No. 90
March 2011

MERCATUS ON POLICY

BEYOND CYBER DOOM

By Sean Lawson

MERCATUS CENTER
George Mason University

News media and policy makers in the United States are focusing their attentions on prospective threats to and through cyberspace. Current U.S. cyber-security policy—with its military Cyber Command and suggestions for an "Internet kill switch"—supports a centralized, militarized approach. Cyber security is a serious concern, but if policy makers want to actually address these threats, they should pursue strategies that focus on increasing technological and infrastructural resilience while promoting decentralization, self-organization, economic strength, and strong social systems.

CYBER THREATS

Cyber security has received intense scrutiny in the past three years.[1] Some proponents of far-reaching cyber security policies posit "cyber doom" scenarios that reflect long-held, but ultimately incorrect, assumptions and fears about the fragility of modern societies and infrastructure systems. Research by technology historians, military historians, and disaster sociologists consistently shows that modern technological and social systems are more resilient than military and disaster planners often assume. Fears and assumptions to the contrary often lead to an ultimately counterproductive centralized and militarized quest for top-down control.

NEGATIVE EFFECTS OF FLAWED ASSUMPTIONS

The United States's most significant response to perceived cyber threats is the establishment of the military's U.S. Cyber Command (USCYBERCOM), which reflects fears of cyber-doom scenarios that present cyber security in terms of war and disaster. Alarmists warn of "cyber 9/11," "cyber jihad," and "cyber Katrina." But most of what gets lumped under the term "cyber war" is really crime, espionage, or political protest. Framing the discussion in terms of war and disaster often leads

to counterproductive, militarist, command-and-control solutions that could be fraught with danger.

First, USCYBERCOM—which has both an offensive and defensive mission—could undermine the U.S. policy of promoting a free and open Internet worldwide by encouraging Internet censorship and filtering, as well as more rapid militarization of cyberspace.[2] Some have already called for USCYBERCOM to launch strikes on Wikileaks, which released hundreds of thousands of classified U.S. documents about the wars in Iraq and Afghanistan.[3] Such a response would create a "say-do gap" that potential adversaries could use to justify their own development and use of offensive cyber weapons and their efforts to thwart international cooperation on cyber security.[4]

Second, there is the danger of blowback. In an extremely interconnected world, an offensive cyber attack launched by the United States against another country might result in serious collateral damage or cause harm to the United States.[5] Indeed, in a recent case, the United States military took down a Jihadist discussion forum, causing collateral damage to noncombatant computers and websites and undermining an ongoing U.S. intelligence-gathering operation.[6]

Third, cyber attacks, especially attacks against less technologically adept countries, raise the risk of conflict escalation. If the United States launches a cyber attack against a state or non-state actor that cannot respond in kind, that actor might respond with physical attacks.[7] Moreover, the United States considers physical attacks a valid response to cyber attacks. A 2009 review of U.S. military strategy documents and statements from officials indicate that a nuclear strike remains an option for U.S. response to cyber attacks.[8]

PANICKED ABOUT PANIC

Assumptions of inevitable panic and social collapse increasingly dominate official U.S. disaster planning.[9] Government officials panic about the possibility of panic and then exacerbate the situation by not only failing to provide victims with the help they need, but also preventing them from effectively helping themselves, a phenomenon clearly seen in the official response to Hurricane Katrina.[10]

However, "decades of disaster research shows that people behave rationally in the face of danger;"[11] even group panic and specific antisocial behaviors, such as looting, are rare in modern societies.[12] Instead of engaging in a mass panic or paralysis that leads to social collapse, most people in disaster situations rely upon existing social bonds and norms of behavior to launch an effective response.[13]

Consider the terrorist attacks of September 11, 2001. Disaster sociologist Lee Clarke notes, "people did not become hysterical but instead created a successful evacuation."[14] That evacuation of Lower Manhattan, which involved nearly half a million people, "was a self-organized volunteer process that could probably never have been planned on a government official's clipboard."[15] Moreover, at the economic level, the Congressional Research Service concluded, "The loss of lives and property on 9/11 was not large enough to have had a measurable effect on the productive capacity of the United States." The U.S. economy is more resilient in the face of disaster and intentional attack than many assume.[16]

