H-**Diplo** | **ISSF**

Article Review 84

issforum.org

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

Erica D. Borghard and Shawn W. Lonergan. "The Logic of Coercion in Cyberspace." *Security Studies* 26:3 (May 2017): 452-481. DOI: http://dx.doi.org/10.1080/09636412.2017.1306396; and **Travis Sharp. "Theorizing Cyber Coercion: The 2014 North Korean Operation against Sony."** *Journal of Strategic Studies* (2017): 1-29. DOI: https://doi.org/10.1080/01402390.2017.1307741.

Review by **Richard J. Harknett**, University of Cincinnati[1]

Published by ISSF on 26 September 2017

http://tiny.cc/ISSF-AR84
https://issforum.org/articlereviews/84-cyber
https://issforum.org/ISSF/PDF/ISSF-AR84.pdf

It is good social science practice, and from a Kuhnian perspective expected, that we should seek to understand emerging security dynamics through reference to existing concepts and theory.[2] Erica Borghard, Shawn Lonergan, and Travis Sharp offer such analysis examining cyber capabilities as coercive tools. Appropriately, both articles return to the master, Thomas Schelling,[3] while additionally offering the reader a helpful set of footnoting of the relevant subsequent literature. In stepping back and looking at the fundamental elements of coercion theory, the authors provide an important contribution to current thinking. The challenge for security studies academics attempting to bring our literature to bear in understanding cyberspace is significant. For example, these two articles, published within a month of each other, come to apparently opposite conclusions—the former suggesting that cyber operations are of limited coercive value

[1] The analysis found in this essay are the views of the author alone and do not necessarily reflect the official policy position of the United States Department of Defense, U.S. Cyber Command or any agency of the U.S. Government. The author wishes to thank Monica Kaminska and Jelena Vivic for their comments on early drafts.

[2] For more on whether we are facing the friction that appears when paradigms need to shift see Richard J. Harknett. "Correspondence: J. Nye." *International Security* 42:1 (Fall 2017): forthcoming.

[3] Schelling's oft-cited influential works, include, *The Strategy of Conflict*. Cambridge: Harvard University Press, 1960 and *Arms and Influence*. New Haven: Yale University Press, 1966.

and the latter allowing that cyber operations might be more effective than critics conclude. This divergence of analysis points to the importance of building a cyber security studies sub-field through more extensive empirical research and theory testing, which both articles attempt. But the divergence of views also highlights the need to consider the development of new explanations beyond existing analytical frameworks.

While seeking to gain insight through existing theory, both academics and policymakers must allow for the potential that some of the core dynamics associated with operating in cyberspace represent more discontinuity than similarity in fundamental security dynamics and thus require new conceptual thinking. If there is a disconnect between what we are observing empirically and the analytical variables we are using to explain dynamics, we may need to spend more time considering different analytical frames or modifications to existing constructs than just applying legacy constructs. It is important to note that we did not anchor our thinking of how to use nuclear weapons on Second World War concepts and operations. From Bernard Brodie[4] onward, we allowed the unique characteristics of atomic technology to drive us toward new analytical conceptualizations that illuminated the critical finding that security had to be found not in offense-defense exchange, but in deterrence of aggression. As cyberspace becomes an increasing focus for security studies research, we must engage in the *process* exemplified by that early nuclear thinking, rather than remain tied simply to applying the *findings* of that thinking. Both articles reveal the limits of post-1945 concepts, in this case coercion,[5] and urge more study of those concepts, rather than considering or urging more expansive conceptual development. However, a takeaway from both articles is that they offer analysis from which we can glean new directions; and that is what we really need to do if cyber security studies literature is going to progress.

Borghard and Lonergan offer two distinct, yet related, assessments: one that looks at the features of cyber capabilities and operations set against four central conditions of successful coercion—communication, cost-benefit calculus, credibility, and reassurance; and a second that examines cyber war-fighting strategies. The authors conclude that “cyber power has limited effectiveness as an independent tool of coercion” (453) across a narrow band of war-fighting contexts. They offer their overall analysis, however, with a significant caveat—that their assessment is based on current capabilities. In fact, at the end of the article they open up the possibility of simply setting aside the arguments that have just been presented, stating: “However, as technology evolves and the Internet of Things makes societies more interconnected and vulnerable, states may find strategies that explicitly aim to wreak havoc on civilian populations more effective” (480). This conclusion is of critical importance in that interconnectedness and inherent vulnerability are two structural features of cyberspace that are not going away. Beyond the emergence of the Internet of Things, machine learning and pervasive reliance on algorithmic decision-making will only deepen the consequences of these two structural features. By implication, according to Borghard and Lonergan, state actors will find potentially more opportunity for cyber coercion and thus work harder at making it more effective. But this conclusion

[4] Bernard Brodie, ed., *The Absolute Weapon: Atomic Power and World Order*. New York: Harcourt Brace, 1946; *Strategy in a Missile Age* (Princeton: Princeton University Press, 1959).

