more than just "a rebranding exercise to help [these] fledgling organization[s] find [their] footing in a crowded bureaucratic arena," as Lindsay suggests.

The United States has moved towards a strategy of "defend forward" and "persistent engagement," emphasizing continual engagement against cyber threat actors beyond U.S. networks.[8] It is only possible to assess the viability of this strategy if we have a good understanding of the nature of cyber activity. If cyber conflict is an intelligence contest, as Rovner suggests, and not a military contest, we need to change our conception of success. Victory will not be an achievable goal.

This roundtable discussion has implications for the negotiation and development of cyber norms. If cyber activity is part of an older intelligence practice, then discussions regarding the establishment of *new* norms are less necessary.[9] The rules of the game have

Lawfare, July 24, 2017, https://www.lawfareblog.com/should-nsa-and-cybercom-split-legal-and-policy-hurdles-they-developed-over-past-year.

[8] U.S. Cyber Command, *Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command*, March 2018, https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf; U.S. Department of Defense, *Summary: Department of Defense Cyber Strategy 2018*, 2018, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF; Cyberspace Solarium Commission, *Report*, March 2020, https://www.solarium.gov/report; For a discussion about the history and implications of the strategy, see, Jason Healey, "The Implications of Persistent (and Permanent) Engagement in Cyberspace," *Journal of Cybersecurity,* 5, no. 1 (2019): 1–15, https://doi.org/10.1093/cybsec/tyz008.

[9] This is not just about the interaction between adversaries. It may also influence how allies perceive the U.S. change in strategy and how it may clash with their interpretations of sovereignty in cyberspace. Max

already been set — through practice rather than declaratory policy — perhaps even before the existence of cyberspace.[10] If cyber conflict is classified as something other than an intelligence contest, it suggests the importance of new initiatives to promote norms in cyberspace.[11]

Finally, this roundtable is about redefining the interdisciplinary boundaries separating cyber conflict and competition. What is at stake in this debate is an understanding of the discipline's intellectual footing. Who are we to learn from? And what literature should we build on? When cyber conflict is offered as a course of study on university curricula, should the syllabus start with key works drawn from international security literature focusing on concepts such as coercion, the offense-defense balance, and disarmament?[12]

Smeets, "US Cyber Strategy of Persistent Engagement & Defend Forward: Implications For the Alliance and Intelligence Collection," *Intelligence and National Security* 35, no. 3 (2020): 444–453, https://doi.org/10.1080/02684527.2020.1729316.

[10] Ilina Georgieva, "The Unexpected Norm-Setters: Intelligence Agencies in Cyberspace," *Contemporary Security Policy* 41, no. 1 (2020): 33–54, https://doi.org/10.1080/13523260.2019.1677389; Geoffrey B. Demarest, "Espionage in International Law," *Denver Journal of International Law and Policy*, 17 (1995-1996): 321–48, https://digitalcommons.du.edu/djilp/vol24/iss2/4/.

[11] Although experts may still disagree about what type of new initiatives are most suitable to promote standards or proper or acceptable cyber behavior. For a review of some of the most important declaratory practices as the U.N. level, see, Anders Henriksen, "The End of the Road for the UN GGE Process: The Future Regulation of Cyberspace," *Journal of Cybersecurity* 5, no. 1 (2019): 1–9, https://doi.org/10.1093/cybsec/tyy009; Eneken Tikk, "International Cyber Norms Dialogue as an Exercise of Normative Power," *Georgetown Journal of International Affairs* 17, no. 3 (Jan. 2016): 47–59, https://doi.org/10.1353/gia.2016.0036.

[12] This remains the current practice. For a systematic review, see, Trey Herr, Arthur P.B. Laudrain, and Max Smeets, "Mapping the Known Unknowns of Cybersecurity Education: A Review of Syllabi on Cyber Conflict

Or should the course instructor put literature on secrecy, covert action, subversion, counter-intelligence and other intelligence-related topics on the recommended reading list for students?[13] This roundtable is a debate about where the growing contingent of scholars within international relations and beyond should look to in order to understand the field.

While this roundtable answers a series of important questions, we should be humble and realize that it will not settle the debate. One of the main normative questions remains unanswered: Should we *want* cyber conflict to be an intelligence contest? If it is something we can control, is it something to strive for — or do we want cyber conflict to be something different? And, relatedly, is there room for change in the future? If it is an intelligence contest today, can it become something different tomorrow? All the authors highlight the importance of scale in relation to cyber operations. But how does scale size-up with secrecy? We might be looking at a paradox underlying this field, in that cyberspace at its core enables two new forms of behavior that run at odds. The potential negative correlation between secrecy and scale — that an increase in scale leads to a decrease in secrecy and vice versa — is not well-addressed here and deserves more attention in future work.[14] We therefore hope that this roundtable, above all, opens up new avenues for productive conversation and research.

and Security,*" Journal of Political Science Educatio*n (Published Online February 2020), https://doi.org/10.1080/15512169.2020.1729166.

[13] For example, the recent works of Lindsay A. O'Rourke, *Covert Regime Change: America's Secret Cold War* (Ithaca, NY: Cornell University Press, 2018); and Austin Carson, *Secret Wars: Covert Conflict in International Politics* (Princeton, NJ: Princeton University Press, 2018).

[14] A potential starting point for discussion is provided outside this roundtable. See, Michael Ponansky and Evan Perkoski, "Rethinking Secrecy in Cyberspace: The Politics of Voluntary Attribution," *Journal of Global*

Robert Chesney *is the James A. Baker III chair and associate dean for academic affairs at the University of Texas School of Law. He also serves as director of the University's Robert S. Strauss Center for International Security and Law and is the author of the free interdisciplinary casebook* Chesney on Cybersecurity Law, Policy, and Institutions (*available via the Social Science Research Network*). *He is one of the co-founders of* Lawfare *and is co-host of the weekly show* The National Security Law Podcast.

Max Smeets *is a senior researcher at the Center for Security Studies* (*CSS*)*. He also serves as the director of the European Cyber Conflict Research Initiative* (*ECCRI*)*. Max is an affiliate at Stanford University Center for International Security and Cooperation and research associate at the Centre for Technology and Global Affairs, University of Oxford.*

Security Studies 3, no. 4 (2018): 402–416, https://doi.org/10.1093/jogss/ogy022; Florian J. Egloff, "Cybersecurity and Non-State Actors: A Historical Analogy With Mercantile Companies, Privateers, and Pirates," (Ph.D. diss, University of Oxford, 2018); Jon R. Lindsay, "Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence against Cyber Attack," *Journal of Cybersecurity* 1, no. 1 (2015): 53-67, https://doi.org/10.1093/cybsec/tyv003.

What is an Intelligence Contest?

Joshua Rovner

An intelligence contest is an information duel. Rival intelligence services compete to steal information from one another, protect what they have acquired, and corrupt the other side's data and communications. This is fundamentally different from overt arms-racing, where the goal is convincing adversaries that the balance of power is not in their favor. It is also different from war, which is the use of organized violence to compel enemies to change their behavior. In both cases, states seek to convince adversaries that they cannot compete militarily in peacetime and cannot win in a violent conflict. Transparency is required. An intelligence contest, by contrast, is about maintaining an information advantage. All things being equal, the goal is to have more and better information, and success means keeping the other side in the dark.

The ongoing cyberspace competition is largely an intelligence contest. National intelligence services operate in the digital domain to intercept communications and steal data at rest. Because they understand their own vulnerability to espionage, they also practice counter-intelligence to protect digital information against prying eyes. Deception plays a critical role for both intelligence and counter-intelligence operations in cyberspace because successful network intrusion depends on trickery.[15] Some states view cyberspace as a particularly promising venue for propaganda and political manipulation. Finally, they use cyberspace operations to sabotage rival organizations. None of these activities are

[15] Defenders can also use deception to lure attackers away from valuable targets. Jon R. Lindsay and Erik Gartzke, "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace," *Security Studies* 24, no. 2 (2015): 316–348, http://dx.doi.org/10.1080/09636412.2015.1038188.

new. They differ from traditional intelligence activities in degree, not kind. Present debates over Chinese theft of intellectual property, Russian meddling in foreign elections, and U.S. sabotage of rivals' command and control systems are conceptually the same as debates over the uses and limits of intelligence in the past. The fact that they are occurring in cyberspace is interesting and raises a host of important questions for scholars and practitioners. Answering them does not require a new theoretical framework, however. We have one already.

Elements of an Intelligence Contest

Information is the coin of the realm for intelligence agencies, who exist to collect it, to protect it, and to corrupt it. Rival agencies seek relative advantage in the amount and quality of information they acquire. Doing so is important for policymakers seeking to outwit their rivals.[16] Intelligence agencies also compete to secure their own data and prolong the state's decision advantage.[17] Finally, they seek to corrupt their rivals' information and communications. Undermining the integrity or reliability of data has immediate and lasting effects. In the short term, it increases fog by reducing confidence in the quality of information. In the long term, it exacerbates friction by inspiring frustration and anger among personnel in rival organizations.

[16] Jennifer E. Sims, "Decision Advantage and the Nature of Intelligence Analysis," in *The Oxford Handbook of National Security Intelligence*, ed. Loch K. Johnson (Oxford, UK; Oxford University Press, 2010).

[17] Better defense can be a double-edged sword, however, if the price of information security is excessive compartmentalization. Too much compartmentalization makes comprehensive analysis impossible. It also gets in the way of coordinated responses to network intrusions.

An intelligence contest has five defining characteristics. First, it is an effort to collect more and better information on adversaries' capabilities and intentions. Some of this information is available through open sources, but most often, the key details require more elaborate measures. Intelligence services use a variety of collection techniques to discover these secrets.

Second, an intelligence contest is an effort to exploit discovered information for practical gain. Intelligence services provide the "library function" for policy, combining open and secret information to give policymakers a decision advantage.[18] States also try to exploit intelligence to change the balance of capabilities, using stolen intellectual property to reverse engineer weapons systems and other technologies.

Third, an intelligence contest is a reciprocal effort to undermine adversary morale, institutions, and alliances. Secret intelligence services are particularly well-suited for operations targeting adversaries' confidence. Their ability to work clandestinely allows them to craft information campaigns that are not obviously state propaganda. They work through witting or unwitting intermediaries to spread messages in ways that give the state plausible deniability. In some cases, they target specific individuals or groups with specific messages. The advent of email and text messaging makes this particularly appealing today.

Fourth, an intelligence contest is an effort to disable adversary intelligence capabilities through sabotage. All bureaucracies suffer from some amount of friction — the inevitable

[18] Richard K. Betts, *Enemies of Intelligence: Knowledge and Power in American National Security* (New York, NY: Columbia University Press, 2007), 5–6.

daily hiccups that slow down operations and make organizations less efficient. Sabotage in cyberspace weaponizes friction to undermine rival capabilities and morale.

Fifth, an intelligence contest is a campaign to pre-position assets for future collection in the event of a conflict. Rival states may believe that they can compete over information without resorting to violence, but the threat of war looms over enduring rivalries. Intelligence services may be instructed to build the kind of physical clandestine infrastructure that may be useful in the case of war. They may also cultivate human sources who are expected to provide important details about military operations.

The Intelligence Contest in Cyberspace

The United States has recently embraced an approach to cyberspace which emphasizes competition. In 2018, the U.S. Department of Defense recently unveiled a more aggressive approach to cyberspace, promising to "defend forward" and stop attacks before they reach American targets. Successful implementation of this policy requires more ambitious intelligence collection, which in turn creates opportunities to sabotage rival intelligence services and undermine their operations. U.S. Cyber Command (CYBERCOM) is operationalizing Defense Department guidance through what it calls "persistent engagement." CYBERCOM believes that by contesting adversaries continuously in cyberspace, it can impose cumulative costs upon them. Adversaries will recognize the costs of aggression over time, and this will help to set the boundaries of acceptable and unacceptable behavior.

Other great powers have engaged the intelligence contest in cyberspace, though their methods and purposes vary. China and Russia view cyberspace as a venue for espionage

— each state has invested heavily in computer network exploitation over the last two decades. China's main effort has been to steal intellectual property, though it casts the net widely for other kinds of political and military information. Russia has increased its investment in computer network exploitation against a variety of state and nonstate actors.[19] The race to use that information is also ongoing. China has endeavored to use stolen information to reduce its conventional military disadvantages, though with mixed results. [20]

The offensive elements of the intelligence contest were on display during the 2016 election and afterwards, when Russia attempted to sow discord and division throughout the American population. Whether deliberately or not, these efforts may have contributed to public questions about the integrity of American institutions. For its part, the United States has begun talking about using cyberspace to contest adversaries by injecting friction into their systems and organizations.[21]

[19] For examples of different espionage targets, see Thomas Rid, "All Signs Point to Russia Being Behind the DNC Hack," *Vice*, July 25, 2016, https://www.vice.com/en_us/article/4xa5g9/all-signs-point-to-russia-being-behind-the-dnc-hack; Jen Weedon, "Beyond 'Cyber War': Russia's Use of Strategic Cyber Espionage and Information Operations in Ukraine," in *Cyber War in Perspective: Russian Aggression Against Ukraine*, ed. Kenneth Geers (Tallinn, Estonia: NATO Cooperative Cyber Defense Center of Excellence, 2015); and Chris Bing, "Russian Linked Group Tied to Winter Olympics Attack is Now Targeting Biochemical Researchers," *Cyberscoop*, June 19, 2018, https://www.cyberscoop.com/olympic-destroyer-kaspersky-biochemical-research/.

[20] Jon R. Lindsay and Tai Ming Cheung, "From Exploitation to Innovation: Acquisition, Absorption, and Application," in *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, eds. Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron (Oxford, UK: Oxford University Press, 2015).

[21] Jason Healey, "The Implications of Persistent (and Permanent) Engagement in Cyberspace," *Journal of Cybersecurity* 5, no. 1 (2019): 1–15, https://doi.org/10.1093/cybsec/tyz008.

In theory, offensive cyberspace operations are well-suited to this task because they offer a range of tools for the saboteur. States can opt for cheap and easy harassment campaigns like denial of service attacks, or they can engineer sophisticated operations against specific facilities. In either case, the benefits to the saboteur are both practical and psychological. Practical results include harm to networks, data, and infrastructure, all of which forces the target to spend time and money on recovery. Psychological results are equally important. It may not be necessary to cause physical damage if personnel in target organizations fall victim to frustration and finger pointing.

So far, news of direct sabotage of adversary systems has been infrequent. Examples include alleged efforts against Iran's uranium enrichment facility at Natanz, alleged Iranian efforts to disable thousands of workstations at Saudi Aramco, and supposed interest in "left of launch" attacks against North Korean ballistic missile facilities. These operations may foreshadow more ambitious efforts among the great powers. Department of Homeland Security advisories suggest that foreign adversaries have already begun laying the groundwork for possible operations against critical infrastructure and key resources.[22] Such efforts would invite new risks, however, which may explain why they have not moved beyond preparation. A key question, then, is how to compete without triggering a military crisis.

[22] U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, "Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors," March 15, 2018, https://us-cert.cisa.gov/ncas/alerts/TA18-074A.

