Cor

DAVID L. BOREN
COLLEGE OF INTERNATIONAL STUDIES
The UNIVERSITY *of* OKLAHOMA

CGPC Home

People

News and Events

Speaker Series

Contact Us

The Cyber Governance Blog

Aaron Brantly
Assistant Professor, Department of Political Science, Virginia Tech

Aaron Brantly is an Assistant Professor of Political Science. Previously, he has held positions at the United States Military Academy and the National Security Studies Institute. Dr. Brantly has worked on issues related to cybersecurity from multiple angles including, human rights and development, intelligence

COLLEGE OF INTERNATIONAL STUDIES / CENTERS & PROGRAMS / CYBER GOVERNANCE AND POLICY CENTER / THE CYBER GOVERNANCE BLOG / CONCEPTUALIZING CYBER DETERRENCE BY ENTANGLEMENT

Conceptualizing Cyber Deterrence by Entanglement

03-15-2018 | Aaron Brantly

The evolution of cyberspace from ARPAnet to the Internet and now a domain of military interactions warranting its own combatant command has been rapid and extensive. The number of connected devices now exceeds 17 billion and will continue to grow in the coming years.[1] For all the benefits afforded by the development of cyberspace it is also a domain rife with crime, espionage and conflict. Rarely does a day go by in which news stories do not discuss some new cyber-attack, theft or espionage activity.[2] As cyberspace has developed and increased in importance to the economy and to national security, considerations on how to foster deterrence have increased. To date, with some notable exceptions, most conversations on deterrence have focused on activities that threaten punishment to or denial of adversaries.[3] Analyses frequently make parallels back to cold war deterrence strategies that emphasize the logic surrounding nuclear weapons. A variety of scholars of international relations and technical specialists view strategies heavily focused on threatening retaliation or on denial as unsatisfactory when applied to cyberspace.[4] These strategies remain unsatisfactory because cyberspace has unique characteristics which undermine key components of deterrence including credibility, signaling, specificity, attribution and decision-making.[5]

and national security and military cybersecurity. His interests span the political science and computer science divide. He is currently working on a year-long project on cyber deterrence funded by OSD Minerva R-Def.

Chris Demchak and Peter Dombrowski in writing on the future of cyberspace entertained the idea of the rise of a new “Cybered Westphalian Age.”[6] Yet, perhaps there is another potential path forward for enhancing stability and deterrence within cyberspace. The divergent path does not focus on the building of barriers and the establishment of hard sovereignty over cyberspace, but rather a world in which the barriers are lowered. Joseph Nye proposed this path forward for cyberspace in 2017 is known as entanglement.[7] Entanglement challenges the notion that states can ever fully secure themselves in an ever-evolving man and soon man and machine made technological domain. Entanglement is worthy of examination because it alters the costs and benefits matrix from ante-impetum (pre-attack) and post-impetum (after-attack) to one that emphasizes the management of risk aversion and risk seeking through a continuous relationship between parties. Entanglement as a strategy seeks to enhance benefits such that it creates a disincentive (risk aversion) and minimizes risk seeking by an adversary.

The challenges associated with deterrence at present are centered on an inability to establish credibility in both denial and threatening activities in cyberspace. In 2014 Secretary General Rasmussen in a speech at the United States Military Academy declared that NATO maintains an “ambiguous deterrence” strategy.[8] One of the central tenets of deterrence theory prevalent from early scholars such as Bernard Brodie,[9] Thomas Schelling[10], and others is the need to establish clear, unambiguous signals to potential adversaries of what is and is not acceptable behavior. Moreover, upon violation states must have the ability to successfully act upon threats and have an adversary clearly understand that these acts of punishment are linked to their violations of pre-established red-lines. Cyberspace complicates both sides of this equation. First, it is difficult to convey where and what a red-line is in cyberspace, and second it is very difficult to threaten or hold at risk an asset in cyberspace after a violation has occurred.[11] There should be little doubt that the US possesses the capabilities to achieve strategic, operational and tactical effects in and through cyberspace, but how to incorporate these into a robust strategy of deterrence remains unsettled as recently as February 2018 at a USCYBERCOM sponsored strategy symposium. Publicly the unsettled nature of deterrence in and through cyberspace was further highlighted by both the current USCYBERCOM Commander Admiral Rogers and the incoming USCYBERCOM Commander LTG Nakasone in Congressional testimony in February 2018.[12]

In their seminal work in the 1970s Joseph Nye and Robert Keohane challenged the International Relations establishment with the concept of complex interdependence and highlighted the importance of absolute gains brought about through deepening ties between nations across sectors, in particular, economies.[13] Their work was further bolstered by that of Robert Axelrod in his analysis of iterative games and norm development over time.[14] Axelrod demonstrated that it was possible, through iterated interactions, to extend the shadow of the future outward to create a more robust steady state. Extending beyond Axelrod, Daniel Kahneman and Amos Tversky established that humans are inherently predisposed to different concepts of risk predicated on changes in the reference point of actors.[15] By combining these scholarly works and those that followed, the potential for entanglement as one strategy for fostering deterrence and stability in cyberspace is derived.