Then there's Hurricane Katrina. Some sponsors of cyber-security legislation have spoken of a possible "cyber Katrina."[17] While there was some looting and antisocial behavior in the immediate aftermath of Katrina, Enrico Quarantelli, a pioneer in the field of disaster sociology, reports that "pro-social and very functional behavior dwarfed on a very large scale the antisocial behavior that also emerged."[18] And though the economic impacts of Katrina were severe, especially for the Gulf Coast region, Katrina did not collapse the entire U.S. economy. "Cyber 9/11s" and "cyber Katrinas" are unlikely to do so as well, so long as policy makers consider the following principles when forming cyber-security policy.

Define the problem clearly.

The first step to formulating and evaluating prospective cyber-security policies is defining the problems clearly. As cyber-security policy analyst James Lewis argues, "Pronouncements that we are in a cyber war or face cyber terror conflate problems and make effective response more difficult."[19] To avoid this, disaggregate the different types of cyber threats—cyberspace-enabled economic espionage, political and military espionage, crime, cyber war, cyber terror, etc.—so that an appropriate and effective response addresses a particular threat. There is no one-size-fits-all solution for cyber security.

Seek guidance from empirical research.

Empirical research, not hypothetical scenarios, needs to guide cyber-security policy. By relying too heavily on cyber-doom scenarios, current cyber-security planning, like contemporary disaster planning, is "organized to deal with predicted vulnerabilities rather than to mobilize social capital to deal with actual threats."[20] Experts and policy makers need to assess whether they are planning based on empirical evidence or on anxieties about technology and erroneous assumptions about infrastructural and social fragility. Additionally, while technical research is crucial, the formulation and evaluation of cyber-security policy requires knowledge of relevant "non-technical" matters like geopolitics, economics, and law.[21]

Promote resilience in technological and social systems.

While policy makers should seek to prevent cyber attacks when possible, they should also promote resilience in tech-

POLICY MAKERS SHOULD CONSIDER THE FOLLOWING PRINCIPLES WHEN FORMING CYBER-SECURITY POLICY:

1. Define the problem clearly.
2. Seek guidance from empirical research.
3. Promote resilience in technological and social systems.
4. Promote repair, maintenance, and modernization of infrastructure systems.
5. Promote decentralization and self-organization in social systems.
6. Promote strong local communities, economies, and good local governance.

nological and social systems. More resilient technological and social systems could help deter cyber attacks by providing would-be attackers with fewer valuable and vulnerable targets and could help mitigate effects of a cyber attack should one occur.[22]

Promote repair, maintenance, and modernization of infrastructure systems.

Promoting resilience hinges upon supporting ongoing repair, maintenance, and modernization of critical infrastructures. Such improvements would reduce system fragility—preventing some failures—and promote learning and adaption among repair crews that would be the first responders to failure.[23]

Thus, instead of "think[ing] of the grid as a fortress to be protected at every point"[24] by a central authority, we should invest in the more mundane, ongoing, and decentralized work of repair and maintenance—the true source of resilient infrastructures.[25]

Promote decentralization and self-organization in social systems.

Cyber-security policy should promote decentralization and self-organization in efforts to prevent, defend against, and respond to cyber attacks. Victims are often first responders to disasters, and centralized, bureaucratic responses can hamper their abilities to respond in an effective, decentralized, self-organized manner.[26]

After all, private actors own most critical infrastructures. Thus, a centralized, military-led effort to protect the fortress at every point will not work. The owners and operators of critical infrastructures are ones on the front lines and will be the first responders. Policy makers must empower them to act. Similarly, if the worst should occur, policy makers need to let average citizens know that it is helpful if they act in a decentralized, self-organized way to help themselves and others.