Other practical problems will emerge as the intelligence contest in cyberspace evolves. Intelligence officials will face hard choices about tasking and priorities, much as their predecessors struggled to allocate scarce collection assets. Bureaucratic fights will deepen because organizations outside of intelligence agencies have a stake in cyberspace operations. Intelligence officials will also face increasing scrutiny from overseers, who have legitimate questions about how states compete in a domain they share with civilians. Allies and partner states, meanwhile, will likely have questions about activities on their own networks. The practical demands on an intelligence contest are as much about navigating diplomacy and domestic politics as they are about overcoming adversaries.

Questions For Theory

Intelligence contests have a long history in great-power politics, and one is ongoing in cyberspace today. That said, international relations theorists might be skeptical that an intelligence contest is distinct from peacetime diplomacy and war, where concealment and deception are common. Diplomats value information advantages because they increase bargaining leverage. Diplomats also share secret information with their partners in order to bind their alliance more tightly, or, more cynically, to create a dependent relationship.[23] Wartime concealment is important to keep enemies off balance, and deception encourages enemies to make bad choices. A vast literature exists on how information is collected, hidden, and distorted for military purposes. So how is an

[23] Albert O. Hirschman, *National Power and the Structure of Foreign Trade* (Berkeley, CA: University of California Press, 1945). On dependence and intelligence liaison arrangements, see Jennifer E. Sims, "Foreign Intelligence Liaison: Devils, Deals, and Details," *International Journal of Intelligence and Counterintelligence* 19, no. 2 (2006): 195–217, https://doi.org/10.1080/08850600500483657.

intelligence contest different? And do we gain analytical traction by treating it separately?

There is no denying that intelligence contests overlap military conflicts and diplomacy. Any international rivalry is likely to feature all three varieties of conflict, often simultaneously. Nor is it useful to pretend that intelligence is independent of the foreign policy it serves. What makes an intelligence contest unique is its emphasis on the control and manipulation of secret information. In fact, a thoroughgoing intelligence contest may continue even when policy goals are unclear. Maintaining information advantages gives leaders flexibility whether they seek more or less ambitious goals. If leaders are unsure of their goals, it gives them time to figure out what they want.

War is different. If an intelligence contest is about information, the essence of military conflict is violent coercion. Translating force into political objectives is extremely demanding, of course, and requires professional education and expertise. Military officers are fundamentally "managers of violence."[24] And unlike an intelligence contest, which requires no definitive end, success in war requires an end to the bloodshed. Deception and concealment have tactical value in war, but strategic success requires transparency. Lasting victory in war requires a common understanding about the balance of power after the shooting stops.

Peacetime diplomacy is also different. Unlike an intelligence contest, which is about gaining information advantages, diplomacy is about persuading self-interested states that

[24] Samuel P. Huntington, *The Soldier and the State: The Theory and Practice of Civil-Military Relations* (Cambridge, MA: Harvard University Press, 1957).

cooperation is in their best interests. Transparency is especially important among allies who, despite common interests, still need to verify that they are trustworthy.

A better analogue is *adversarial* diplomacy. Here, there is not much trust and a great deal of misgiving. Adversaries are inclined against sharing information. Doing so is necessary if diplomats seek détente, but even in these cases they have strong incentives to keep a close hold on what they reveal. Adversarial diplomacy includes selective revelation for the purpose of deceiving rivals about one's own intentions. It resembles clandestine signaling, which can include hints of secret offensive capabilities meant to cause adversaries to doubt their defenses, or hints of intelligence capabilities meant to disabuse them of the notion that they can operate undetected.[25] This mix of concealment and revelation, of truth and deception, will be familiar to intelligence scholars and diplomatic historians. Indeed, adversarial diplomacy is probably close to an intelligence contest.

To say it is close is not to say it is the same. If an intelligence contest is about information, adversarial diplomacy focuses on manipulating the adversary's policy. Depending on circumstance the goal may be to inject a dose of sobriety in the adversary's decision-making, or to induce the adversary to make costly blunders in the service of a competitive strategy.[26] Alternatively, the goal may be to convince third parties to isolate

[25] Brendan Rittenhouse Green and Austin G. Long, "Signaling with Secrets: Evidence on Soviet Perceptions and Counterforce Developments in the Late Cold War," in *Cross-Domain Deterrence: Strategy in an Era of Complexity*, eds. Erik Gartzke and Jon R. Lindsay (Oxford, UK: Oxford University Press, 2019).

[26] Thomas G. Mahnken, ed., *Competitive Strategies for the 21st Century: Theory, History, and Practice* (Stanford, CA: Stanford University Press, 2012).

the adversary or reduce their commitments.[27] In all of these cases, we measure results by looking at the behavior of other states. Concealment, deception, and clandestine signaling are means to an end. In some cases, transparency might be the best way to conduct adversarial diplomacy. Open demonstrations of military capabilities, for example, may be the best way to deal with rivals who harbor absurd fantasies about their own strength.

Intelligence Contests and International Politics

Research on intelligence contests raises other theoretical questions, for which I have few answers. For example, how do we characterize cases in which only one side competes? The weak may believe that intelligence can help them overcome stark material disadvantages. The strong may view intelligence as unimportant. We need a way of describing these lopsided interactions. We may also explore the conditions that cause states to start competing. Under what conditions do great powers to start taking intelligence seriously? When and why do they tolerate foreign powers' efforts? No such theory exists, to my knowledge.

A related question: How do we characterize intelligence contests in multipolar systems, where alliances and rivalries are fluid? The international system before 1945 was multipolar, meaning that most intelligence services operated against a collection of friends and rivals. The discussion here implies that intelligence contests occur between two states. As an analytical shortcut, this may be useful, but intelligence agencies rarely have the luxury of a main adversary. Their attention necessarily wanders. In addition,

[27] Timothy W. Crawford, "The Strategy of Coercive Isolation," in *Coercion: The Power to Hurt in International Politics*, eds. Kelly M. Greenhill and Peter Krause (Oxford, UK: Oxford University Press, 2018).

agencies may reach out to adversaries if policy demands. Shifting alliances may interrupt and confuse even long-running intelligence contests. How they manage these shifts is an open theoretical question.

Multipolar intelligence contests are more complex than bipolar ones. Multipolar contests with nonstate actors are most complex of all. Intelligence work often intermingles with the private sector. Spies seeking cover pretend to be businesspeople, for example, and intelligence services outfits pretend to be businesses. In some cases, they may use commercial networks as venues for recruiting and as conduits of information, leaving private sector actors as unwitting players. The role of the private sector is especially important to the intelligence contest in cyberspace because the domain is mostly operated and maintained by nonstate actors. The internet only functions because of a sprawling constellation of engineers, computer scientists, IT and cyber security firms, and volunteers. States may seek to coopt some of these actors for their own purposes, but they cannot compete without them.

Not all states are interested in enlisting the private sector. Some might hesitate out of concerns for operational security of civil liberties. For whatever reason, they might choose to draw a sharp line between state and nonstate activities and rarely interact with private interests. Other states might be much more enthusiastic, seeing private sector collaboration as essential to operating successfully in cyberspace. They might reason that nonstate actors have a much bigger role to play in cyber competition than in other intelligence contests, given that they largely operate the domain where it takes place. States might also fear that ignoring nonstate actors will leave them at a relative disadvantage.

What does effectiveness mean, and how do we know which side is winning? Traditional understandings of strategic success are inapt in an intelligence contest. Conventional military progress is measured in ground taken, enemy personnel killed or captured, and so on. Analogous intelligence measures are hard to come by. At the tactical level, we can imagine metrics that assess performance against certain targets. With access to classified information, for example, we can ask whether an intelligence agency recruited a certain number of assets in a foreign country. But such arbitrary metrics are not intrinsically important. The critical question is not whether the agency met its quota, but whether the quota was a reasonable proxy for gaining enough information to provide decision advantage to political and military leaders. The intelligence consumer gets to decide how much is enough. Because different leaders are satisfied by varying degrees of success, it is hard to conceive of consistent measures of effectiveness.

As in any intelligence contest, we should be humble about estimating the results in cyberspace. The U.S. approach, for example, calls for imposing cumulative costs over time, but there is no formula for determining when irritation will become intolerable. Nor is there a simple method for distinguishing the independent effects of cyberspace operations, given the variety of other policy tools at work. The simultaneous growth of the internet also complicates efforts to measure progress. We may see more high-profile attacks even if they are declining in proportion to the overall volume of cyberspace activities. In addition, what constitutes "success" will reflect differing value judgments. Those who believe the government is obligated to protect private firms, for instance, will view all breaches as failures. Those who believe that the government has no such obligation will likely view private sector attacks as unfortunate, but unrelated to its campaign against foreign state adversaries.

In a general sense, success means gaining information advantages without creating new dangers. This is not easy, because some elements of an intelligence contests are clearly provocative. The goal for states is to compete energetically while striving to establish Cold War-style "rules of the game." These are tacit understandings that govern the actions of rival intelligence services, a set of expected behaviors that both sides deem acceptable. Without such rules, intelligence collection can turn into a very nasty business. The rules of the game limit the kinds of collection that is permissible and off-limits against certain targets (e.g., family members). The rules also lay out tacit understandings about unacceptable methods (e.g., kidnapping and torture). Over a long period of competition, intelligence services can arrive at quiet and informal agreements about where the lines are drawn. If the rules of the game are sufficiently clear, intelligence leaders will be careful not to break them, because the diplomatic consequences would outweigh the value of whatever new information they acquired.

Intelligence contests might have other effects on enduring rivalries. In some cases, they might prolong hostility. Particularly aggressive espionage and sabotage campaigns work at cross-purposes with détente, delaying better relations even when both sides have reasons to come together. On the other hand, aggressive intelligence may serve as a release valve that keeps simmering rivalries from boiling over. States might believe they can trade knowledge for power, increasing their intelligence effort in order to draw down military forces abroad and reduce the danger of crises. Secret intelligence may also have counterintuitive benefits for international stability, even during periods of intense competition. States who take counter-intelligence seriously might be more likely to comply with peacetime arms control agreements, because they do not fear revealing military capabilities that could leave them vulnerable in a future conflict.[28] Covert action is also useful in proxy wars, because it is a release valve for great-power rivals who want to compete but who fear the consequences of open warfare.[29]

Finally, we can attempt to situate intelligence contests in the broader debate over grand strategy. What role does intelligence play for those who favor restraint? Is it really possible to trade knowledge for power, as suggested above? Similarly, is it logically possible to wage an intelligence contest while pursuing an institutionalist grand strategy? At first glance, the answer seems to be no, because institutionalism requires sharing information to realize the benefits of collective action and lower transaction costs. But some scholars suggest that intelligence efforts can play a role in grand strategy by supporting covert attempts to topple illiberal rivals. Successful efforts may help bring new liberal states into the institutional order. In this sense, covert action represents a kind of temporary but useful hypocrisy in the service of a liberal internationalist grand strategy.[30]

Theoretical work on these questions is likely to shed light on intelligence contests from the past. It might also help practitioners compete in cyberspace today, especially given

[28] Jane Vaynman and Andrew J. Coe, "Why Arms Control is So Rare," *American Political Science Review* (forthcoming).

[29] Austin Carson, *Secret Wars: Covert Conflict in International Politics* (Princeton, NJ: Princeton University Press, 2018).

[30] Michael Poznansky, *In the Shadow of International Law: Secrecy and Regime Change in the Postwar World* (Oxford, UK: Oxford University Press, forthcoming). For an initial attempt to map intelligence onto grand strategy, see Joshua Rovner, "Intelligence and Grand Strategy," in *The Oxford Handbook of Grand Strategy*, eds. Ronald R. Krebs and Thierry Balzacq (Oxford University Press, forthcoming).

the fact that they are waging overlapping contests with numerous adversaries. Intelligence officials already face hard choices about tasking and priorities, much as their predecessors struggled to allocate scarce collection assets. Bureaucratic fights are likely to deepen because organizations outside of intelligence agencies have a stake in cyberspace operations. Intelligence officials will face increasing scrutiny from overseers, who have legitimate questions about how states compete in a domain they share with civilians. Allies and partner states, meanwhile, will likely have questions about activities on their own networks. Navigating these thorny issues will not be easy in the ongoing cyberspace competition. A firmer theoretical foundation will surely help.

Joshua Rovner *is an associate professor in the School of International Service at American University. In 2018 and 2019, he served as a scholar-in-residence at the National Security Agency and U.S. Cyber Command. The views here are his alone.*

The Character of Cyber Conflict

Michael Warner

What is a cyber conflict? Over the last decade, scholars have enthusiastically argued about the term's definition and the implications of its growing salience. Nations have joined in these debates, building cyberspace forces, sponsoring more- or less-secret missions in this new operating space, and disputing international norms for cyber activities. Is this war, muscular diplomacy, crime, or something else? I have published elsewhere on the evolutionary ties between cyberspace operations and intelligence work. Indeed, the historical record clearly shows their kinship.[31] Recently, several scholars have argued that the former are in fact the latter — that cyber conflict represents an "intelligence contest." This notion merits a closer examination.

In pondering whether the character of cyber conflict resembles an "intelligence contest," we commence with the findings of Jon Lindsay and Joshua Rovner. In 2017, Lindsay suggested that cyber conflict is "a form of cheating within the rules, rather than an anarchic struggle, more like an intelligence-counterintelligence contest than traditional war."[32] He and his co-author Erik Gartzke explained in another essay that "[b]y and large, cyber options fill out the lower end of the conflict spectrum, when deterrence is not as credible or reliable." The exceptions to this rule are "mainly powerful states conducting

[31] Michael Warner, "Intelligence in Cyber – and Cyber in Intelligence," in *Understanding Cyber Conflict: Fourteen Analogies*, eds. Ariel Levite and George Perkovich (Washington DC: Georgetown University Press, 2017).

[32] Jon Lindsay, "Restrained by Design: the Political Economy of Cybersecurity," *Digital Policy, Regulation and Governance* 19, no. 6 (2017): 493–514, https://doi.org/10.1108/DPRG-05-2017-0023. The quoted portion is from the abstract.

covert action, subversive propaganda, or battlefield support operations against militarily weaker opponents."[33]

Rovner adds that the "ongoing competition in cyberspace is largely an intelligence contest. Although the technology is different, the underlying contest exhibits all the characteristics of traditional spy-versus-spy battles."[34] Last September, he explained that such a contest entails five elements:

> First, it is a race among adversaries to collect more and better information. Second, it is a race to exploit that information to improve one's relative position. Third, it is a reciprocal effort to covertly undermine adversary morale, institutions, and alliances. Fourth, it is a contest to disable adversary capabilities through sabotage. Fifth, it is a campaign to preposition assets for intelligence collection in the event of a conflict.[35]

Let us explore this topic, beginning with intelligence, then considering cyberspace itself, and finally revisiting cyberspace conflict.

[33] Jon R. Lindsay and Erik Gartzke, "Coercion Through Cyberspace: The Stability-Instability Paradox Revisited," in *Coercion: The Power to Hurt in International Politics*, eds. Kelly M. Greenhill and Peter Krause (Oxford: Oxford University Press, 2018), 202.

[34] Joshua Rovner, "The Intelligence Contest in Cyberspace," *Lawfare*, March 26, 2020, https://www.lawfareblog.com/intelligence-contest-cyberspace.

[35] Joshua Rovner, "Cyber War as an Intelligence Contest," *War on the Rocks*, Sept. 16, 2019, https://warontherocks.com/2019/09/cyber-war-as-an-intelligence-contest/.

