H-Diplo | ISSF

Article Review 75
issforum.org

H-Diplo/ISSF Editors: **Thomas Maddux** and **Diane Labrosse**
H-Diplo/ISSF Web and Production Editor: **George Fujii**

Erik Gartzke and Jon R. Lindsay. "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace." *Security Studies* 24:2 (2015): 316-348. DOI: http://dx.doi.org/10.1080/09636412.2015.1038188.

Review by **Brandon Valeriano**, Donald Bren Chair at the Marine Corps University/Cardiff University

Published by ISSF on 21 April 2017

tiny.cc/ISSF-AR75
https://issforum.org/articlereviews/75-cyberspace
https://issforum.org/ISSF/PDF/ISSF-AR75.pdf

The recent Democratic National Committee e-mail hack, and revelations passed on to Wikileaks, by Russia, illustrate the complicated nature of cyber statecraft. While there are many theories and ideas about cyber war, few scholars have articulated a realistic way to examine the cyber domain as it confronts a new way to conduct espionage and information warfare. Erik Gartzke and Jon Lindsay's article on deception in cyber security offers an important fourth way in the study of modern cyber strategy. They clearly articulate a path beyond the offense, defense, and deterrence strategies, which can often be ineffective or outdated modes given current realities.

Deception, combined with theories of technology as a force multiplier or a restraining device, provides a language that moves beyond stale Cold War concepts in order to explain how states now interact on the diplomatic and military battlefield. As they note, "deception should rise in prominence in a world that increasingly depends on technology to mediate interaction" (316).

Much of the article seeks to break down the myth of offensive dominance in cyberspace. In fact, offense dominance should be assumed to be neither easy nor cheap; it is often difficult, expensive, and requires an extreme amount of luck to work. Defense can often be more effective than one may think. Given the reality that the United States and Israel are probed perhaps millions of times each day, defense could be the dominating outcome in cyberspace. Yet defense is also problematic in that our openness and desire to connect everything to reach the 'internet of all things' invites opportunities for attack. With the Office of Personal Management hack in 2014 or the Edward Snowden information dumps, we also witness the fallacy of relying on third parties having significant access to important systems given this is how both of these intruders

collected information. These issues then invite the new way, deception, which offers both avenues and advantages for defensive and offensive strategies (318).

Manipulation, traps, and digital destruction of information are the real concerns, not some mythical cyber warfare that invites thoughts of digital disaster. Digital disaster might come, but it will aided by our tendency to invite attack through digital dependencies and ease of access. As James Clapper, the Director National Intelligence, notes, the most likely scenario for disaster involves the manipulation of information to comprise its integrity.[1] In fact, the TV series "Mr. Robot" (2015) articulates a Cyber Armageddon, but this apocalypse is not one of digital destruction that invites death but one of the destruction of information that allows for revolution against the one percent to fight global inequality. By wiping out financial records and their cloud based backups, the Mr. Robot team achieves something much more dangerous than any vision of future cyber warfare offered so far.

The importance of Gartzke and Lindsay's article is that it pushes cyber security theory forward and forces us to rethink old concepts or articulate new ones. As they suggest, "just as the nuclear revolution led to new modes of strategic interaction, the expansion of computer networks may necessitate reconsideration of security logics" (317). Reviving deception as a key strategic concept (operations meant to deceive, trick, or confuse) is an important advance when one considers the general inability of the cyber security field to move beyond the concepts of cyber war, revolutions of military affairs, deterrence, and the offense-defense balance. All these concepts have serious flaws given theoretical and empirical analysis of their efficacy in the real world for cyber issues. Since cyber security represents an important policy consideration and a framework that might guide future military and strategic affairs, the dependency on infeasible and unviable concepts is both surprising and depressing.

This dependency on old concepts in the security studies field is why Gartzke and Lindsay's article on cyber deception is so important. It is one of the few relatively novel and new (or retro, if you like Sun Tzu) theoretical ideas that can help us explain why cyber security is utilized by states, why it often fails as a tactic, and how it can be used as an effective means of both attack and defense. Instead of cyber being an effective means of coercive intent and changing the military or diplomatic battlefield, what cyber as a tactic has done is revolutionize methods of espionage and information warfare, bringing deception back as a key concept.