Promote strong local communities, economies, and good local governance.

Finally, preparation for responding to cyber attacks requires strong local communities and economies and good local governance. Just as more resilient technological systems can better respond in the event of failure, strong social systems are better able to respond to disasters. The response of individuals and groups in disasters depends largely on the structural conditions in existence before the disaster. Communities with weaker social ties among members, corrupt or ineffective local government and law enforcement, and economic hardship prior to a disaster will find it more difficult, if not impossible, to respond effectively in a time of crisis.[27]

In part, this requires, during normal, pre-disaster periods, policies and planning by local governments that not only promotes the growth of strong local civil-society organizations like businesses, churches, nonprofits, and neighborhood associations, but also plans to involve those organizations in post-disaster response and recovery efforts.

CONCLUSION

Policy makers need to reframe the discourse if they wish to address cyber-security concerns effectively. Flawed assumptions and conflated language have created policy proposals that could harm the United States's ability to respond to cyber attacks effectively. Instead of yielding to the hyperbole, policy makers should first clearly define the issue and distinguish potential threats. Then, they should purse policies that focus on increasing technological and infrastructural resilience and promoting decentralization, self-organization, economic strength, and strong social systems so that we are prepared to defend against cyber threats.

ENDNOTES

1. Experts attribute two large-scale cyber attacks, one against Estonia in the spring of 2007 and one Georgia in summer of 2008, to Russia. See G. Evron, "Battling Botnets and Online Mobs: Estonia's Defense Efforts During the Internet War," *Georgetown Journal of International Affairs* 9, (2008): 121–126 and J. Bumgarner and S. Borg, "Overview By the US-CCU of the Cyber Campaign Against Georgia in August of 2008," *US-CCU Special Report*, August 2009. Most recently, many have speculated that a computer worm called Stuxnet may have been a cyber attack by Israel on Iranian nuclear facilities. See E. Mills, "Symantec: Stuxnet Clues Point to Uranium Enrichment Target," CNET News, November 15, 2010, http://news.cnet.com/8301-27080_3-20022845-245.html.
2. M. Cavelty, *Cyber-Security and Threat Politics: U.S. Efforts to Secure the Information Age* (New York: Routledge, 2007), 143.

3. D. McCullagh, "Wikileaks Draws Criticism, Censorship Threats," CNet News, August 2, 2010, http://news.cnet.com/8301-31921_3-20012430-281.html.

4. M. Mullen, "Strategic Communication: Getting Back to Basics," *Joint Forces Quarterly* 55, no. 4 (2009): 2–4. The danger is that potential adversaries could justify their development of offensive cyber capabilities by asserting that the United States is saying one thing—claiming to support an open and free Internet—while doing another—considering using offensive cyber attacks in cases, such as the Wikileaks releases of war logs, where an open and free Internet is counterproductive to U.S. foreign-policy interests.

5. Cavelty, *Cyber-Security and Threat Politics*, 143.

6. E. Nakashima, "Dismantling of Saudi-CIA Web site illustrates need for clearer cyberwar policies," *Washington Post*, March 19, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/03/18/AR2010031805464.html.

7. R. Clarke, "War From Cyberspace," *The National Interest*, October/November 2009.

8. J. Markoff and T. Shanker, "Panel Advises Clarifying U.S. Plans on Cyberwar," *New York Times*, April 30, 2009, http://www.nytimes.com/2009/04/30/science/30cyber.html; W.A. Owens et al., *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (Washington, DC: National Academies Press, 2009).

9. E.L. Quarantelli, "Conventional Beliefs and Counterintuitive Realities," *Social Research: An International Quarterly* 75, no. 3 (2008): 897.

10. R. Dynes, "Panic and the Vision of Collective Incompetence," *Natural Hazards Observer* 31, no. 2 (2006); L. Clarke and C. Chess, "Elites and Panic: More to Fear Than Fear Itself," *Social Forces* 87, no. 2 (2009): 999–1004.