What Is Meant by an Intelligence Contest?

First, we should define "intelligence." Rovner implicitly agrees with the notion that intelligence at the strategic level includes both information on *and* activity to influence adversaries and contexts.[36] In keeping with this definition, an intelligence contest would be a mutual, national, and competing employment of secret means — spies, surveillance, and the analysis of their results, plus covert action and counter-intelligence. Such activities entail tactical risks, up to and including the execution of spies. Its means are typically employed in a sort of diplomatic and military twilight, in which nations are neither friends nor shooting enemies. Each opponent suspects the other is using such means — if not where he is employing them — and each side does what it can to mitigate rival intelligence activities. Each side also, however, tacitly concedes that ending all such activities is not worth the loss of ill-gotten knowledge (which can be invaluable), or worth the hyper-vigilance necessary to eliminate all cloak-and-dagger work by the opponent. The intelligence contest thus proceeds with certain unspoken but nonetheless efficacious *limits* that keep its risks manageable and tolerable. Both sides, as Rovner hints, tacitly agree not to exceed those limits, and by and large they restrain their intelligence operations accordingly.

Second, it is important to look at the purpose of intelligence. It is not a "thing" with an independent existence. Dr. Mark Stout and I define it as an additive to some other state

[36] Intelligence is that set of activities that is both *secret* and *sovereign*; see Michael Warner, "Wanted: A Definition of Intelligence," *Studies in Intelligence* 46 (2002): 15–22, https://apps.dtic.mil/dtic/tr/fulltext/u2/a525816.pdf.

function: war, diplomacy, and internal security.[37] In other words, intelligence supplements activities that sovereign powers undertake "against" or "with" other sovereignties to guard, maintain, or expand their national freedom of action. For states and armed nonstate actors, intelligence is the sustained use of secret means for sovereign purposes, and it always serves military, diplomatic, or internal security missions. It does not exist on its own, unless it is dysfunctional (and soon to be reformed or dismantled).

Intelligence is thus a support function rather than an end in itself. War, diplomacy, and security work better with intelligence, of course, but they can and do work without it. Indeed, they functioned for thousands of years in hundreds of sovereignties without any organized and sustained intelligence services like those that began emerging in the late 19th century.

Here I note a slight hitch in Rovner's analysis, specifically where he contrasts "military contests" with "intelligence contests." He explains that "most activities in cyberspace have little to do with the use of force. Instead, they are part of an intelligence contest." A military contest, by contrast, "is a test of physical power."[38] This is not quite right. Intelligence methods do not contrast with military methods — the methods of intelligence *are* military methods. This is not to say that military and civilian intelligence services all work the same way. But modern intelligence grew up in military establishments, which still provide the bulk of global intelligence resources. Those militaries expect their intelligence services to serve military ends, which by definition include the use of force.

[37] Mark Stout and Michael Warner, "Intelligence Is As Intelligence Does," *Intelligence and National Security* 33, no. 4 (2018): 517–526, https://doi.org/10.1080/02684527.2018.1452593.

[38] Rovner, "Cyber War as an Intelligence Contest."

Rovner ought to have said that the five features he lists above show intelligence activities in the service of diplomatic or internal security purposes, rather than serving strictly military ends. One hastens to add that force can still come into play in a non-military context — plenty of internal security arms happily use force on their fellow citizens and employ intelligence methods to aid its application.

The Role of "Scale"

Intelligence is military, diplomatic, or security work by secret means. It is sustained, yes, but not *at-scale*. What does this mean? Simply that in the intelligence context secrecy rules: It sharply limits the size and scope of intelligence operations because it imposes a certain "drag" on the efficiency of diplomatic, military, and security actions.[39] Rovner's choice of historical analogies implicitly concedes that intelligence contests are relatively small in scale, involving far fewer people and resources than diplomatic or even military competitions:

> During the Cold War, Soviet and U.S. intelligence professionals came to observe some rules of the game. Aggressive counter-intelligence methods

[39] Michael Warner, "Fragile and Provocative: Notes on Secrecy and Intelligence," *Intelligence and National Security* 27, no. 2 (April 2012): 223–240, https://doi.org/10.1080/02684527.2012.661644. Note here Clausewitz's analysis of "cunning," where he hints that commanders can deceive opponents on a tactical but not a strategic scale: "To prepare a sham action with sufficient thoroughness to impress an enemy requires a considerable expenditure of time and effort, and the costs increase with the scale of the deception. Normally they call for more than can be spared, and consequently so-called strategic feints rarely have the desired effect." Carl von Clausewitz, *On War*, trans. Peter Paret (Princeton NJ: Princeton University Press, 1976), 203.

> were expected, for example, but not against family members. Neither side could deter intelligence efforts, but they could structure the contest in order to reduce the risk.[40]

We can call intelligence "sustained secrecy" — though that phrase is a mild contradiction in terms. Intelligence is like the bumblebee which, according to urban legend, flies despite its small wings, in supposed defiance of the laws of aerodynamics. Scientists pondering this riddle ultimately proved how small animals with flexible wings achieve flight even though they could never do so with rigid wings disproportionate to their body mass. Intelligence, by analogy, sustains secrecy to serve diplomatic, military, and security purposes by using methods that soldiers, diplomats, and officials do not regularly employ. Secrecy limits the scale of intelligence activities and contributions, and it also adds a *frisson* of danger to their work. After all, the premature revelation of intelligence activities can be detrimental to the military, security, and especially the diplomatic purposes they are conducted to serve. Intelligence operations involve their own contradiction: They are useful only in modest amounts.

Here we confront something that challenges the notion of cyberspace conflict as an intelligence contest. We need to reflect on the sheer scale of cyberspace, which now links billions of users on billions of networked devices — a universe which grows by several factors if we add in those devices comprising the "Internet of Things." The cataracts of data that surge around the internet beggar description — and they grow exponentially at ever-decreasing intervals. The resource demands of cyberspace, moreover, seem insatiable. It is reshaping society as both a means and an end. We once spoke, for

[40] Rovner, "The Intelligence Contest in Cyberspace."

instance, of the “digital economy.” Today such a term seems not only quaint but redundant.

Strategic competition in cyberspace thus occurs in a very big environment. But if we can call its environment an arena — or a venue — for force, then we must also note that the competitors themselves help us maintain that environment through their interactions. They cooperate constantly, for only through mutual agreement can they stay connected to the internet and continue to swap data packets. Here we note Jon Lindsay′s insight that cyberspace itself is a fraught cooperation. Lindsay explains that cyberspace’s continued functioning implies a constant and consensual technical interchange between allies, neutrals, and adversaries:

> Maintenance of common protocols and open access is a condition for the possibility of attack, and successful deceptive exploitation of these connections becomes more difficult in politically sensitive situations as defense and deterrence become more feasible. The distribution of cyber conflict is, thus, bounded vertically in severity but unbounded horizontally in the potential for creative exploitation.[41]

How does this mesh with the strategic competition discussed in the 2017 *National Security Strategy*? That document contends that “great-power” rivalry occurs across the diplomatic, information, military, and economic spheres, which means it reaches into cyberspace. No surprise, then, that strategic competition manifests itself in contending

[41] Lindsay, ″Restrained By Design.”

cyberspace policies, activities, and operations. Some of these strongly resemble covert action. As I recently argued in the CIA's in-house journal *Studies in Intelligence*:

> Cyberspace allows states to conduct operations that look much like covert action just as cheaply but far more broadly … It offers (relative) anonymity, and its near-instantaneous delivery of finely tailored appeals to thousands or even millions of computer users provides the venue and means to do what covert actions once could attempt at a fraction of the extent. Indeed, cyberspace seems to have fixed covert action's problem of scale.[42]

Taking note of Russian efforts to affect the 2016 U.S. elections, the Mueller report reached a similar conclusion about the St. Petersburg-based Internet Research Agency (IRA):

> By the end of the 2016 U.S. election, the IRA had the ability to reach millions of U.S. persons through their social media accounts. Multiple IRA-controlled Facebook groups and Instagram accounts had hundreds of thousands of U.S. participants. IRA-controlled Twitter accounts separately had tens of thousands of followers, including multiple U.S. political figures who retweeted IRA-created content.[43]

[42] Michael Warner, "A Matter of Trust: Covert Action Reconsidered," *Studies in Intelligence* 63, no. 4 (2019): 33–41, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol-63-no-4/pdfs/Covert-Action-Reconsidered.pdf.

[43] Robert S. Mueller, III, *US Department of Justice, Report on the Investigation Into Russian Interference in the 2016 Presidential Election*, Vol. I, March 29, 2019, 14–15, https://www.justice.gov/storage/report.pdf.

I argued in *Studies* that the scope of cyber-enabled efforts like the Internet Research Agency's dwarfs anything that had been possible before the internet. Even radio broadcasts to entire countries during the Cold War did not make active, unwitting participants of their audiences. Passive listening and recounting recent news reports lacks the authenticity and immediacy of a retweet that perfectly replicates and spreads covert action messages produced by a foreign power.

Thus, cyberspace seems to be facilitating operations and effects that resemble covert actions but are much larger in their scale and reach. If covert action represents one way to bridge the gap between diplomacy and war, then cyberspace operations might offer another span, as it were, for exerting influence. ISIL does not have to inspire more than a handful of "lone wolves" in the West, for instance, to achieve its goal of spreading fear of Muslims and fueling debates over immigration. Country-wide arguments over attribution, response, and collusion do not seem to be receding.

Quantity has assumed its own quality. Cyberspace operations are not just "bigger" covert actions or espionage activities. Their scale gives them a character different from that of intelligence activities. The U.S. Congress would seem to agree. In 2018, it passed legislation via the National Defense Authorization Act (for Fiscal Year 2019) that amended Title 10 of the U.S. Code, affirming that clandestine U.S. military operations against adversary activities in cyberspace do not have to be regulated and overseen like covert actions. Such activities or operations by American forces could instead be governed as "traditional military activity" under Title 50 of the U.S. Code. A year later Congress expanded this point beyond cyberspace in the National Defense Authorization Act (for Fiscal Year 2020), declaring that even a "clandestine military operation in the information environment shall be considered a traditional military activity" — and not espionage or covert action.[44]

The Role of Ideology

What is so different about cyberspace operations, as opposed to the sort of activities historically seen in intelligence contests? Here, we look to history as a reference point for any subsequent theory-building. Fortunately, the history of cyber conflict is clear in this regard. First, the cyber competitions that matter between states (i.e., the ones that could potentially lead to war) are *strategic*. They can and do touch states at their bases of sovereign power, even if those instruments of national power do not connect directly to the internet. That means that foes, even those with modest military forces, can now "contact" and threaten assets that a rival regime cannot afford to lose.[45] Second, such strategic competitions in cyberspace are also *ideological*: They involve disputes over competing and even mutually exclusive societal visions.

Some clarification is needed here. My point is not that all cyber conflict occurs between ideological opponents — clearly that is not the case. Likewise, several states and movements that are quite aggressive in cyberspace do not possess coherent ideologies they are seeking to impose on their neighbors. They are nonetheless seeking to shape the

[44] U.S. Congress, *S1790-National Defense Authorization Act for Fiscal Year 2020*, December 20, 2019, Chapter 19, https://www.congress.gov/116/plaws/publ92/PLAW-116publ92.pdf.

[45] Michael P. Fischerkeller and Richard J. Harknett, *Persistent Engagement, Agreed Competition, Cyberspace Interaction Dynamics, and Escalation* (Alexandria, VA: Institute for Defense Analyses, May 2018), 3, https://www.ida.org/-/media/feature/publications/p/pe/persistent-engagement-agreed-competition-cyberspace-interaction-dynamics-and-escalation/d-9076.ashx.

international order, as the Joint Chiefs' *Joint Concept for Integrated Campaigning* explained in 2018:

> Strategic challenges such as China, Russia, Iran, and North Korea are employing coercive methods to accomplish objectives in the competitive space between peace and war. These competitors aim to change international norms with operations characterized by uncertainty to create ambiguity meant to confuse public opinion, paralyze political decision making, subvert legal frameworks, and avoid crossing the threshold of military response.[46]

What these regimes share is a conviction that they are locked in a desperate ideological competition with "the West," whose liberal/pluralist/Crusader values (pick your adjective) pervade the internet and cannot be allowed to extend that control into the regime's territory. Thus, it is significant that cyberspace conflict occurs primarily between states ruled by anti-liberal (often one-party) regimes and the more or less democratic states that they deem threatening.

Expanding on this point, we should also note that cyberspace has itself altered the sources of strategic power that opponents can "touch" by digital means. The sources of power (and thus the strategic prizes) in the 20th century naturally included the means of production and the routes along which goods and people moved. The growing

[46] Joint Chiefs of Staff, *Joint Concept for Integrated Campaigning,* March 16, 2018, 2,https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concept_integrated_campaign.pdf?ver=2018-03-28-102833-257.

connections between states and the increasing salience of democracy and international law after 1945 also added a new strategic factor: public opinion and global audiences. Over the last generation, the inter-connectedness of cyberspace has added three more sources of national power to this list of strategic prizes. These are a nation's 1) intellectual capital; 2) privacy of its citizens; and 3) legitimacy of its government (as perceived by its citizens, allies, and creditors). All of these can now be threatened *on a systemic level* by cyberspace operations.

We can cite as an authority the chief of Russia's armed forces, Gen. Valery Gerasimov, who reflected on the danger of an Arab Spring in Russia. Wars in the 21st century, he told the Academy of Military Science in 2013, "are no longer declared and, having begun, proceed according to an unfamiliar template."[47] Yet contemporary struggles are no less deadly for unready regimes, he explained:

> The experience of military conflicts — including those connected with the so-called [color] revolutions in north Africa and the Middle East — confirm that a perfectly thriving state can, in a matter of months and even days, be transformed into an arena of fierce armed conflict, become a victim of foreign intervention, and sink into a web of chaos, humanitarian catastrophe, and civil war.[48]

[47] Gerasimov spoke at the Academy of Military Science in February 2013. See, Robert Coalson, "Top Russian General Lays Bare Putin's Plan for Ukraine," *Huffington Post*, Sept. 2, 2014, https://www.huffpost.com/entry/valery-gerasimov-putin-ukraine_b_5748480?guccounter=1.

[48] Coalson, "Top Russian General Lays Bare Putin's Plan for Ukraine."

Gerasimov perceived in the Arab Spring “the use of technologies for influencing state structures and the population with the help of information networks.” Such non-military means of achieving strategic goals often exceeded “the power of force of weapons in their effectiveness,” for “methods of conflict” such as “political, economic, informational, humanitarian, and other non-military measures” could now be “applied in coordination with the protest potential of the population.”[49]

As Gerasimov hinted, Russia and other anti-liberal states could not afford to cede cyberspace to Western governments, corporations, non-governmental organizations, and social media. States have thus engaged in a struggle over intellectual capital, privacy, and legitimacy. The incidents of that struggle often take place in cyberspace. Various states are employing all five of Rovner's elements of an intelligence contest, albeit not all at once or against every opponent. Several anti-liberal regimes, however, have stepped well outside that list in campaigns to secure intellectual property, privacy, and legitimacy. They act to secure those digital elements of power within their own territorial limits, as former Secretary of State Hillary Clinton lamented in her memoirs:

> Around the world, some countries began erecting electronic barriers to prevent their people from using the internet freely and fully. Censors expunged words, names, and phrases from search engine results. … One of the most prominent examples was China, which, as of 2013, was home to nearly 600 million internet users but also some of the most repressive limits on internet freedom. The “Great Firewall” blocked foreign websites

[49] Coalson, “Top Russian General Lays Bare Putin’s Plan for Ukraine.”