The research of Gartzke and Lindsay provided a new theoretical pathway in my own work. *Cyber War versus Cyber Realities*, my book with Ryan Maness, scopes out the domain of cyber conflict and presents data on all cyber actions between rivals.[2] We were able to demonstrate that most attacks are regional in intent, that state actors are restrained in their operations, and few malicious cyber actions provoke a reaction in the target. Yet, the work on deception has made us rethink and refocus our framing of cyber strategy in our subsequent work. In a forthcoming book we note that only 27 percent of cyber actions are truly coercive degrading and denial

[1] Cheryl Pellerin, "Defense, Intel Leaders: Cybersecurity Priorities are Defense, Deterrence," *DoD News*, 29 September 2015, https://www.defense.gov/News/Article/Article/621018/defense-intel-leaders-cybersecurity-priorities-are-defense-deterrence.

[2] Brandon Valeriano and Ryan C. Maness, *Cyber War versus Cyber Realities: Cyber Conflict in the International System.* (New York: Oxford University Press, 2015). See the H-Diplo/ISSF review of the book at https://issforum.org/roundtables/9-7-cyber.

strategies. Instead most actions are either espionage (50%) or disruption (21%) – actions that might be described as deception.

Once we move away from the cyber war framework and its focus on offense and defense, the field can truly begin to think about the nature of cyber actions and their impact. The method is mainly utilized in the domain of espionage, yet unfortunately the field of International Relations has had little connection or consideration of what how espionage affects the levels of cooperation and conflict between states. "Today, the specter of cyber warfare and espionage seems to pose conditions in which the strategies of the past again appear inadequate" (317). The strategies of the past are often built on assumptions, which as Gartzke (2013) has pointed out, are often inadequate and irrational.[3] The language of deception, with new terms leveraged in cyber security research such as simulation and dissimulation; seduction and deception; and finally, misdirection and indirection, might all offer new avenues for exploration.

As the authors note, the problem with their claims of deception being important is the inability to empirically test many of their propositions given that deception is a self-hiding phenomenon (346). This weakness is great given the plethora of speculative claims in the domain, but their analysis is based on very real examples that can be expanded to investigate the nature of their claims with rigorous case research. What is not beyond empirical evaluation is the claim of the offensive dominant domain of cyberspace being either overstated or incorrect. More research on these claims is sure to come; as some have demonstrated, the cyber security field is not an arena that lacks evidence, it is only an arena that has so far lacked engagement with scholars trained in the evaluation and collection of macro-evidence.[4]

Gartzke and Lindsay are exemplars and others should take their lead in thinking about new ways of describing and theorizing about cyber security in international politics. The hype-based perspective of cyber war is inflated and non-existent in reality. We are left with the more basic processes of information control, deception, and espionage. These frames are a bit less exciting than an all-out cyber war, but sometimes the real world is a bit less exciting and revolutionary than presented.

Brandon Valeriano (Ph.D. Vanderbilt University) the Donald Bren Chair of Armed Conflict at the Marine Corps University and a Reader at Cardiff University. Ongoing research explores cyber coercion, external threats and video games, biological and psychological examinations of cyber threat, and arms races and arms control in cyberspace.

[3] Erik Gartzke, "The Myth of Cyberwar: Bringing War on the Internet Back Down to Earth," *International Security* 38:2 (Fall 2013): 41-73. DOI: https://doi.org/10.1162/ISEC_a_00136.

[4] Key data based investigations include: Robert Axelrod and Rumen Iliev. "Timing of cyber conflict," *Proceedings of the National Academy of Sciences* 111:4 (2014): 1298–1303; Nadia Kostyuk and Yuri Zhukov, "Can Cyber Attacks Shape Battlefield Events?" Working Paper, 2017; Maness. And Valeriano, "The Impact of Cyber Conflict on International Interactions," *Armed Forces and Society* 42:2 (2016): 301-323, DOI: https://doi.org/10.1177/0095327X15572997; Valeriano and Maness, "The Dynamics of Cyber Conflict between Rival Antagonists, 2001-2011," *Journal of Peace Research* 51:3 (2014): 347-360.