[5] Much of the current literature and policy discussion on cyber security dynamics is dominated with a focus on deterrence, for example. While most of the deterrence focus highlights its limitations, the dominant view is that we need to keep trying to figure out a deterrence mechanism, rather than consider that deterrence is simply the wrong strategy. Michael Fischerkeller and Richard Harknett. “Deterrence is Not a Credible Strategy for Cyberspace,” *Orbis* (Summer 2017): 1-14.

raises the dual questions as to whether there is a qualitatively distinguishable level of interconnectedness and vulnerability (scope) at which coercion will work that we have not yet achieved, or a quantitative degree of both variables (scale) that, once reached, will make coercion more effective. Cyberspace is interconnected and vulnerable now, and yet they find that cyber coercion is of limited utility. Is that simply because of scope or scale? Or is it possible that what they are illuminating is not coercive limitation, but conceptual limitation; that is, we are applying the wrong explanatory frameworks. Is the assessment measure associated with coercion theory ideally suited to capture the dynamics of cybersecurity as they are and into the future?

Drawing from traditional coercion theory, the authors focus on wreaking havoc (480) as the measure of coercive utility. Sharp's examination of the attack on Sony Entertainment Pictures (SPE) has the same underlying measure in mind. Both articles align with the literature they cite, which, drawing from nuclear concepts, assumes that strategic effect equates with large scale destruction or disruption associated with war or acts of war. This has translated directly into the policy space as well, with many current national cyber security strategies focused first and foremost on deterring attacks against critical infrastructure. Set against that measure, interestingly both articles' conclusions about cyber coercion are warranted, but their analysis of the technology itself suggests that perhaps a different measure of utility is in order when examining strategic effect. First, the articles appropriately distinguish coercion from war or acts of war. While war involves coercion, compellence can occur short of war in both its coercive diplomacy version or through limited controlled application of force and compellence, in certain cases, can have impact on regional and even global distributions of power. Whether cyber compellence can work, tactically or strategically, is two different questions. While not always clear about this distinction, both articles offer analysis to suggest that even at the tactical level cyber compellence is difficult.

Borghard and Lonergan examine the four core conditions associated with successful coercion. They argue convincingly that cyber communication is problematic since it is difficult to extract intent from code and thus signaling is complex. They note that this communication is complicated by the attribution problem that is routinely debated in cyber security literature and conclude that "to be coercive, a cyber signal must be attributable" (459). The problem in a compellence strategy is not attribution per se, however, which the state seeking to compel would have control over, but more precisely the method by which compellers makes themselves known (self-attribution). The challenge is really that the intent of a cyber operation is not apparent when code is discovered or an effect occurs unless coupled with a signaling strategy. The WannaCry ransomware global attack on May 2017 is a good example. This was a very obvious coercive (extortion) effect, but was this crime at a global scale, a criminal act that got out of control, a signal by a state of a disruptive capability, or a strategic operation to circumvent global sanctions and produce state revenue? Even if one concluded with certainty that the source was North Korea, we would not know what it intended through this exploitation. So we know what happened, we know (assume) who did it, but we do not know what to make of it because we do not know the intent. Borghard and Lonergan do examine signaling limitations, but it would have been helpful if they had more fully examined these implications and the flip side in depth—creative ways coercing states could signal using cyber means. There is a big difference between saying one cannot effectively signal with cyber operations and pushing forward with the notion that signaling in cyberspace will have to look very different than nuclear Defense Readiness Condition (DEFCON) messaging if it is to be effective. While we can start with understanding the differences between nuclear and cyber signaling, the literature needs to spend more time on the unique ways signaling can be done effectively in cyberspace.

Borghard and Lonergan raise some very good points about the limits of cost infliction through cyber operations and the issue of establishing credibility both in will and capability. They draw an unnecessary distinction, however, between credibility and what they call reassurance. In separating it out, they offer analysis that "implies that a coercive cyber attack that both reassures and maximizes costs for the target may be unachievable" (472). This tension does not hold deductively or empirically. First, what they are really talking about is contingent violence—the actor to be coerced must believe that the infliction of cost is contingent on his behavior, otherwise he does not have incentive to acquiesce. This is better understood as simply another component of credibility rather than a separate variable. Fundamentally, a coercive threat has to be contingent in order to be credible, so there is not an inherent tension here between forms of operations if the threat is credible. This point is actually a signaling and credibility issue, not an issue of operational tension. The challenge for the coercer is: can you credibly signal contingency? The pertinent question here is whether cyber technology creates unique opportunities or challenges to such signaling. The authors' earlier analysis would suggest that given signaling issues, cyber capabilities might complicate dynamics, but in the end, the credibility of contingency is likely more dependent on the perceived reputation of the coercer, rather than the technical means being used.