> and particular pages with content perceived as threatening to the Communist Party.[50]

Such censorship and control amounted to information war that targeted the populace, Clinton suggested. She pushed the State Department to counter such restrictions by training activists around oppressive regimes to employ cyber tools that could "protect their privacy and anonymity online and thwart restrictive government firewalls." By 2011, she noted, "[the United States] had invested more than $45 million in tools to help keep dissidents safe online and trained more than five thousand activists worldwide, who turned around and trained thousands more." Clinton herself visited one of these workshops in Lithuania, a nation figuratively on Russia's doorstep, not long before massive protests rocked the Kremlin.[51]

Efforts by anti-liberal regimes to defend themselves against Western liberalism have reached into Western democracies. One example is Russia's campaign to confuse and provoke American voters in the 2016 election. According to the indictment of 13 Russians handed up by Special Counsel Robert Mueller in 2018, Moscow mounted a covert campaign to get Americans arguing with one another. Russia's Internet Research Agency "as early as 2014 … began operations to interfere with the U.S. political system, including the 2016 U.S. presidential election," noted the indictment.[52] The Russians employed

[50] Hillary Rodham Clinton, *Hard Choices* (New York: Simon & Schuster, 2014), 545

[51] Clinton, *Hard Choices*, 545–9.

[52] *United States of America v. Internet Research Agency et al.*, US District Court for the District of Columbia, Feb. 16, 2018, 3, https://www.scribd.com/document/371718383/Internet-Research-Agency-Indictment-pdf#from_embed.

classic divide-and-conquer tactics, attacking the presidential candidates whom they (along with most American experts) considered strongest while ignoring their apparently weaker challengers. Russian agents…

> …engaged in operations primarily intended to communicate derogatory information about Hillary Clinton, to denigrate other candidates such as Ted Cruz and Marco Rubio, and to support Bernie Sanders and then-candidate Donald Trump. … On or about February 10, 2016, Defendants and their co-conspirators internally circulated an outline of themes for future content to be posted to [Internet Research Agency]-controlled social media accounts. Specialists were instructed to post content that focused on "politics in the USA" and to "use any opportunity to criticize Hillary and the rest (except Sanders and Trump— we support them)."[53]

The means that the anti-liberal regimes employ in cyberspace go well beyond the range and scale of an intelligence contest because the threat they see from Western commerce and social media far exceeds an intelligence threat. China's "Great Firewall" is not an intelligence operation — it is an internal security overwatch for nearly a billion users, which can also be used as an offensive weapon.[54] Openly training civil society activists to use encrypted channels, as Secretary Clinton hinted, was perhaps coercive diplomacy, but not an intelligence activity. These are diplomatic, military, and security measures, often

[53] *United States of America v. Internet Research Agency et al.*, 17. See also, Scott Shane, "These Are the Ads Russia Bought on Facebook in 2016," *New York Times*, Nov. 1, 2017, https://www.nytimes.com/2017/11/01/us/politics/russia-2016-election-facebook.html.

[54] See, for instance, Bill Marczak, et al., "China's Great Cannon," *Citizen Lab*, Munk School of Global Affairs, University of Toronto, April 10, 2015; https://citizenlab.ca/2015/04/chinas-great-cannon/.

performed transparently rather than secretly. Chinese theft of intellectual property was hardly hidden, even if individual instances worked in stealth. U.S. Cyber Command's capture of malware in foreign networks and its decision to post the malware on VirusTotal is not an intelligence mission, even if it impairs another state's intelligence gathering by neutralizing operational infrastructure.[55] Such activities can look like intelligence, but that is because intelligence activities look like, and indeed are, military, diplomatic, and internal security actions by secret means.

Such campaigns proceed against liberal societies whether or not the democracies resist them. They do so because they are primarily *defensive*. Anti-liberal regimes that are most aggressive in cyberspace believe Western online actors are constantly menacing their legitimacy, secrets, and control over their citizens by overt and covert means. Since this is an ideological struggle, it could break out in war. But it does not have to. This conflict seems more like a cold war — what George Orwell foresaw in 1945 as "an end to large-scale wars at the cost of prolonging indefinitely a 'peace that is no peace.'"[56]

Ideology is key to the *strategic* competition we see in cyberspace. Tactical cyber skirmishes between states and even nonstate actors will continue and even grow, but we cannot analyze the strategic cyber conflicts we see now as if they could happen between any pair of random states. Cyber conflict on that level occurs between liberal and anti-liberal states, and it seems destined to continue until the anti-liberal regimes somehow acquire less paranoid and aggressive ideas about history and their neighbors. They

[55] Statement of General Paul M. Nakasone, United States Cyber Command, before the House Committee on Armed Services, Subcommittee on Intelligence, Emerging Threats, and Capabilities, March 13, 2019.

[56] George Orwell, "You and the Atomic Bomb," *Tribune*, Oct. 19, 1945.

contend with each other at times in ways that resemble an “intelligence contest,” but their strategic competition is more like a cold war.

Conclusion

Many *cyberspace operations* proceed in a manner that looks a lot like a sort of intelligence contest. But *strategic cyberspace conflict* is not fundamentally an intelligence contest, for the reasons articulated in this essay. We should nevertheless study the intelligence contests of the Cold War to see how they limited, as well as deepened, competition. We should also look to some of the wiser policies of the Cold War, especially in the 1980s, for ideas on how our current strategic competition could end.

***Dr. Michael Warner** serves as command historian at U.S. Cyber Command. The opinions in this essay are his own alone, and do not necessarily reflect official positions of the Department of Defense or any U.S. government entity.*

Military Organizations, Intelligence Operations, and Information Technology

Jon R. Lindsay

I am grateful for the opportunity to comment on the idea of cyber security as an intelligence contest. This idea has gained traction recently and offers a useful contrast to alternative framings of cyber operations in terms of military warfare and strategic deterrence.[57] Thankfully, it is becoming less common to hear cyber described as a more affordable version of strategic bombing or as an anonymous weapon of mass destruction. The empirical record of cyber conflict, now decades long, does not support such arguments, which also suffer from numerous theoretical problems.[58] More useful precedents can be found in the history of piracy, espionage, subversion, disinformation,

[57] Critical perspectives on the analogies mobilized in cyber security discourse include David J. Betz and Tim Stevens, "Analogical Reasoning and Cyber Security," *Security Dialogue* 44, no. 2 (April 1, 2013): 147–64, https://doi.org/10.1177/0967010613478323; George Perkovich and Ariel E. Levite, eds., *Understanding Cyber Conflict: 14 Analogies* (Washington DC: Georgetown University Press, 2017); Jordan Branch, "What's in a Name? Metaphors and Cybersecurity" (Typescript, 2019); James Shires, "Cyber-Noir: Cybersecurity and Popular Culture," *Contemporary Security Policy* 41, no. 1 (January 2, 2020): 82–107, https://doi.org/10.1080/13523260.2019.1670006.

[58] For analytical reviews of international relations scholarship on cybersecurity see Hans-Inge Langø, "Competing Academic Approaches to Cyber Security," in *Conflict in Cyberspace: Theoretical, Strategic and Legal Perspectives*, eds. Karsten Friis and Jens Ringsmose (Abingdon: Routledge, 2016), 7–26; Robert Gorwa and Max Smeets, "Cyber Conflict in Political Science: A Review of Methods and Literature" (International Studies Association Annual Convention, Toronto, 2019), https://doi.org/10.31235/osf.io/fc6sg.

and sabotage. From this perspective, cyber conflict is simply a new evolution of the ancient contest between intelligence and counter-intelligence.[59]

This idea has received some pushback. While there is a growing consensus that cyber conflict is something other than war, there is less agreement on whether it should be described as intelligence, special operations, or something novel unto cyberspace itself. This debate is not simply an academic exercise. Rather, it has institutional consequences. In this essay, I argue that U.S. Cyber Command (CYBERCOM) has strong organizational incentives to describe cyber security in military terms, even though cyber conflict is essentially an intelligence contest, albeit a contest conducted at unprecedented technological scale.[60]

The Organizational Context

Strategists at CYBERCOM, supported by the work of civilian academics and the Congressional Cyberspace Solarium Commission, stress that cyberspace is a domain of "constant contact" that makes it possible to achieve strategic effects without resorting to

[59] See Joshua Rovner, "Cyber War as an Intelligence Contest," *War on the Rocks*, Sept. 16, 2019, https://warontherocks.com/2019/09/cyber-war-as-an-intelligence-contest/; David V. Gioe, Michael S. Goodman, and Tim Stevens, "Intelligence in the Cyber Era: Evolution or Revolution?," *Political Science Quarterly* 135, no. 2 (2020): 191–224, https://doi.org/10.1002/polq.13031; Jon R. Lindsay, "Cyber Espionage," in *The Oxford Handbook of Cybersecurity*, ed. Paul Cornish (New York: Oxford University Press, Forthcoming).

[60] I use the term "cyber conflict" here to describe the contest between offensive and defensive operations in and through "cyberspace"—itself a poor territorial metaphor. I use "cyber security" to refer more broadly to both the study and practice of cyber conflict, analogous to "international security."

war.[61] As a 2018 CYBERCOM vision document states, “Through persistent action and competing more effectively below the level of armed conflict, we can influence the calculations of our adversaries, deter aggression, and clarify the distinction between acceptable and unacceptable behavior in cyberspace.”[62] In this respect, CYBERCOM seems to have more in common with U.S. Special Operations Command (SOCOM) than either of its former homes in U.S. Strategic Command (STRATCOM) or the National Security Agency (NSA). STRATCOM controls the nation’s nuclear deterrent, which is most successful when advertised but never used; the NSA is a signals intelligence agency, which is most successful when used but never advertised. SOCOM, by contrast, combines diplomatic communications and military operations by building up the military capacity of foreign partner forces and conducting sensitive unilateral activities to shape the environment. Somewhat like SOCOM, but without any commandos, CYBERCOM works with partners outside the U.S. government (the tech industry and information security community) to build cyber security capacity and operates discretely to shape the information environment.

[61] E.g., Michael P. Fischerkeller and Richard J. Harknett, “Deterrence Is Not a Credible Strategy for Cyberspace,” *Orbis* 61, no. 3 (January 1, 2017): 381–93, https://doi.org/10.1016/j.orbis.2017.05.003; Richard J. Harknett and Max Smeets, “Cyber Campaigns and Strategic Outcomes,” *Journal of Strategic Studies* (Published online, March 4, 2020): 1–34, https://doi.org/10.1080/01402390.2020.1732354; United States Cyberspace Solarium Commission, *Report* (Washington, DC: U.S. Cyberspace Solarium Commission, March 2020).

[62] U.S. Cyber Command, *Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command*, March 2018, https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf.

What is at stake in determining whether cyber security is "really" intelligence or not? The rectification of terms is always a fraught enterprise. Definitional debate often says more about discursive politics than strategic inquiry. One might reasonably wonder if this is all just a rebranding exercise to help a fledgling organization find its footing in a crowded bureaucratic arena. CYBERCOM is a unified military command that was extruded from, and still cohabitates with, the NSA. Both organizations share the same "dual-hatted" commander and CYBERCOM remains dependent on the NSA's technical expertise. Yet most CYBERCOM personnel would insist that they are conducting military operations, not simply providing supporting intelligence or even covert action, which would be outside the U.S. military's (Title 10) purview. In the military worldview, intelligence is a supporting function that assists the operational commander. Commanders use operational forces to create military and political effects, while intelligence aids with targeting and assessment. The creation of CYBERCOM embodies a military tendency to elevate operations over intelligence.

Classic organization theory holds that organizations seek resources, autonomy, and control, guided by their historical cultural heritage or identity.[63] For military organizations, this translates into a predilection for offensive doctrines that require expensive resources and provides expanded authorities, enabling them to set the tempo

[63] E.g., Philip Selznick, *The Organizational Weapon: A Study of Bolshevik Strategy and Tactics* (Santa Monica, CA: RAND Corporation, 1952); James G. March and Herbert A. Simon, *Organizations* (New York: John Wiley and Sons, 1958); Graham T. Allison and Morton H. Halperin, "Bureaucratic Politics: A Paradigm and Some Policy Implications," *World Politics* 24, no. S1 (April 1972): 40–79, https://www.jstor.org/stable/2010559.

and reduce uncertainty, which reinforce and are reinforced by a warrior ethos.[64] The U.S. Air Force is a useful example in this regard. Even when formally part of the U.S. Army, airmen developed their own doctrine — strategic bombing — that was supposed to deliver victory independently of the other services.[65] The ideology of strategic bombing served the Air Force well in its formative years as an independent service, even if the theory often proved disappointing in practice.[66] CYBERCOM's new doctrine of "persistent engagement" and "defend forward" plays a similar institutional role as strategic bombing did for the Air Force. New ideas about cyber operations, and accompanying authorities to carry them out, are intended to enable CYBERCOM to create strategic effects. This means the CYBERCOM has the potential to act beneath the threshold of war without the involvement of other services, or in a supported rather than supporting role. The doctrine of persistent engagement thereby helps a new military organization to do what is inclined to do anyway: enhance its autonomy, influence, and control within a competitive bureaucratic environment.

The United States makes important legal distinctions between intelligence collection, covert action, and military operations, special or otherwise. But this is a 20th century

[64] Jack L. Snyder, *The Ideology of the Offensive: Military Decision Making and the Disasters of 1914* (Ithaca, NY: Cornell University Press, 1984); Barry R. Posen, *The Sources of Military Doctrine: France, Britain, and Germany between the World Wars* (Ithaca, NY: Cornell University Press, 1984).

[65] Phil Haun, ed., *Lectures of the Air Corps Tactical School and American Strategic Bombing in World War II* (Lexington, Kentucky: University Press of Kentucky, 2019).

[66] Robert Anthony Pape, *Bombing to Win: Air Power and Coercion in War* (Ithaca, NY: Cornell University Press, 1996).

development. Many other countries still do not make such bright distinctions.[67] It is also understandable that the operational impulses that eventually gave rise to CYBERCOM would not sit well in an intelligence agency like the NSA, which was founded on passive signals intelligence collection. It is easy to take the NSA's prowess in exploiting computer networks for intelligence for granted, but initially this innovation was controversial within Fort Meade.[68] Nevertheless, many intelligence agencies have become involved not only in espionage but also in covert action, counter-intelligence, and ancillary activities like policing and prisons.[69] Once again, the distinctions between CYBERCOM and the NSA, or between covert action and intelligence collection, might say more about the institutional context of intelligence and cyber security in the United States than the intrinsic definition of either one.

What Is Intelligence?

This raises the question of how to define "intelligence," such that cyber security might, or might not, be an instance of it.[70] Michael Warner, in his contribution to this symposium,

[67] Michael Warner, "A Matter of Trust: Covert Action Reconsidered," *Studies in Intelligence* 63, no. 4 (December 2019): 33–41, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol-63-no-4/pdfs/Covert-Action-Reconsidered.pdf.