Entanglement focuses on mutual establishment and recognition as well as perception management of benefits both in the present and over time. By shifting the focus away from punishment and denial entanglement seeks to alter the reference point from risk seeking behaviors commonly found within conventional deterrence modeling to risk aversion. Entanglement both alters the calculus of states interactions and extends out the shadow of the future. Areas such as information sharing and analysis centers within critical sectors such as finance and energy, the development of heterogeneous and diverse markets inclusive of software and hardware from diverse ecosystems, the establishment of global supply chains, and the broadening and deepening of ties with key strategic allies all coalesce to entangle potential adversaries. Moreover, as entanglement deepens so too does risk aversion.

Entanglement between conventional allies further raises the costs for non-allied interventions as it creates systemic hands tying behaviors across countries and sectors. It also discourages allies from breaking with one another for fear of losing the benefits of entanglement. Moreover, entanglement with traditional or potential adversaries can serve as a self-deterrent mechanism that promotes risk aversion. For example: because China benefits from US and European markets it is dissuaded from harming them with cyber-attacks that degrade/deny, destroy or disrupt or in any way damage their existing benefits both in the short and the long-term. If further entangled, China might also be willing to provide information to enhance resilience or counter threats by third parties that might adversely impact their own benefits. By more thoroughly entangling both friend and foe the aggregate benefits for maintaining and enhancing good behavior within the cyberspace increase and reinforce risk averse behaviors.[16]

---

[1] Evans, Dave. 2011. “The Internet of Things: How the Next Evolution of the Internet Is Changing Everything.” CISCO Internet Business Solutions Group.

[2] Zetter, Kim. 2014. “Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon.” Crown Publishers; Greenberg, Andy. 2015. “Hackers Remotely Kill a Jeep on the Highway—with Me in It.” *Wired.com*. July

21. https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/; Harris, Shane. 2014. "@War: the Rise of the Military-Internet Complex." Boston: Houghton Mifflin Harcourt.

[3] Mandel, Robert. 2017. *Optimizing Cyberdeterrence : a Comprehensive Strategy for Preventing Foreign Cyberattacks*. Georgetown University Press;

[4] Libicki, Martin C. 2009. *Cyberdeterrence and Cyberwar*. Santa Monica, CA: RAND Corporation; Valeriano, Brandon, and Ryan C Maness. 2015. *Cyber War Versus Cyber Realities : Cyber Conflict in the International System*. New York: Oxford University Press.

[5] Glaser, Charles. 2011. "Deterrence of Cyber Attacks and U.S. National Security." GW-CSPRI-2011-5. Washington, DC: Cyber Security Policy and Research Institute.

[6] Demchak, Chris C, and Peter Dombrowski. 2011. "Rise of a Cybered Westphalian Age." *Strategic Studies Quarterly*.

[7] Nye, Joseph S, Jr. 2017. "Deterrence and Dissuasion in Cyberspace." *International Security* 41 (3). MIT Press: 44–71. doi:10.1162/ISEC_a_00266.

[8] Speech given to Corps of Cadets at the United States Military Academy, West Point in the Fall-Term prior to his departure from his post.

[9] Brodie, Bernard, Frederick Sherwood Dunn, Arnold Wolfers, Percy Ellwood Corbett, and William T. R. Fox. 1946. *The absolute weapon: atomic power and world order*. New York: Harcourt, Brace and Co.

[10] Schelling, Thomas C, Harvard University., Center for International Affairs. 1966. *Arms and Influence*. New Haven: Yale University Press.

[11] Buchanan, Ben. 2017. *The Cybersecurity Dilemma Hacking, Trust and Fear Between Nations*. Oxford: Oxford University Press.

[12] https://www.c-span.org/video/?441677-1/nsa-chief-testifies-fiscal-year-2019-budget; https://www.c-span.org/video/?441917-1/nsa-nominee-testifies-senate-armed-services-committee.

[13] Keohane, Robert O, and Joseph S Nye. 1977. *Power and Interdependence : World Politics in Transition*. Boston: Little, Brown.

[14] Robert Axelrod, *The Evolution of Cooperation* (New York: Basic Books, 1984).

[15] Kahneman, Daniel, and Amos Tversky. 1979. "Prospect Theory: an Analysis of Decision Under Risk." *Econometrica* 4 (2): 1–30.

[16] It should be noted that entanglement is not applicable for espionage or for criminal activities. These types of activities fall within different domestic and international considerations and should be dealt with differently.

David L. Boren College of International Studies
Farzaneh Hall, Room 107
729 Elm Ave.
Norman, OK 73019

Updated 3/15/2018 by David L. Boren College of International Studies: cis@ou.edu