Clarifying this analytical issue over whether contingency is part of credibility or is separable as reassurance is important, because the authors suggest that the "greatest obstacle to successful coercion in cyberspace" is "assuring a target state that, once it capitulates to the aggressor's demands the punishment will cease" (471). The authors' analysis on signaling and cost infliction is much more compelling in revealing obstacles to achieving success than the loss of contingency due to the technology. The authors do raise an important point, however, about command and control, noting that some cyber attacks have used distributed capabilities and such operations once begun might be more difficult to cease immediately upon acquiescence. While true, this is a consequence of the style of operation being conducted, not inherent to the technology itself. The point to be taken here is that a coercer who wishes to be credible must insure that the operation does not undermine contingency. That is by no means an obstacle that cannot be overcome through proper planning.

Borghard and Lonergan propose that their analysis of coercion can illuminate why states might integrate cyber capabilities into war-fighting strategies. Specifically they write, "cyber power is not an ideal independent tool of coercion. Nevertheless, governments may still choose to use cyber power to pursue warfighting strategies aimed at eroding a target's ability or willingness to resist due to the perceived ease or cost effectiveness of conducting cyber operations" (472). It is inconceivable that modern states will commence war without employing cyber capabilities at some level, so shifting our literature toward analysis of different war-fighting strategies is an important advance. The authors offer a useful 2x2 matrix that assesses viability/non-viability and effective/non-effective measures. Unfortunately, more work needs to be done. They examine what they refer to as six warfighting strategies—attrition, denial, decapitation, intimidation, punishment, and risk, but the latter three are assessed as coercion strategies instead (which is what they are) with most of the focus remaining on the management of threat signals and the application of their analysis on coercion theory. The article would have benefited if those latter three strategies had been part of the first part of the article and critiqued using their framework of limited cyber utility. The other three are more clearly addressed as war-fighting strategies in the second half of the article, but not adequately enough. For example, concluding that attrition is a viable war-fighting strategy in cyberspace seems to run counter to the empirical evidence. While vulnerable, cyberspace is remarkably resilient to sustained disruption. Regarding destructive acts that destroy data or the systems upon which they reside, proper resiliency planning allows for reconstitution of systems. If we are in a war-fighting context and not a coercive diplomacy threat environment, then one has to assume into their model the active reaction and use of counter cyber capabilities that a defender can employ. Cyberspace, unlike nuclear space, is not an offense dominant environment. You can defend (although you only defend in the moment and on the digital terrain as it is configured in that moment).[6] This resiliency is evidenced in such cases as Saudi Aramco, which suffered some 30,000 computers being made inoperative and yet was able to sustain its operations, and Sony Pictures Entertainment (SPE), which continued to function as a company after its attack. The authors do not examine counter-strategies, all of which are inherently reinforced by digital technology and when properly organized can provide defenders significant capacity to undermine the effectiveness of any of the three war-fighting strategies (attrition, denial, or decapitation) they examine.

Travis Sharp challenges the notion that "cyber operations have limited coercive value" and suggests that "cyber operations contribute to coercion by imposing costs and destabilizing an opponent's leadership" (1). He correctly broadens analysis of cyber coercion to include non-state actors such as corporations and introduces the interesting outcome variable of leadership destabilization as distinct from cost imposition as a possible extension of our assessment of coercive action. His single case study of SPE is properly understood as an example of cyber compellence and he uses it effectively to show that there was financial cost inflicted and operational and reputation disruption of leadership. The case thus does illuminate how cyber operations might meet these two coercive conditions, but it is far from an ideal case. Unfortunately, the author attempts to make too much of the evidence and introduces a flurry of concepts that are either repackaging older notions or adding a sense of precision when in fact a broader construct has sufficient explanatory power.

For example, Sharp separates out the notion of credibility, suggesting it is better to understand coercion requiring credibility (perceived willingness to carry out a contingent threat) and persuasiveness (the perceived ability to carry out punishment or denial). It is not clear what we gain theoretically from this separation (explanatory-wise). In Schelling's rendering of coercion you cannot have a credible threat without both. Sharp references my 1994 *Security Studies* article during this discussion in which I make that argument and note that much of the nuclear literature took for granted the capacity to inflict costs and focused primarily on conveying will when considering credibility, while in conventional environments the condition holds that the ability to inflict cost or deny gain can be contested through technical, tactical, or operational manipulation.[7] Thus, the credibility of capability is a critical aspect of a coercive deterrent threat that creates a higher burden for states that wish to deter relying on conventional rather than nuclear forces. Cyber capabilities seem even more contestable than kinetic forces, and, thus, problematic from at least a deterrence credibility perspective. It is not clear that adding a different definitional split between credibility and persuasiveness lends greater explanatory power here.