[68] Craig Wiener, "Penetrate, Exploit, Disrupt, Destroy: The Rise of Computer Network Operations as a Major Military Innovation" (Ph.D. diss, George Mason University, 2016).

[69] Mark Stout and Michael Warner, "Intelligence Is as Intelligence Does," *Intelligence and National Security* 33, no. 4 (June 7, 2018): 517–26, https://doi.org/10.1080/02684527.2018.1452593.

[70] Conceptual consensus is elusive in the intelligence studies field, e.g., Len Scott and Peter Jackson, "The Study of Intelligence in Theory and Practice," *Intelligence and National Security* 19, no. 2 (June 1, 2004): 139–69, https://doi.org/10.1080/0268452042000302930; Peter Gill and Mark Phythian, "Developing Intelligence Theory," *Intelligence and National Security* 33, no. 4 (2018): 467–71,

likens intelligence to a shadow or a horizon — always present but impossible to grasp. Intelligence operations are transgressive by nature: They cross protected boundaries, break established laws (at least those observed by the target), and subvert established systems. Small wonder that intelligence refuses to be contained by a definition.

Warner, who has served as an official historian with the Central Intelligence Agency, the NSA, and CYBERCOM, has probably done more than anyone to bring some clarity to the murky notion of intelligence.[71] Warner highlights three essential features. First, intelligence traffics in secrecy and deception, which distinguishes it from other information practices with superficially similar methodologies like scholarship, data science, journalism, or marketing. Intelligence deals in either secret means or secret ends, clandestine sources and methods that can support overt information requirements, and open-source intelligence that can support hidden motives. Second, intelligence can produce strategic effects, usually by enhancing or guiding other military or diplomatic activities. Intelligence provides information to inform targeting and policy and provides a few additional covert options in war and peace. Covert action and counter-intelligence should be considered properly part of intelligence, even if they are missing from the canonical intelligence cycle and even if legal institutions distinguish them in practice.

https://doi.org/10.1080/02684527.2018.1457752; Gregory F. Treverton, "Theory and Practice," *Intelligence and National Security* 33, no. 4 (June 7, 2018): 472–78, https://doi.org/10.1080/02684527.2018.1452596; Hamilton Bean, "Intelligence Theory from the Margins: Questions Ignored and Debates Not Had," *Intelligence and National Security* 33, no. 4 (June 7, 2018): 527–40, https://doi.org/10.1080/02684527.2018.1452544.

[71] Michael Warner, "Wanted: A Definition of 'Intelligence,'" *Studies in Intelligence* 46, no. 3 (2002), https://apps.dtic.mil/dtic/tr/fulltext/u2/a525816.pdf; Michael Warner, "Fragile and Provocative: Notes on Secrecy and Intelligence," *Intelligence and National Security* 27, no. 2 (April 1, 2012): 223–40, https://doi.org/10.1080/02684527.2012.661644.

Third, Warner emphasizes that intelligence is sovereign activity, usually but not necessarily conducted by state intelligence agencies. In my opinion, this is the weakest of Warner's criteria, because sovereignty itself is such a problematic concept and because nonstate actors (firms, insurgencies, criminal syndicates, etc.) employ deceptive tradecraft to collect information and influence rivals on the sly. To quote the title of one of Warner's articles, "Intelligence is as intelligence does."[72] It is helpful to understand Warner's third criteria a bit more broadly in terms of "statecraft," which encompasses the political, economic, and military activities that any autonomous actor conducts to survive and thrive in a competitive environment, and not simply "states." In this sense, even al-Qaeda and the Cosa Nostra engage in statecraft by building up military power, establishing alliances, and engaging in skullduggery. To express Warner's criteria more compactly, we might define intelligence simply as *secret statecraft*.

Cyber security may look new, but it is essentially a digital manifestation of secret statecraft. Chinese economic espionage, Russian active measures, U.S. military disruption, and North Korean fraud all use cyber means for political ends. All types of offensive cyber operations, and much of network defense, rely on deception to collect data or exert influence.[73] Yet the same classic intelligence practices, now practiced by new actors, have received new names. Corporate IT departments, for instance, are actively reinverting the art of counter-intelligence as "network security monitoring" or "threat hunting." Some of this evolution is occurring within classical intelligence agencies, as when the NSA transitioned from passive signals intelligence to active cyber exploitation. Much of cyber

[72] Stout and Warner, "Intelligence Is as Intelligence Does."

[73] This argument is developed further in Erik Gartzke and Jon R. Lindsay, "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace," *Security Studies* 24, no. 2 (2015): 316–48, http://dx.doi.org/10.1080/09636412.2015.1038188.

security in the wild, however, is an example of convergent evolution: Dolphins look like sharks because they are both marine predators, but their common ancestor is exceedingly remote. Likewise, in modern cyber security, new actors are responding to the same functional imperatives for intelligence and counter-intelligence that have long motivated state agencies. To take just one example: The Citizen Lab at the University of Toronto, which seeks to expose the intelligence activities of states targeting civil society, has itself taken on many of the trappings of a sensitive compartmented information facility, with physical access controls, compartmented data, and regular security audits.[74] Other academic information security laboratories have reinvented counter-intelligence tradecraft as they study cyber criminals who do not want to be studied.[75] Cyber security should thus be understood in this general sense as intelligence — by, with, and through digital systems. As the ongoing digital revolution reduces the costs of gathering and using information, more actors (and more types of actors) have new opportunities to practice intelligence (or become intelligence targets).

The Question of Scale

When does a difference in degree become a difference in kind? Joshua Rovner argues that "Ongoing competition in cyberspace is largely an intelligence contest. Although the technology is different, the underlying contest exhibits all the characteristics of traditional spy-versus-spy battles."[76] According to Warner, however, "The technology of

[74] Ronald J. Deibert, *Black Code: Inside the Battle for Cyberspace* (Toronto: McClelland & Stewart, 2013).

[75] Chris Kanich et al., "No Plan Survives Contact: Experience With Cybercrime Measurement" (Workshop on Cyber Security Experimentation and Test, San Francisco, 2011).

[76] Joshua Rovner, "The Intelligence Contest in Cyberspace," *Lawfare*, March 26, 2020, https://www.lawfareblog.com/intelligence-contest-cyberspace.

cyberspace seems to be producing something unexpected: operations and effects that resemble covert actions but are much larger in their scale and reach."[77] Traditional conspiracies and espionage rings were limited in their scale. The more people involved and the more ambitious their reach, the more likely they would be compromised. Since secrecy is necessary to intelligence, compromise was a limiting factor on the scale of intelligence. Yet Warner argues that "cyberspace seems to have fixed covert action's problem of scale."[78] The ubiquity of information technology appears to make collection and influence cheaper, easier, and less risky. Scale gives more actors the opportunity to participate in activities that previously might have required some governmental black chamber. Scale also gives actors the opportunity to achieve new kinds of effects, such as tailoring messages for millions of different users, that were simply impossible before. For this same reason, Richard Harknett and Max Smeets resist the reduction of cyber security to intelligence, preferring instead to describe cyber campaigns as a novel way of achieving strategic effects beneath the threshold of armed conflict.[79]

I believe that Warner and others are onto something by highlighting the importance of scale. I have also argued that the scale of a cyber operation or its target condition many of the features that are often ascribed categorically to cyberspace.[80] For instance, the attribution problem — the difficulty of identifying the actor responsible for a cyber attack — is hard only when there are many potential culprits and the victim is not willing to invest in an investigation. When there are only one or two actors with the requisite

[77] Warner, "A Matter of Trust," 39–40.

[78] Warner, "A Matter of Trust," 38.

[79] Harknett and Smeets, "Cyber Campaigns and Strategic Outcomes."

[80] Jon R. Lindsay, "Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence against Cyber Attack," *Journal of Cybersecurity* 1, no. 1 (2015): 53–67, https://doi.org/10.1093/cybsec/tyv003.

capability and damning circumstantial context, then the attribution problem is easier to solve. Similarly, offense has the advantage, and deterrence tends to fail, only when it is easy to plan an intrusion and the consequences of failure are scant, not when targets are politically sensitive and technologically complex. These scale effects tend to drive cyber operations toward the lower end of the conflict spectrum, where deterrence (in any domain) is less credible.

Yet the scale of technological operations does not necessarily alter the basic political logic of intelligence. Intelligence employs deceptive tradecraft to collect information, exert influence, and protect against deception by deceiving the deceivers. I use the terms "intelligence" and "deception" very broadly here, even as there are good practical reasons to use more restrictive definitions in many institutional and legal contexts. The broad terms point toward a set of political strategies that are distinct from war, coercion, and peace. Whereas defense explicitly resists and deterrence explicitly warns, deception encourages the target to voluntarily, yet unwittingly, act against its own interests.[81] More compactly, intelligence is a way of pursuing conflictual ends within cooperative means. The same systems and institutions that enable trust can be subverted and corrupted to abuse trust.[82] Moles masquerade as trusted comrades. Malware masquerades as reliable software. Even "noisy" cyber operations like denial of service attacks still rely on a tactical form of deception, by sending so many legitimate requests to a remote server that

[81] This argument is developed further in Gartzke and Lindsay, "Weaving Tangled Webs"; Jon R. Lindsay and Erik Gartzke, "Politics by Many Other Means: The Comparative Strategic Advantages of Operational Domains," *Journal of Strategic Studies*, Forthcoming.

[82] Reliance on cooperation also constrains the expression of conflict. See Jon R. Lindsay, "Restrained by Design: The Political Economy of Cybersecurity," *Digital Policy, Regulation and Governance* 19, no. 6 (2017): 493–514, https://doi.org/10.1108/DPRG-05-2017-0023.

it becomes overloaded. Benign forms of defensive cyber security also employ deception: Encryption, for instance, disguises valuable data as meaningless noise. Not every cyber operation is intelligence, of course, as clear and open communication is the whole point of many information and communication applications. Yet any form of discrete surveillance, tactical surprise, or dissimulation is, to some extent, an expropriation or reinvention of classic intelligence tradecraft.

Espionage and subversion have been a part of statecraft for millennia, but they have usually been practiced intuitively on the margins of diplomacy and warcraft. Consequently, international relations scholars have traditionally neglected them.[83] The global scale of cyberspace, however, increases the opportunities for deception in all its forms — active and passive, offensive and defensive, simulating or dissimulating, clandestine or covert, etc.[84] It is no longer possible to ignore the role of espionage and covert influence operations in the cyber age. Scale does not make intelligence new, but it makes it newly relevant.

It is difficult to say much definitively about the scale of intelligence operations at this juncture, given the immature state of international relations theory about intelligence. Military operations depend more than ever on intelligence, but we still lack refined concepts to describe the relationship between intelligence and war. Policymakers reach for cyber operations more than ever before, but we still lack refined theory about the conditions for and utility of covert operations. Fortunately, these gaps are being filled

[83] Christopher Andrew, "Intelligence, International Relations and 'Under-Theorisation,'" *Intelligence and National Security* 19, no. 2 (June 1, 2004): 170–84, https://doi.org/10.1080/0268452042000302949.

[84] Barton Whaley, "Toward a General Theory of Deception," *Journal of Strategic Studies* 5, no. 1 (1982): 178–92, https://doi.org/10.1080/01402398208437106.

with a new generation of international relations scholarship on intelligence and covert action.[85] The renewed interest in secret statecraft is inspired in part by the larger profile of digital intelligence operations in global politics. This is good news for students of both intelligence and cyber security. The demand for theory about secret statecraft is increasing at the same time as empirical data about it. Cyber security scholars should embrace an intelligence framing because it expands the pool of comparative cases for them to study.

Conclusion

The growing importance of cyber security in military operations really says more about the increasing role of intelligence in diplomacy and war than it does about the emergence of a new technological domain of warfighting. Nevertheless, a better understanding of the political logic of intelligence is unlikely to change any minds at CYBERCOM. Although cyber conflict is essentially an intelligence contest, the military cyber community has strong incentives to describe it as something else. The dark arts of espionage and subversion have historically played subordinate and supporting roles in military affairs. As the digital revolution enhances their potential, it is understandable that military

[85] See, Robert Jervis, *Why Intelligence Fails: Lessons from the Iranian Revolution and the Iraq War* (Ithaca, NY: Cornell University Press, 2011); Joshua Rovner, *Fixing the Facts: National Security and the Politics of Intelligence* (Ithaca, NY: Cornell University Press, 2011); Keren Yarhi-Milo, *Knowing the Adversary: Leaders, Intelligence, and Assessment of Intentions in International Relations* (Princeton, NJ: Princeton University Press, 2014); Austin Carson, *Secret Wars: Covert Conflict in International Politics* (Princeton, NJ: Princeton University Press, 2018); Lindsey A. O'Rourke, *Covert Regime Change: America's Secret Cold War* (Ithaca, NY: Cornell University Press, 2018); Michael Poznansky, *In the Shadow of International Law: Covert Intervention in the Postwar World* (New York: Oxford University Press, 2020).

practitioners should attempt to redefine them in more familiar terms. Strategic and operational concepts enable a fledgling military organization like CYBERCOM to distinguish itself from both the intelligence community from which it emerged and other military commands with which it competes. In particular, the new doctrine of "defending forward" through "persistent engagement," which aims to create independent strategic effects below the threshold of armed conflict, helps CYBERCOM to make its bureaucratic case for more authorities, resources, and responsibilities.

To be sure, the institutional and operational challenges of scaling up covert action and reconnaissance cannot be underemphasized. The challenges of implementing intelligence at scale are daunting. Military organizations probably have a comparative advantage over boutique intelligence agencies in this regard. Intelligence agencies are specialists in tailored operations to specific political goals, while military organizations have more experience standardizing personnel, processes, material, and logistics for more sustained and global operations. There are also important distinctions in U.S. law governing foreign intelligence activities and military operations. Nevertheless, policy implementation should not be confused with strategic essence. Cyber security is intelligence, even if CYBERCOM is not.

***Jon R. Lindsay** is an assistant professor at the Munk School of Global Affairs and Public Policy and in the department of political science at the University of Toronto. He is the author of* Information Technology and Military Power (*Cornell, 2020*) *and co-editor of* Cross-Domain Deterrence: Strategy in an Era of Complexity (*Oxford, 2019*) *and* China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain (*Oxford, 2015*).

Policy Roundtable: Cyber Conflict as an Intelligence Contest

https://tnsr.org/roundtable/policy-roundtable-cyber-conflict-as-an-intelligence-contest/

Cyber Persistence, Intelligence Contests, and Strategic Competition

Michael P. Fischerkeller and Richard J. Harknett

Cyberspace actions that impact national security are of increasing importance. What is driving states to engage in this behavior? This article examines two alternative sets of explanations — one that argues cyber actions represent strategic competition and another that posits those actions as an intelligence contest. We argue that understanding these cyber actions as "strategic cyber competition" provides greater explanatory power along with better support for sound policy development than thinking about them as intelligence contests. Interestingly, however, the two perspectives do share important common ground, which should not be overlooked when highlighting their differences.