11. Ibid.

12. Clarke, "War From Cyberspace"; Quarantelli, "Conventional Beliefs," 873–904.

13. N.R. Johnson, "Panic and the Breakdown of Social Order: Popular Myth, Social Theory, Empirical Evidence," *Sociological Focus* 20 (1987): 171–183.

14. L. Clarke, "Panic: Myth Or Reality?" *Contexts* 1, no. 3 (2002): 21–26.

15. D. Glenn, "Disaster Sociologists Study What Went Wrong in the Response to the Hurricanes, But Will Policy Makers Listen?" *The Chronicle of Higher Education*, September 29, 2005, http://chronicle.com/article/Disaster-Sociologists-Study/120178/.

16. G. Makinen, *The Economic Effects of 9/11: A Retrospective Assessment*, (Washington, DC: Congressional Research Service, 2002).

17. K. Epstein, "Fearing 'Cyber Katrina,' Obama Candidate for Cyber Czar Urges a FEMA for the Internet," *Business Week*, February 18, 2009, http://www.businessweek.com/the_thread/techbeat/archives/2009/02/fearing_cyber_katrina_obama_candidate_for_cyber_czar_urges_a_fema_for_the_internet.html; Olympia J. Snowe, "Senator Snowe and Chairman Rockefeller Introduce Comprehensive Cybersecurity Legislation," Olympia J. Snowe Press Releases, April 1, 2009, http://snowe.senate.gov/public/index.cfm?FuseAction=PressRoom.PressReleases&ContentRecord_id=6306ecb2-802a-23ad-4a08-163f03f287da.

18. Quarantelli, "Conventional Beliefs," 873–904.

19. Research conducted as part of the Gulf Coast Recovery Project at the Mercatus Center has corroborated these findings. See http://mercatus.org/program/research/1000005.

20. J.A. Lewis, "The Cyber War Has Not Begun" (unpublished manuscript, Center for Strategic and International Studies, Washington, DC, March 2010), http://csis.org/files/pblication/100311_TheCyberWarHasNotBegun.pdf.

21. Dynes, "Panic and the Vision of Collective Incompetence."

22. J. Carr, *Inside Cyber Warfare: Mapping the Cyber Underworld* (Sebastopol, CA: O'Reilly Media, 2009); J.A. Lewis, "The 'Korean' Cyber Attacks and Their Implications for Cyber Conflict" (unpublished manuscript, Center for Strategic and International Studies, Washington, DC, October 2009), http://csis.org/files/publication/091023_Korean_Cyber_Attacks_and_Their_Implications_for_Cyber_Conflict.pdf.

23. J.A. Lewis, "The War on Hype," *San Francisco Chronicle*, February 19, 2006, http://articles.sfgate.com/2006-02-19/opinion/17283144_1_cyber-attack-pandemic-avian-flu; D. E. Nye, *When the Lights Went Out: A History of Blackouts in America* (Cambridge, MA: MIT Press, 2010), 189, 191.

24. S. Graham and N. Thrift, "Out of Order: Understanding Repair and Maintenance," *Theory, Culture & Society* 24, no. 3 (2007): 5, 14; Nye, *When the Lights Went Out*, 189.

25. Nye, *When the Lights Went Out*, 197.

26. Quarantelli, "Conventional Beliefs," 895–896.

27. Nye, *When the Lights Went Out*, 185; D. Alexander, "Symbolic and Practical Interpretations of the Hurricane Katrina Disaster in New Orleans," (presentation, Understanding Katrina: Perspectives from the Social Sciences, the Forum of the Social Science Research Council, 2006); A. Lakoff, "From Disaster to Catastrophe: the Limits of Preparedness," (presentation, Understanding Katrina: Perspectives from the Social Sciences, the Forum of the Social Science Research Council, 2006).

Sean Lawson is an assistant professor in the Department of Communication at the University of Utah. His research focuses on the relationships among science, technology, and the development of military theory and discourse, in particular the intersections of national security and military thought with new media, information, and communication technologies.