A related but second unnecessary repackaging occurs with his introduction of what he calls the disclosure dilemma—that cyber operations might be undermined if they are revealed to the opponent who could become more effective in countering the cyber operation. The work of John Mearshimer, Jonathan Shimshoni, and me on conventional deterrence a few decades ago dealt with this contestability dynamic, so

[6] See Fischerkeller and Harknett for a discussion of cyberspace as an offense persistent strategic environment.

[7] Richard J. Harknett. "The Logic of Conventional Deterrence and the End of the Cold War." *Security Studies.* 4:1 (Autumn 1994): 86-114.

this is not new to cyberspace.[8] The more relevant question is whether cyber capabilities and operations allow potential coercers to manage contestability differently and whether deterrence and compellence dynamics differ in cyberspace. Sharp hints at the latter, noting that cyber compellence might not be as hard to practice as nuclear and conventional compellence, but Sharp does not develop this potential key distinction sufficiently.

This is important because Sharp implies that contestability (what he calls disclosure) seems to be managed with a tendency toward greater secrecy about cyber capabilities. More empirical studies are needed to test that hypothesis, but academics should be open, as well, to a different assessment variable altogether. Countering cyber operations might be aided more through discovery of an operation than in conventional environments, but it also might not matter as much for coercive outcomes, because of the low entry costs and iterative nature of the technology itself that allows attackers to modify quickly and persist in an attack despite effective countering of the first operation. Cyberspace may not be a strategic interaction environment in which attrition holds and, thus, discovery can lead to effective countering and, *simultaneously*, not matter to the coercer, who can adapt and iterate if countered. Strategic analysis should not presume that all cyber operations are based on highly sophisticated and demanding capabilities development that would make attrition salient.

Ultimately, Sharp confidently concludes that the SPE case itself represents successful cyber coercion (compellence), but his own presentation should lead to a more qualified assessment. The case does show that cyber operations can inflict costs and destabilize leadership, but the goal of the operation was to coerce the cancellation of the movie *The Interview*, and this, simply, did not occur. SPE's initial decision to pull the movie only occurred when a non-cyber cross-domain threat of physical destruction (terror attacks) against movie theaters was made and, in response, SPE and independent theaters found another way to release the movie. However, Sharp's treatment of the case opens up an interesting question about how we might begin to assess cyber operations differently than traditional theory would hold. Rather than examine his variable of leadership disruption as a means to an end, what if a main utility of cyber operations is that one can disrupt leadership functionality and legitimacy (reputation) short of war? What if disruption of governance is not a means of coercion, but an end in and of itself? The delegitimization of authority that might flow from such disruption might be something to which not only democracies are susceptible, but also authoritarian leaders, who are quite concerned about the preservation of their 'cults' of personality. While traditional coercion theory orients us to assess whether such action has compellent or deterrent utility, we must be also open to the notion that such a cyber operation might be pursued as an end in itself to shape the power projection capability of a state—a leader distracted at home, may mean a country less effective on the international stage.

Both Borghard and Lonergan and Travis Sharp advance thinking about the limitations of cyber coercion within the confines of existing theory. Cyber security studies, however, will only become more robust if our

[8] John Mearshimer, *Conventional Deterrence* (Ithaca: Cornell University Press, 1983); Jonathan Shimshoni, *Israel and Conventional Deterrence* (Ithaca: Cornell University Press, 1988); and, Richard J. Harknett, "State Preferences, Systemic Constraints, and the Absolute Weapon," in T.V. Paul, James Wirtz and Richard Harknett, eds., *The Absolute Weapon Revisited: Nuclear Arms and the Emerging International Order* (Ann Arbor: University of Michigan Press, 1997), 65-100.

growing exploration is not limited solely to 'inside-the-paradigm' analysis. These articles should point us toward that exploratory direction.

Dr. Richard J. Harknett is Professor and Head of the Department of Political Science at the University of Cincinnati. He recently served as Scholar in Residence at U.S. Cyber Command and the National Security Agency (2016) and Fulbright Professor in Cybersecurity at the Cyber Studies Programme, Oxford University. Relevant recent publications include those cited in the above review and The Search for Cyber Fundamentals," *Journal of Information Warfare* 15:2 (Spring 2016): 81-88 (co-author with Emily Goldman) and "The Struggle for Autonomy: A Realist Structural Theory of International Relations" *International Studies Review* 14 (2012): 499-521 (co-author with Hasan Yalcin). He is currently writing a journal article, "Nuclear Prominence and Cyber Persistence: the dynamics of 21st Century international security."