For a better part of two decades, much of cyber theory and policy revolved around the construct of cyber war. In a 2020 article, Richard Harknett and Max Smeets examine the cyber war debate in detail and conclude that "strategy must be unshackled from the presumption that it deals only with the realm of coercion, militarized crisis, and war in cyberspace" because empirically much of state behavior in cyberspace is not captured through the construct of war and coercion.[86] The authors align with the work of Michael Fischerkeller, Michael Warner, and Emily Goldman in arguing that strategic outcomes in, through, and from cyberspace are possible short of war. An alternative view has taken shape principally around the work of Erik Gartzke, Jon Lindsay, and Josh Rovner, who

[86] Richard Harknett and Max Smeets, "Cyber Campaigns and Strategic Outcomes: The Other Means," *Journal of Strategic Studies* (March 2020), https://doi.org/10.1080/01402390.2020.1732354.

argue that the bulk of cyber activity short of war is best understood as anchored on the use of deception and, thus, can be defined as an intelligence contest.

Both perspectives share the common ground that most cyber state activity is not war and agree that states are incentivized to increase this activity. But they differ on classifying the activity (defining it as either strategic campaigns or intelligence operations) and offer rival explanations of why ever-increasing cyber actions do not presage war. In this article, we argue that cyber competitive actions are bounded in a strategic calculus that is reinforced by the structure of the cyber strategic environment itself. Specifically, we conclude that the dynamics of cyber persistence create incentives for the pursuit of cyber *faits accomplis* that are strategic in potential (i.e., they can affect relative state power) yet reinforcing of an agreed competition short of war.

Structure and Deception as Anchors

In previous scholarship we have advanced a structural understanding of cyberspace actions.[87] The logic of cyber persistence derives from the underlying fundamental features of networked computing.[88] Cyberspace is "a global domain within the information

[87] Michael P. Fischerkeller, Richard J. Harknett, and Jelena Vicic, "The Limits of Deterrence and the Need for Persistence," in *The Cyber Deterrence Problem*, ed. Aaron Brantly (Lanham, MD: Rowman and Littlefeld, forthcoming 2020); Michael P. Fischerkeller and Richard J. Harknett, "Deterrence Is Not a Credible Strategy for Cyberspace," *Orbis* 63, no. 1 (Summer 2017): 381–93, https://doi.org/10.1016/j.orbis.2017.05.003. See also, Richard J. Harknett and Emily Goldman, "The Search for Cyber Fundamentals," *Journal of Information Warfare*, 15, no. 2 (Spring 2016): 81–8, https://www.jstor.org/stable/26487534.

[88] Harknett and Goldman, "The Search for Cyber Fundamentals." The logic of cyber persistence aligns with the structural-centric theorizing introduced by Kenneth Waltz, *Theory of International Politics* (New York: MacGraw-Hill, 1979); in Richard J. Harknett and Hasan Yalcin, "The Struggle for Autonomy: A Realist

environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[89] The theory of cyber persistence begins with the recognition that this technical environment rests on a fundamental ordering principle — interconnectedness.[90] To be interconnected means states are in contact with not just adversaries, but with all other actors in this global system. Being structurally derived, this contact is constant. This is in contrast to unit-level (state) behaviorally derived contact that may, for example, be imminent, potential, or episodic. If states technically segment themselves, i.e., leave the interconnected environment, this condition falls away. But to be in an interconnected environment is to be in constant contact.[91]

Structural Theory of International Relations," *International Studies Review* 14 (2012): 499–521, https://www.jstor.org/stable/41804152, the authors modify the Waltzian constructs and argue that anarchy creates the condition of self-reliance and a state imperative to seek autonomy.

[89] Joint Chiefs of Staff, *Joint Publication 3-12: Cyberspace Operations* (Washington, DC: Joint Chiefs of Staff, 2018), https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf.

[90] The notion that cyberspace is global and interconnected is a general default of most policy documents and common parlance, but its theoretical implications have typically been missed. See, White House, *International Strategy for Cyberspace* (Washington, DC: U.S. Government, 2011), https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf. For more on structural concepts, see Harknett and Yalcin, "The Struggle for Autonomy," in which the authors modify Waltzian constructs and argue that anarchy creates the condition of self-reliance and a state imperative to seek autonomy.

[91] Richard J. Harknett, "Reframing the Fundamentals of Cyberspace: CAG Talk 2016," *YouTube*, https://www.youtube.com/watch?v=tA1Uixj44ic.

The nature and substance of the technology itself adds an additional system attribute — global networked computing is a vulnerable and resilient technological system with very low entry costs for core access. The global network represents a global warehouse of and gateway to troves of sensitive, strategic assets that translate into wealth and power. The fact that cyberspace is both vulnerable and resilient creates a distinct dynamic — one can seek to exploit vulnerabilities at scale without fundamental concern over destabilizing the environment. Since the potential for exploitation is ever-present and states are in constant contact due to interconnectedness, they should assume their sources of national power may be vulnerable. From a national security perspective, states should now be concerned that core economic, political, social, and military capability and capacity could be undermined. This elevates the potential of cyber activity to a strategic concern. Thus, a state's only logical choice is to anticipate and proactively mitigate the exploitation of its vulnerabilities in order to be more secure than other states.

The structural imperative for a state thus becomes persistence in seizing the initiative in order to set the conditions of security by exploiting adversary vulnerabilities and reducing the potential for exploitation of its own. If states do not persist, they cannot secure national interest in, through, and from cyberspace.[92]

The theory of cyber persistence argues that cyber strategic competition will primarily play out in the competitive space *short* of armed conflict because there exists a structural imperative for states to act persistently short of armed conflict. Interconnectedness

[92] Michael P. Fischerkeller and Richard J. Harknett, "Persistent Engagement, Agreed Competition, Cyberspace Interaction Dynamics and Escalation," *Cyber Defense Review – Special Edition*, 2019, https://cyberdefensereview.army.mil/Portals/6/CDR-SE_S5-P3-Fischerkeller.pdf.

creates vectors to others' instruments of national power in a technology environment that provides significant opportunities to "exploit user trust and design oversights" within an overall environment of technological resilience.[93] Through significant experimentation, states have discovered that the combination of system resiliency and vulnerability enables the realization of strategic gains through competition via cyber operations and campaigns short of armed conflict, thus presenting a *strategic incentive* for continued activity and further experimentation.[94] We have introduced the construct of "agreed competition" to capture how the interplay of the structural imperative and strategic incentives result in a self-limited cyber strategic competitive space.[95]

Alternatively, proponents of the intelligence contest perspective argue that advantages in cyberspace do not result from "categorical features or attributes of the internet" but from "relative organizational capacity for employing deception and integrating it with broader strategic initiatives." [96] Thus, an actor's capacity for deception is a core feature for explaining state behavior in cyberspace. To gain advantage, this capacity is applied against cyberspace's abundant organic opportunities to exploit its users.[97] Specifically, Jon Lindsay argues that "most cyber operations rely on deception to collect intelligence

[93] To borrow a phrase from Erik Gartzke and Jon R. Lindsay, "Weaving Tangled Webs: Offense, Defense and Deception in Cyberspace," *Security Studies* 24, no. 2 (2015): 316–48, http://deterrence.ucsd.edu/_files/Weaving%20Tangled%20Webs_%20Offense%20Defense%20and%20Deception%20in%20Cyberspace.pdf.

[94] A structural imperative is a theoretically derived absolute, but it does not mean that states can't make bad decisions and suffer the consequences. A strategic incentive is a set of cost/benefit calculations that creates a rationale for a certain set of choices.

[95] Fischerkeller and Harknett, "Persistent Engagement."

[96] Gartzke and Lindsay, "Weaving Tangled Webs."

[97] Gartzke and Lindsay, "Weaving Tangled Webs."

or steal intellectual property, exert influence through propaganda or sabotage, or defend against these activities."[98] Drawing on the field of intelligence studies, Gartzke and Lindsay, together with Josh Rovner, claim that "cyber warfare is not a 'sui generis' phenomenon, but rather a member of a class of phenomena — intelligence and covert operations" and "nothing in cybersecurity makes sense except in the light of intelligence."[99]

In terms of rival explanations, therefore, the proponents of understanding national security-relevant cyber actions as strategic competition emphasize the nature of cyberspace itself as creating an *imperative* to persist over who has initiative in cyberspace reinforced by an *incentive* to pursue sustained initiative since it can yield cumulative gains shifting political, economic, military, diplomatic, and informational power. Those that frame this activity as intelligence contests emphasize that it is the relative capacity to deceive that affords states the potential to exploit an environment ripe with opportunity, which they expect states will use regularly, but supports the achievement of limited gains. Both argue that the majority of cyber operations and campaigns will be conducted in such a manner as to remain below the threshold of what might be considered armed attack or war.

[98] Jon R. Lindsay, "Cyber Espionage," in Paul Cornish, ed., *The Oxford Handbook of Cyber Security* (New York: Oxford University Press, forthcoming), https://drive.google.com/file/d/0B7IN_AGAVuy-WFFFX04yNVVjM3c/view.

[99] Gartzke and Lindsay, "Weaving Tangled Webs," and Lindsay, "Cyber Espionage."

Divergence: Cyber as Strategic Competition or Cyber as Intelligence Contest

The difference in causal explanation noted above leads to a divergence in classification of cyber activity as either potentially cumulative strategic action or primarily as intelligence activity. Intelligence contest scholars argue that computer network operations should mainly be understood as "expanding the scope of intelligence and covert operations" and conclude that cyber warfare "is best understood as low-intensity conflict behavior … rather than as a separate form of strategic warfare."[100] Gartzke asserts that in order for cyber operations to be relevant in "grand strategic terms" or "pivotal in world affairs," they would have to "accomplish tasks typically associated with terrestrial military violence," including deterring or compelling, i.e., generating influence through the prospect of damage or loss, maintaining or altering the balance of power, and resisting or imposing disputed outcomes.[101] Lindsay suggests that the strategic significance of offensive cyber operations would be found in their ability to unambiguously communicate cyber capability and resolve in a coercive bargaining process (deterrence and compellence). Such clear communication is "especially problematic" in cyberspace.[102] The intelligence contest perspective concludes that cyber operations cannot independently generate strategic outcomes.

[100] Gartzke and Lindsay, "Weaving Tangled Webs."

[101] Gartzke and Lindsay, "Weaving Tangled Webs."

[102] Jon R. Lindsay, "Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence Against Cyberattack," *Journal of Cybersecurity* 1, no. 1 (2015): 53–67, https://academic.oup.com/cybersecurity/article/1/1/53/2354517.

It is further argued that the operational needs required to sustain large deceptions in fact create limits.[103] Thus, "deception is useful for only a subset of political aggression, and *it does not scale*," meaning that it cannot easily, if at all, be achieved at greater orders of magnitude to potentially generate strategic political effects.[104] According to the intelligence contest authors, deception's inability to scale is due to inherent constraints on two different axes. First, offensive deception becomes more difficult if the target possesses greater political value. The more important the target, the less likely deception can succeed (i.e., failure to vertically scale). Second, offensive deception constrains pursuing multiple, simultaneous operations against heterogeneous and/or well-defended or higher-value targets because each intrusion requires significant and unique deception efforts (i.e., failure to horizontally scale).[105] Lindsay argues that "deception will be more useful for pursuing some positive benefit today … rather than coercively threatening harm tomorrow."[106] Two arguments are embedded here: First, the presumption that coercion is the primary route to change, and second, that future gain rather than present gain is a state's preference. Cyberspace is, therefore, enabling a greater scope for intelligence activity, but not by a substantial margin.

There is no dispute that many cyber operations rely on deception and are informed by the traditional practices of intelligence. We contend, however, that advocates of the intelligence contest perspective have adopted the wrong core variables and concepts against which to assess the potential strategic significance of states' cyber behaviors short of armed conflict. It should not be assumed that the only route to strategic gain is

[103] Lindsay, "Cyber Espionage."

[104] Lindsay, "Tipping the Scales."

[105] Lindsay, "Tipping the Scales."

[106] Lindsay, "Tipping the Scales."

through coercion or the potential thereof. Rather, adjusting one's assessment away from coercion to include variables like unilateral gains that cumulatively shift power over time through campaigns allows for the consideration that such campaigns can impact disputed outcomes indirectly. This perspective opens up the analytical aperture of the intelligence contest lens to see that both scale, along with scope, is in play.

Cumulative Cyber *Faits Accomplis*

Cyber persistence theory argues that states abiding by the structural imperative to act persistently will continuously execute campaigns populated by cyber operations short of armed conflict. These campaigns seek to generate cumulative gains to serve desired strategic effects (i.e., to achieve strategic outcomes) over time and space.[107] Further, the theory argues that the security studies construct of the *fait accompli*, rather than coercion, better describes the dominant behavior through which states seek to achieve these gains and effects. Changing the strategic frame from one based on coercive bargaining to the "cyber" *fait accompli* — that is, changing one's focus to immediate gains rather than seeking prospective threat leverage for future action — leads to a conclusion that deception need not act as a constraint on a state's quest to realize strategic effects or outcomes through cyber behaviors short of armed conflict.[108]

[107] For more on the pursuit of strategic effects, advantage and outcomes through campaigns, see Harknett and Smeets, "Cyber Campaigns and Strategic Outcomes."

[108] Cyber persistence theory assumes that all states act in their best interests and thus there is a convergence of behavior above restraint, because restraint means states lose, and war, because war means states sub-optimize cyberspace's novel contribution to strategic competition. The competition that ensues is thus "agreed" behaviorally at first and can become more explicitly agreed as rules of the game or norms of cyber competition emerge. Michael P. Fischerkeller and Richard J. Harknett, "Persistent Engagement and

The *fait accompli* in the cyber strategic environment (henceforth the cyber *fait accompli*) is defined as a limited unilateral gain at a target's expense where that gain is retained when the target is unaware of the loss or is unable or unwilling to respond.[109] This is distinct from its definition as used when describing state behavior in the terrestrial frame,[110] but shares a characteristic that "*faits accomplis* are more likely to succeed at making a gain without provoking war when they take that gain without crossing use-of-force red lines."[111] The empirical record of states' dominant cyberspace behaviors (not already engaged in militarized crises or armed conflict) reveals this very pattern of unilateral cumulative gains being achieved through campaigns short of armed conflict. We have argued that security in a cyber persistent strategic environment rests on retaining the initiative in changing the conditions of security and insecurity. The construct of cyber *faits accomplis* (a pluralization to capture the linkage that can be produced through

Tacit Bargaining: A Path Toward Constructing Norms in Cyberspace," *Lawfare*, November 2018, https://www.lawfareblog.com/persistent-engagement-and-tacit-bargaining-path-toward-constructing-norms-cyberspace.

[109] For a more complete explication of the cyber *fait accompli*, see Michael P. Fischerkeller, "The *Fait Accompli* and Persistent Engagement in Cyberspace," *War on the Rocks*, June 24, 2020, https://warontherocks.com/2020/06/the-fait-accompli-and-persistent-engagement-in-cyberspace/.

[110] For example, Dan Altman says, "The *fait accompli* imposes a limited unilateral gain at an adversary's expense in an attempt to get away with that gain when the adversary chooses to relent rather than escalate in retaliation." Dan Altman, "Advancing Without Attacking: The Strategic Game Around the Use of Force," *Security Studies* 27, no. 1 (2017): 58–88, https://doi.org/10.1080/09636412.2017.1360074.

[111] Dan Altman, "By Fait Accompli, Not Coercion: How States Wrest Territory From Their Adversaries," *International Studies Quarterly* 61 (2017), 881–91, https://www.researchgate.net/publication/322126880_By_Fait_Accompli_Not_Coercion_How_States_Wrest_Territory_from_Their_Adversaries.

coherent campaign activity) can illuminate much of what we are seeing in state cyber behavior. Thus, cyber *faits accomplis* in the cyber strategic environment are not bounded to a limited episodic effect, and, importantly, as we will explain below, those effects are not predominately tied to coercion.

