

HSPI Commentary Series

MANAGING COMPLEXITY IN A WIKILEAKS WORLD

HSPI Commentary 20


December 13, 2010

Sharon L. Cardash and Frank J. Cilluffo

Before PFC Bradley Manning there was Philip Agee. In 1975, disillusioned with and disaffected by his CIA career, Agee published *Inside the Company* which named scores of his onetime fellow officers, and generated shockwaves and significant consequences worldwide. As a result of this systematic attempt to destabilize the US intelligence community and its operations, officials were recalled from their posts, operatives' lives—both US and others—were placed at risk, protests against Agee's actions were registered, and some (comparatively few, but notably the Soviet KGB and Cuban DGI) came to his defense. The analogy with WikiLeaks is today imperfect in a wired world where information spreads instantaneously and to even the most obscure quarters. Here, the complexity of coping with the horse that has left the barn is staggering.

In support of Julian Assange and the larger cause of internet freedom (though ironically, WikiLeaks as an organization devoted to transparency is itself cloaked in secrecy), a team of "hacktivists" of unknown size called "Anonymous" has rallied. Targeting companies perceived to be obstructing that goal, and using relatively simple "point and click" tools, these hacktivists caused the temporary shutdown of online enterprises from MasterCard to PayPal. Through Twitter, they claimed responsibility for their attacks and spread word of their ongoing efforts, whose downstream impact included individuals dependent on the targeted businesses.

Social media are value neutral in the sense that their power as tools to further a given end can be harnessed by any and all, from a single individual to a large organization. With access to information broadened by these and other means, an array of questions about security, accountability and other fundamental issues is raised. Existing conceptual, legal and other frameworks (including the Espionage Act of 1917) may be ill suited to handle these matters. While the debate over remedies to redress the situation has begun—including in Congress where Senator Lieberman and Representative King have each introduced legislative measures for consideration—replacements or effective adjustments to these structures have yet to be implemented. Technology has simply outpaced policy.




In cyberspace, anonymity complicates attribution. Smoking keyboards are hard to find. Since an attacker's return address is not obvious, and may not even be discoverable, retaliation and deterrence remain a real challenge, even for a nation state. Both offense and defense are complicated in an ecosystem characterized by ambiguity, where basic questions remain unanswered. National and international authorities continue to struggle with definitional problems such as: What constitutes an act of war in cyberspace? Do we need a cyber equivalent of NATO Article V, which enshrines the principle of collective defense? How might cyber deterrence capability be best developed? Counterintelligence is just one aspect of defense in an environment marked by a range of actors with an equally wide range of motivations, capabilities, and resources. For years however, Russia has been the most sophisticated and China the most active in this space, from a US national security perspective.

In a virtual world with multiplicity of threat and seeming absence of control, the playing field is leveled and the few can take on the many or the once mighty. In response, a thoughtful national dialogue is needed to help recalibrate for today's world our notions of ethics, privacy, economic competitiveness and national security, for example. Tomorrow's leaders will need robust understandings of such concepts, as well as technical knowledge and skills. The need for public-private partnerships in this context is often referenced, and rightly so. Not only does the bulk of critical infrastructure in this country reside in private hands, but the WikiLeaks make clear that banks are no more immune than a country's diplomatic corps is to tumultuous times online.

Universities have a central role to play in all this, as they are uniquely situated to bridge the worlds of theory and practice in a number of domains including policy, technology and law. A nationwide cadre of cyber professionals with multidimensional expertise is sorely needed, and the bench must be as deep as it is wide. Unless and until we reach that goal, our posture will be more vulnerable and reactive than it ought to be.

From Strangelove to Stuxnet, the path has evolved dramatically. Now the challenge is to bring doctrine and policy into line with technology by closing the gap between the two. To allow the lag between them to persist does none of us any favors. The WikiLeaks chapter in cyber history, while colorful and significant, will not be the last. But this latest episode brings to the fore a number of major policy questions that have gone unaddressed for too long. Moving forward, the innovation and creativity that brought us to this point should continue to drive us and help define the path ahead. The answer is not to stifle technology or to lose appreciation for fundamental values like privacy. At the same time, it is clear that new approaches and mechanisms may be needed to cope with complexity, and to ensure that our national objectives continue to be fulfilled.



***Frank J. Gilluffo** is Director of The George Washington University Homeland Security Policy Institute (HSPI). **Sharon L. Cardash** is Associate Director of HSPI.*

HSPI Commentaries are intended to promote better policy by fostering constructive debate among leading policymakers, academics, and observers. Designed to be timely and relevant, HSPI Commentaries seek to illuminate the issues of the day by raising important questions and challenging underpinning assumptions. Opinions expressed in Commentaries are those of the author(s) alone. Comments should be directed to hspi@gwu.edu.

Founded in 2003, The George Washington University Homeland Security Policy Institute (HSPI) is a nonpartisan think and do tank whose mission is to build bridges between theory and practice to advance homeland security through an interdisciplinary approach. By convening domestic and international policymakers and practitioners at all levels of government, the private and non-profit sectors, and academia, HSPI creates innovative strategies and solutions to current and future threats to the nation.