Embracing the cyber *fait accompli* concept instead of coercion, signaling resolve and brinkmanship, opens the aperture for how scholars should understand the political value of cyberspace targets. Rather than presume states equate high political value with future coercive value, the calculus of political value for the cyber *fait accompli* becomes which targets, if exploited, result in positive gains or benefits today.[112] The cyber *fait accompli* can accurately describe and explain states' cyber behaviors short of armed conflict because it accounts for both unilateral operations seeking gains from disparate targets and mutual efforts to routinely avoid operations that could justify armed retaliation.

While the cyber *fait accompli* comprising a single cyber operation short of armed conflict may only generate a limited gain of marginal significance, a cyber campaign comprising cumulative *faits accomplis* executed at scale (horizontally) could generate cumulative gains of potential strategic significance. This path to strategic effects or outcomes doesn't square with the intelligence contest conclusion that offensive deception fails to scale (horizontally) by constraining the pursuit of multiple, simultaneous operations against heterogeneous, well-defended, high-political-value targets. Consider as a case in point the

[112] For a related argument on how cost imposition should be reconceptualized in the cyber competitive space short of armed conflict, see Michael P. Fischerkeller and Richard J. Harknett, "Persistent Engagement and Cost Imposition: Distinguishing Between Cause and Effect," *Lawfare*, Feb. 6, 2020, https://www.lawfareblog.com/persistent-engagement-and-cost-imposition-distinguishing-between-cause-and-effect.

hundreds, if not thousands, of companies targeted by Chinese cyber operators seeking with urgency to illicitly acquire U.S. intellectual property.[113] By pursuing unilateral campaigns at scale (horizontally) against low-complexity, high-political-value targets, states can transition from single operations generating a limited gain or benefit of marginal significance to substantial campaigns generating cumulative gains and, potentially, independently strategic effects or outcomes.

Michael Warner makes a related argument associating opportunities for operating at scale with potential strategic significance. Where covert operations' influence in the past was at "the margins of state practice," that may now be changing because cyberspace allows states to execute covert operations *at scale*.[114] The ability to execute continuous cyber campaigns at scale, he says, allows for individual, marginal effects to aggregate into the class of strategic effects. Thus, whereas covert operations have historically been a secret, supplemental factor in international relations, Warner argues that cyberspace facilitates their functioning through scale as a secret, independent strategic factor.[115]

These arguments are consistent with cyber persistence theory. The empirical record makes clear that an expansion in scope of operations, the only expansion predicted by the intelligence perspective, has been accompanied by an expansion in scale. This

[113] This suggests Lindsay's contention that "it is not very controversial to assume that attacker costs will scale with target value" is, in fact, controversial when considered in light of the cyber *fait accompli* vice coercion-based strategic concepts.

[114] Michael Warner, "A Matter of Trust: Covert Action Reconsidered," *Studies in Intelligence* 63, no. 4 (2019): 33–41, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol-63-no-4/index.html.

[115] Warner, "A Matter of Trust."

expansion results in a difference in kind, not merely degree, and produces a situation defined as a strategic competition, not merely an intelligence contest. Indeed, a recognition of and concerns over adversaries operating "at scale" played an important role in elevating the importance of cyberspace in U.S. Department of Defense thinking.[116] These concerns proved prescient, as nearly every annual U.S. director of national intelligence threat assessment report for the past decade references year-over-year *increases* in scope *and scale* of adversary operations targeting U.S. national interests (and the same can be found in private-sector threat reports).[117] These assessments are not based on theory or abstraction but are reflective of operational ground truth.

The Democratic Peoples' Republic of Korea is an excellent example of a state operating in alignment with the expectations of strategic competition.[118] Their cyber activity is one of linked cyber *faits accompli*s anchored on one primary strategic objective — undermining

[116] William J. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs* 89, no. 5 (Sept./Oct., 2010): 97–108, https://www.jstor.org/stable/20788647.

[117] As bookends, consider the 2010 and 2018 annual threat assessments. Dennis C. Blair, "Annual Threat Assessment of the U.S. Intelligence Community for the Senate Select Committee on Intelligence," *Office of the*

Director of National Intelligence, Feb. 2, 2010,

https://www.dni.gov/files/documents/Newsroom/Testimonies/20100202_testimony.pdf; and Daniel R. Coats, "Statement for the Record: Worldwide Threat Assessment of the U.S. Intelligence Community," *Office of the Director of National Intelligence*, Feb. 13, 2018,

https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf. For an example of private sector reporting, see FireEye's M-Trends reports, https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html.

[118] For a second example focusing on China, see Michael P. Fischerkeller, "Opportunity Seldom Knocks Twice: Influencing China's Trajectory via Defend Forward / Persistent Engagement in Cyberspace," *Asia Policy Journal* (forthcoming October 2020).

the "toughest and most comprehensive sanctions regime ever imposed" imposed by the U.N. Security Council via resolution 2321 (2016). North Korean cyber activity is best understood as an example of a state employing a cyber campaign to achieve a strategic gain and, in doing so, resist a disputed outcome.[119] North Korean leadership responded to the international community's challenge through persistent military exploitation of the international banking system in and through cyberspace and other financial digital manipulation. In August 2019, the United Nations Panel of Experts charged with assessing the efficacy of the sanctions concluded that North Korea generated an estimated $2 billion for its weapons of mass destruction programs through "sophisticated use … of cyber means to illegally force the transfer of funds from financial institutions and cryptocurrency exchanges, launder stolen proceeds and generate income in evasion of financial sanctions."[120]

In August 2020, the United States released a joint alert that detailed the continuing North Korean cyber campaign that directly disputed the sanctions through financial digital manipulation of ATM banking.[121] The targets of highest political value for the regime are those that facilitate the acquisition of currencies today, not those that might provide future coercive value. Moreover, these efforts are resulting in strategic effects and outcomes that are arguably pivotal to world affairs — undermining strategic objectives of

[119] United Nations, "Security Council Strengthens Sanctions on Democratic Republic of Korea, Unanimously Adopting Resolution 2321 (2016)," *United Nations*, Nov. 30, 2016, https://www.un.org/press/en/2016/sc12603.doc.htm.

[120] United Nations, "Report of the Panel of Experts Established Pursuant to Resolution 1874 (2009); S/2019/691," Aug. 30, 2019, https://undocs.org/S/2019/691.

[121] U.S. Joint Agency Release, "Joint Technical Alert: FASTCash 2.0: North Korea's BeagleBoyz Robbing Banks," Aug. 26, 2020, https://us-cert.cisa.gov/ncas/alerts/aa20-239a.

both the United Nations and the United States while bolstering a particular state's nuclear capability. Nuclear weapons development, busting U.N. sanctions, and undermining U.S. compellence strategy are not the effects of merely deceptive intelligence operations. They are sophisticated strategic objectives and outcomes sought and produced through cyber means that include deceptive tactics and capabilities.

In 2018, U.S. Cyber Command shifted to a cyber doctrine of persistent engagement that aligns with the expectations of cyber persistence and operationalizes U.S. national strategic guidance denoting cyber activity below the threshold of armed attack as strategic in nature. The combination of "hunt forward" missions linked to public outing of adversaries' malware and techniques and much closer cooperation with the private sector in order to anticipate the exploitation of vulnerability before it occurs is reflective of what persistent operations can cumulate toward — it reflects cyber-based strategic competition.[122] Persistent engagement reaped results in countering the North Korean activities noted above when in August 2020 U.S. Cyber Command supported the U.S. Department of Justice in isolating cryptocurrency accounts used to launder money North Korea had stolen — seizing the initiative back from North Korea in this cyber strategic competition.[123]

[122] See Paul M. Nakasone and Michael Sulmeyer, "How to Compete in Cyberspace: Cyber Command's New Approach," *Foreign Affairs*, Aug. 25, 2020, https://www.foreignaffairs.com/articles/united-states/2020-08-25/cybersecurity.

[123] Spencer Hsu, "US Cyber Command Helps Prosecutors Seize Stolen Cryptocurrency Traced to Illicit North Korea Nuclear Weapons Program," *Washington Post*, Aug. 28, 2020, https://www.washingtonpost.com/local/legal-issues/us-cyber-command-helps-prosecutors-seize-stolen-cryptocurrency-traced-to-illicit-n-korea-nuclear-weapons-program/2020/08/28/12e7959c-e886-11ea-970a-64c73a1c2392_story.html.

Conclusion

Both explanatory frameworks — cyber as strategic competition and cyber as intelligence contest — conclude that cyber competition will primarily play out in a self-limited cyber competitive space short of armed conflict. The two frameworks also agree that escalation is not the dominant strategic interaction dynamic in the cyberspace strategic environment — conclusions supported by the empirical record of reported operations between states not already engaged in armed conflict. This common conclusion is important to note. But the difference in explanation is not a simple academic debate as the two frames offer very different prescriptive paths.

To see cyberspace actions as strategic competition does not necessitate losing the important observations that can flow from seeing an intelligence contest nested within that strategic competition. While convergence of theoretical perspectives is not common in international relations theory, accepting the importance of deception within the context of strategic intent and interaction is worth further study that could advance the subfield of cyber strategic studies. Admittedly, that is not the case in reverse. Seeing an intelligence contest at work unnecessarily narrows both the scope of study and the range of prescription in this vital security area. Thus, it is not simply the greater explanatory relevance of strategic competition that matters here, but also the potential for the one frame (intelligence contest) to inform and strengthen the explanations that emanate from the strategic competition framework. Moving forward, we would advocate for adapting those insights into strategic competition explanations rather than pursuing intelligence contest as a standalone rival explanation.

Policy Roundtable: Cyber Conflict as an Intelligence Contest

https://tnsr.org/roundtable/policy-roundtable-cyber-conflict-as-an-intelligence-contest/

Michael P. Fischerkeller *is a research staff member in the Information Technology and Systems Division at the Institute for Defense Analyses.*

Richard J. Harknett *is professor and head of the Department of Political Science, chair of the Center for Cyber Strategy and Policy, and co-director of the Ohio Cyber Range Institute at the University of Cincinnati.*

Cyber Conflict as an Intelligence Competition in an Era of Open Innovation

Nina Kollars

Last year I got a parking ticket for lingering too long in a limited zone. Parking tickets are not sufficient reason to declare war on a city's thinly veiled vehicular taxation scheme for the absentminded. And yet I wanted to.

So instead of dutifully filling out the online payment form, I started searching for ways to make my payment submission equally tedious and arbitrary. I envisioned mailing $60 worth of pennies originally intended for the Coinstar. But I was stymied: They'd hidden the physical mailing address on their website.

What they failed to hide, however, was just about everything else. After clicking around, I discovered unfettered access to all the other tickets issued through the city's online payment system, complete with time, date, car data, and the name of the parking enforcement officer who issued each ticket. Technically, parking tickets are public data. But these weren't just a few lines of data: They were photographs of everyone's cars, value of the tickets, license plates — anything a person would need to conduct open-source intelligence on the ticketed and ticketers alike.

If intelligence competitions are about "intel" — data, information, and the knowledge one can glean from it — then cyber actions, as agreed upon by this roundtable of thinkers, are decidedly an intelligence competition. What no one has argued thus far, however, is how this competition is just as much about nonstate actors as it is about states. States are not the primary agents in cyberspace. Nor are they the primary players conducting intelligence competitions within the cyber domain. That domain is a collective space in which tech firms, individuals, informal group hacking collectives, and citizen-led counter surveillance organizations coexist, confound, conflict, and collide to the detriment of all.

The internet is a sociotechnical construction — part machine, part human, part cat meme. It is an ever-churning, belching, and expanding mass of connectivity, data-capable devices, data-collecting devices, and data storage devices. It extends from my back pocket to your refrigerator, Poughkeepsie's municipal parking ticket database, the president's iPhone, and a PlayStation 4 streaming on Twitch. The cyber competition between states debated by my colleagues is a subcomponent of a melee-style grindhouse where nonstate actors complicate the capacity of states to dominate cyber interactions.

My colleagues acknowledge the importance of nonstate actors in cyberspace. Jon Lindsay argues that the nonstate world influences and also emulates the elements occurring in state-on-state intelligence interactions. Joshua Rovner's five elements of an intelligence contest needn't necessarily be constrained to states: They contain generalizable reasoning for analyzing adversarial behavior. Rovner really only narrows the scope when he defines an intelligence contest as "part of an open-ended competition among rival states."[124] Even Richard J. Harknett and Michael P. Fischerkeller do not deny the agency of nonstate actors in their interpretation of persistent engagement.[125]

[124] Joshua Rovner, "Cyber War as an Intelligence Contest," *War on the Rocks*, Sept. 19, 2019, https://warontherocks.com/2019/09/cyber-war-as-an-intelligence-contest/.

[125] Even if they derive their analytical frame from the roots of international relation's structuralist tradition, channeling Waltz, who gave analytical priority to states out of theoretical parsimony. Kenneth Waltz, *Theory of International Politics* (Reading, MA: Addison-Wesley Publishing Company, 1979).

It is only Michael Warner — the historian — who declares allegiance to the unique status of states by defining intelligence as a "sovereign" affair, noting "that intelligence is that set of activities, when we consider strategic purposes, that is both secret and sovereign."[126] Sovereign, in Warner's sense and in most security research contexts, is the state.

My intent is to play on a second meaning of sovereign — as one who is not subject to a ruler. Scholarship on cyber competitions between states is often analytically hide-bound to the traditional elements security scholars are accustomed to looking at. We are driving with the rearview mirror.[127] According to Lindsay, we may accidentally be learning "more about the institutional context of intelligence and cyber security in the United States than the intrinsic definition of either one."[128] I will aim to keep us pressed up firmly against the

[126] Now again we begrudgingly (with much footnoted and highly caveated pain) lend the label of "sovereign" to a murky and dubious catch-all term called the "armed nonstate actor," by which we usually mean entities vying for state-like autonomy. And then, with eyes cast down, we recall being chastened by Cold War-era international relations theorizing — and we retreat skulking back into the loving arms of our favorite concept — the state. States are, as we are doggedly taught, the real sovereigns ever since the Treaty of Westphalia. And yes, sometimes there are oddities like al-Qaeda or the Islamic State. But we are mostly calmed when we can re-simplify all the way back to roughly 239 agents, but more likely just five or ten "great powers."

[127] I borrow the phrase here from Wendt's work; this reference is about the development of future organizations and institutions. Alexander Wendt, "Driving with the Rearview Mirror: On the Rational Science of Institutional Design," *International Organization* 55, no. 1 (Autumn 2001): 1019–49, https://doi.org/10.1162/002081801317193682.

[128] I will also bear in mind Lindsay's remarks about wineskins undiscovered that could be refilled and hopefully have some potential wine to stuff into them someday.

windshield, a few millimeters from the world, as our empirical cases comes at us like tiny gnats hitting the glass. In doing so, I will refuse my colleagues the benefit of the mirrors and the rear window for just these few pages because these are my pages, and herein I will play — like a crazed Feyerabend — because it is my right.[129]

I will drag this conversation downward, away from the rarified air of international relations theories, codified practices of spy craft, and historical referents that emphasize either state power or state intelligence systems. Instead, I will point to three general truths (though there are likely many more) that confound the usefulness of giving states analytic primacy in the intelligence competition in cyberspace. These truths are: the proliferation of data-generating consumer electronics and services; the proliferation of tools that enable capture, analysis, and use of data; and the inevitable clash of competing interests for all that data.

Connecting Cheap = Data Rich

The state monopoly in targeted and mass data collection is over. For at least three decades, and perhaps longer, the sophisticated tools necessary to surveil targets and analyze mass data have proliferated in the public sphere, often disguised as consumer services and products: Amazon Alexa, Nest, Wi-Fi-enabled Barbie, Keurig coffee makers, and anything that has a radiofrequency identification (RFID) chip in it.[130]

[129] I place the blame firmly on Dr. Ted Hopf for making me read iconoclasts in methods classes. Paul Feyerabend, *Against Method* (New York: Verso, 1993).

[130] YokoAhava, "What's the Purpose of the Phone Jack on the Keurig 2.0?," *Reddit*, 2015, https://www.reddit.com/r/keurig/comments/2qfop3/whats_the_purpose_of_the_phone_jack_on_the_keurig/.

The global appetite for connecting ourselves and our objects has produced vast swaths of data that make it easy to track, trace, and understand others as targets and at scale. Connective devices present a simple trade-off: Pay less now, and give up your data in exchange. Happily we connect, sending our data zooming out into who knows where, stored however, and kept for … hard to say, really. And, yes, the NSA and associated Five Eyes countries have pathways into these data troves, but let's be clear about the nature of this relationship: Governments are negotiating and breaking in behind the scenes. They are not the owners or managers of this data.

Independent Researchers = NSA Exquisite Tools? Nah, I'm Good …

While the United States and its allied intelligence agencies certainly hold the premier tools and access to sensitive or valuable data, exquisite tools aren't necessary for cyber competition. With all this data flying around, all it takes is an enterprising coder to access and organize it. In the 21st century, government data leaks tend to come in two flavors: leakers tapping into the existing streams of government data — the Snowden types — and researchers finding openly available data on the internet and innocently pointing to it. Individuals and small teams can aggregate masses of data by leveraging cheap tools and moderate expertise.

While the first is a matter of government employee management and malice, the second is a fact of the new era and is both legal and often fabulously political. Military bases suddenly became findable via heat maps of Strava fitness tracker data.[131] Industrial control systems of faraway places are findable via the search engine Shodan. These systems are more than simply findable; they're also manipulatable, as hacker Dan Tentler discovered — his work on Shodan revealed traffic control systems, ice rinks in Denmark, and a French hydroelectric plant that he could manipulate from his desktop.[132] If fitness trackers and industrial control systems are too rich for your technical expertise, don't worry — there's an app you can download to spy on people's cell phone locations. Yes, that includes the iPhone, for all you Android haters out there. There's actually a competitive market for free spyware, just as long as you offer up more data.[133]

Spaghetti Politics

Spying is everyone's game now. It is effectively the intelligence version of Audrey Kurth Cronin's "use of force" argument in *Power to the People*.[134] Cronin argues that militaries prefer that the diffusion of military capabilities be kept under their control. But sometimes social change and adoption overtakes the state's ability to maintain that monopoly — the democratization of violence, as it were.

[131] Jeremy Hsu, "The Strava Heat Map and the End of Secrets," *Wired*, Jan. 29, 2018, https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/.

[132] David Goldman, "Shodan: The Scariest Search Engine on the Internet," *CNN Business*, April 8, 2013, https://money.cnn.com/2013/04/08/technology/security/shodan/index.html.

[133] Komando Staff, "5 Smartphone Spy Apps That Could Be Listening and Watching You Right Now," *Kim Komando*, June 5, 2017, https://www.komando.com/privacy/5-smartphone-spy-apps-that-could-be-listening-and-watching-you-right-now/362160/.

[134] Audrey Kurth Cronin, *Power to the People: How Open Technological Innovation Is Arming Tomorrow's Terrorists* (Oxford: Oxford University Press, 2019).

Cyber and intelligence is particularly befuddling because of its spaghetti nature — interconnected, overlapping, and messy. While states would prefer it be left to geographic boundaries, the interests of businesses, individuals, and governments don't align consistently, or predictably, with national borders. Some telecommunications firms cooperate with states while others don't. Some electronics manufacturers privilege consumer privacy. Others do not. Hacking collectives like Anonymous wax and wane in their political views every four or five operations. If the lines of effort were distinct in some way, then states could compete with one another while everybody else could play their own game. But lines of effort are not that clear-cut. All of Rovner's five elements of an intelligence competition occur inelegantly, confoundingly, on top of one another, throughout the broader context of the greater global competition for data.[135]

In 2018, as Amazon negotiated with the Pentagon on a contract for its JEDI cloud software, WikiLeaks published a global map and a 20-page internal memo of the company's Web Services operating facilities and data colocation sites.[136] In short, WikiLeaks doxed Amazon.[137] While it was unclear who leaked the information, WikiLeaks had been in a standoff with Amazon and other global data management companies for years. The situation was problematic for Amazon, which would have preferred those sites

[135] Let me start first by saying there's something in an academic that loves lists and parameters. And Rovner, in giving us a list, is doomed to fame for it. I am grateful for his willingness to set the anchoring parameter from which I will tether and proceed to deviate.

[136] Jason Murdock, "WikiLeaks Has Published What It Says Is a 'Highly Confidential' Document Revealing Amazon Secrets," *Newsweek*, Oct. 11, 2018, https://www.newsweek.com/wikileaks-publishes-allegedly-highly-confidential-amazon-document-1165031.

[137] Doxing is the act of revealing private information about a company or person with malicious intent.

go unnamed; for the Defense Department, which was in the process of finding a cloud management system; and for anyone whose data may be stored in those highly sensitive sites, which (given Amazon's profile in data storage) could include large portions of the global population. The conflict is cross-cutting and extremely political, and it created political blowback at every level. To be clear, it isn't just states that are actively trying (covertly or openly) to shut down WikiLeaks' capacity to publish data. The standoff here is a triad between the state, data center managers who hold all sorts of secrets — legal, financial, military, and political — and WikiLeaks's own survival. WikiLeaks is pursuing its own political agenda collecting, analyzing, and using intel to (in Rovner's words) "to undermine adversary morale, institutions, and alliances."

These aren't rare cases. Data the Defense Department would consider highly sensitive (and would likely classify) is readily collectable and analyzable. A new study of the novel coronavirus has emerged from an organization called Govini, which specializes in data science analysis for national-level problems. The report and the publicly available map titled *COVID-19 Impacts on the Department of Defense* illustrates COVID outbreaks across the United States and identifies which U.S. military bases are at risk, utilizing bullet points for readiness, power projection, and modernization.[138] The caption under the map reads:

> Govini used its decision science and machine learning platform to analyze COVID-19 infection growth rates, medical facilities, contractors, defense

[138] Marcus Weisgerber, "Coronavirus Is Rising Around US Military, Defense Infrastructure, Analysis Shows," *Defense One*, March 30, 2020, https://www.defenseone.com/threats/2020/03/coronavirus-rising-around-us-military-defense-infrastructure-analysis-shows/164208/.

> supply chains, place of performance, and military installations to provide this prognostic view. The map highlights in red those areas where companies in the Defense Industrial Base are particularly vulnerable to COVID-19. For more information contact info@govini.com.[139]

A few things to note. First, it is highly unlikely that this sort of analysis would have been conducted so quickly by any agency within the Defense Department. Second, even if this sort of analysis was eventually done inside the Defense Department, the classification levels associated with this kind of heat map would ensure that almost no one within the department would be able to read it or distribute it (particularly under current conditions, where most civilian staff telework due to the novel coronavirus and lack access to secure email and the browser network system). But more importantly, the competitive business environment among data analysis agencies selling their wares to the Defense Department involves getting noticed and getting contracts before other analysis firms. The primary way to do this is to publish reports and analysis publicly, even if it makes the Defense Department nervous.

The private sector is faster, less constrained, and more agile with these tools of mass analysis. It is unclear how the Defense Department can keep up.

[139] "COVID-19 Impact on the Department of Defense," *Govini*, 2020, https://www.govini.com/wp-content/uploads/2020/03/Govini-DoD-COVID19-Impact.pdf.

Your Coffee Maker Is Spying Too

Let's consider the firms that are producing internet-enabled technologies for mass consumption. In 1998, Keurig (owned by Keurig Dr. Pepper) began producing coffee pods and brewers. Four years ago, I bought a base model Keurig with almost no functionality — the cheapest possible one — for approximately $50. When you turn the machine over, you will notice an internet port. There is no *current* function for this port. However, Keurig designed these ports into their coffee makers in anticipation of future market developments. Rather than remold the machine or provide new production specifications for that port, Keurig opted to design it into the machine in order to ensure future capabilities should they emerge.

Perhaps this example is too cute by half. Or perhaps it is an example of a firm thinking strategically and emplacing data collection capabilities to ensure future competitiveness. While it is definitely not (in Rovner's words) "a campaign to pre-position assets for future collection in the event of a conflict," it is a case of a pre-positioning that consumers generally cannot detect.

This matters in real terms for national security. One of the most disruptive denial of service attacks in history — the Mirai botnet — leveraged tens of thousands of internet-connected devices against the domain name service provider Dyn in October of 2016.[140] The diffusion of IOT (Internet of Things) devices becomes its own vulnerability, as they are sold cheap and purchased by the millions. IOT attacks can be leveraged by a simple

[140] DNS providers are the naming system for the internet. They are effectively its phonebook, connecting names to IP addresses. When you DDOS a DNS provider, you interrupt that matching of names to numbers.

handful of actors and then reused by a whole other set of actors for other purposes. The Mirai botnet wasn't the first time that code had been leveraged. It had a predecessor: A prior attack had been conducted on a slightly smaller scale (though still 100 times larger than any other in history) on OVH, a cloud computing provider in France in September 2016. The origins of the malware and the OVH attack had nothing to do with states, violent extremist organizations, or even criminal syndicates. The OVH attack was conducted by three U.S. students playing a game called Minecraft.[141] The savvy undergraduates assembled malware that would rock the East Coast and leave intelligence agencies scrambling. That initial piece of malware continues to plague the internet.

For the three students involved, the malware was intended to sabotage other Minecraft hosting sites, causing an increase in traffic and therefore increasing their income collecting from that traffic. It was easily "a contest to disable adversary capabilities through sabotage." Once that malware was publicly shared, plenty of other malicious actors took up the tool to use it for additional acts of sabotage.

Conclusion: Moving Beyond States

The tools of intelligence competition are available to everyone. The battle space for intelligence competitions grows by the minute. The holders of the tools and the space itself is everyone. Although my colleagues do not define an intelligence competition so narrowly as to consider only state-on-state interactions (they sometimes also consider nonstate actors like the Islamic State), my argument is more than an attempt at

[141] Garrett M. Graff, "The Mirai Botnet Was Part of a College Student Minecraft Scheme," *Wired*, Dec. 5, 2018, https://www.wired.com/story/mirai-botnet-minecraft-scam-brought-down-the-internet/.

distinction without difference. It is a front-end assessment of who holds data, who collects it, who has the capacity to interpret it, and who can leverage effects with it.

Everyone is here together. This is the actual landscape of the competition, within which my colleagues' state-based analyses are taking place. State-based cyber competition does not hold a monopoly. It is a tiny parcel of larger competition that often uncomfortably intervenes in state efforts to play their spy games.

If cyber competition among states is an intelligence competition, then we must ask, are states the dominant players? Who are the other players? For the purposes of this thought experiment, I answered "no" to the first question, and for the second question, "Just about everyone who wants to be."

The theoretical development is what comes next. If we are to adhere to Rovner's five elements, it may make sense to consider who has the greatest competitive advantage in each category. For example, on the part of competitive data collection and analysis, the private sector mega-data management companies hold the trophy. Those firms do not necessarily have adversarial relationships with U.S. adversaries. However, this does not mean that they are neutral. They simply have other kinds of politics and other kinds of adversaries.

Defining cyber competition as an intelligence competition should also make us revisit notions of cyber sovereignty, surveillance, and privacy. Too easily do we sweep this away under the rug of domestic legal considerations or technology policy, leaving it as a matter for advocates rather than academics. But recall again Cronin's observation that the social context of this technology has surpassed the state's dominion over it. Retreating to Waltz and parsimony is the wrong idea.

It is unclear to me exactly how to steer this ship. As I said before, there is likely no unified theory that will usefully capture this intelligence competition. The purpose of this piece is to begin a conversation about intelligence, competition, and the boundaries that may have changed in the transition to a newly open fabric of "sousveillance" — where the watched are watched and wait quietly for opportunities to leverage their secrets.[142] As social scientists, we should be cautious that our attempts to bound what is and isn't the purview of governments doesn't result in extremely conservative or status quo-seeking policy behavior; nor should they constitute a retreat from the hard-won elements of liberalism that value the individual citizen.

Insofar as we are in a global intelligence competition, our cup runneth over — into everything else. And the recent empirical record bears this out painfully: Snowden, the Shadow Brokers, Manning, Assange, Bellingcat, WikiLeaks, and anything associated with White House leakers. The dynamics we seek to explore, even if they exist only between states, will be at a minimum mediated by all of these additional practitioners of the use and abuse of data and data-enabled devices.

Privileging states is an exercise in both analysis and tool creation. Political science, in particular International Relations theories (big I, big R), tend to privilege the state as its

[142] Steve Mann, Jason Nolan, and Barry Wellman, "Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments," *Surveillance & Society* 1, no. 3 (2002): 331–55, https://doi.org/10.24908/ss.v1i3.3344.

primary unit not only because they are frequently the primary agents of interaction but also because there is applicable policy value in thinking about how states can conduct themselves among one another. Yet cyberspace, no matter how many times we scream "whole of government," is not owned, operated, or ruled by states. States are not sovereign on the internet, at least when it comes to intelligence competitions. Privileging states in thinking about cyber is folly. It distracts us from resolving hard policy issues by reducing social media's dysfunctional influence to Russian meddling or major systemic vulnerabilities in data management to Chinese IP theft. It leads to incomplete and hypermilitarized policy solutions that are costly, potentially escalatory, and fundamentally unhelpful to pressing back against the swollen gnat swarm of data-driven devices. Our windshields are peppered with the evidence. Now, somebody turn on the wipers, and let's get to work.

Dr. Nina Kollars *is associate professor of the Strategic and Operational Research Department and a core faculty member in the Cyber & Innovation Policy Institute* (*CIPI*). *She holds a Ph.D. in political science from The Ohio State University, a masters in international affairs from the Elliott School at George Washington University, and a bachelors from the College of Saint Benedict/Saint John's University. Kollars conducts research in cyber security, future warfare concepts, and military technological integration, specifically the methods and networks through which white-hat hackers produce security at the national and global levels. Her forthcoming manuscript leverages more than four years of research in and around the U.S. hacking community. She is a fellow at the Atlantic Council, a former fellow of the Modern War Institute at WestPoint Military Academy, a research analyst for the Congressional Cyber Solarium Commission, the former viceroy of* *the DC-based Cigars, Scotch, and Strategy, and currently teaches the Gravely Advanced Research Projects Group within the Center for Naval Warfare Studies.*