MIT
POLITICAL SCIENCE

Massachusetts Institute of Technology
Political Science Department

Research Paper No. 2016-2

Perspectives on Cybersecurity:
A Collaborative Study

Massachusetts Institute of Technology:

Nazli Choucri
Chrisma Jackson
Lyla Fischer
Brooke Gier
Vivian Peron
Ben Ze Yuan
Liu Yangyue
Glenn Voelz

Explorations in Cyber International Relations

Massachusetts Institute of Technology Harvard University

PERSPECTIVES on CYBERSECURITY

A Collaborative Study

Authors

Chrisma Jackson

Lyla Fischer

Brooke Gier

Vivian Peron

Ben Ze Yuan

Liu Yangyue

Glenn Voelz

Editors

Nazli Choucri

Chrisma Jackson

Department of Political Science

MIT

2015

Table of Contents

1 **Cybersecurity – Problems, Premises, Perspectives**
Nazli Choucri and Chrisma Jackson, Editors

2 **An Abbreviated Technical Perspective on Cybersecurity**
Ben Ze Yuan

3 **The Conceptual Underpinning of Cyber Security Studies**
Liu Yangyue

4 **Cyberspace as the Domain of Content**
Lyla Fischer

5 **DoD Perspective on Cyberspace**
Glenn Voelz

6 **China's Perspective on Cyber Security**
Liu Yangyue

7 **Pursuing Deterrence Internationally in Cyberspace**
Chrisma Jackson

8 **Is Deterrence Possible in Cyber Warfare?**
Brooke Gier

9 **A Theoretical Framework for Analyzing Interactions between Contemporary Transnational Activism and Digital Communication**
Vivian Peron

7. Pursuing Deterrence Internationally in Cyberspace

Chrisma Jackson

Deterrence theory associated with warfare dates back centuries. In the Art of War, Sun Tzu said, "It is a doctrine of war not to assume the enemy will not come, but rather to rely on one's readiness to meet him; not to presume that he will not attack, but rather to make one's self invincible."[106] The concept of deterrence in the United States gained momentum and prominence during the Cold War. After the use of two nuclear weapons brought the end of World War II, the destruction and devastation demonstrated by these weapons brought deterrence theory into the forefront of U.S. DoD policy.

Deterrence theory is based on the idea of dissuading an adversary from taking action before a war has started. In 1959, Bernard Brodie stated, "A credible nuclear deterrent must always be ready, never used."[107] Later in 1966, Thomas Shelling highlighted deterrence as the "use of power to hurt is bargaining power is the foundation…and is most successful when it is held in reserve."[108] More recently, Graham Allison discussed the context of nuclear deterrence in the cold war: "…even during the most dangerous moments of the Cold War, a nation that attacked the United States with a nuclear armed ballistic missile would know that it had signed its own death certificate, since US retaliation would be immediate and overwhelming."[109] With deterrence theory a fundamental aspect of Cold War strategy, the "3 Cs" highlighted the theory's key characteristics:

- Clarity – bright lines and unacceptable consequences
- Capability – demonstrated capacity of technology able to demonstrate a response
- Credibility – an administration and government willing to respond when attacked[110]

In the decades following the cold war, the concept of deterrence extended as asymmetric attack/threat scenarios increased. A 2013 United Stated Space Command article described an extension of the use of Deterrence to Space. For these space-based applications, deterrence is defined as "the prevention of action by the existence of a credible threat of unacceptable counteraction and/or the belief that the cost of action outweighs the perceived benefits."[111] With this in mind, four safeguards were implemented to deter actions against U.S. space-based assets: 1) work international norms, 2) build coalitions to enhance security, 3) add resilience to architectures, and 4) prepare for an attack using defenses not necessarily in space.

This extension of deterrence theory into space leads us to comparisons with Cyber:

- Properties:
    1. Nuclear: Visible, visceral and overwhelming destruction.

---

[106] Tzu, Sun, 2009. *The Art of War*, Trans. Lionel Giles, file:///Users/User/Downloads/taowde.pdf.

[107] Bernard Brodie, *Strategy in the missile age* (Princeton, NJ: Princeton University Press, 1959).
[108] Thomas C. Schelling, *Arms and influence* (New Haven, CT: Yale University Press, 1966).
[109] Graham T. Allison, *Nuclear terrorism: the ultimate preventable catastrophe* (New York: Times Books/Henry Holt).
[110] Ibid; Graham T. Allison, personal interview,, Harvard Kennedy School, November, 2014.
[111] Karen Parrish, "Official describes Evolution of Space Deterrence," *American Forces Press Service* September 19 (2013): http://www.defense.gov/news/newsarticle.aspx?id=120818

2. Space: Non-visible attack interface, but destruction impacts military and civilians (particularly in the west).
3. Cyber: Non-visible attack interface with immediate impacts to civilians and military.

- Actions:
  1. Nuclear: Weapon ownership intended for the state with recent broad proliferation.
  2. Space: Investment initiated by nation states, but opening to civilian entrepreneurs.
  3. Cyber: (The Internet) Initiated as a government resource with growth and expansion dominated by academic and civilian entrepreneurs. In the last decade, international state controls vary greatly and will impact future technical direction.

Based on this brief comparison, the traditional notions of deterrence theory developed during the Cold War may not fully extend to other asymmetric threats (Space, Cyber), but that does not deny the successful historic use of deterrence the centuries before nuclear weapons and the notion of the use internationally with modern asymmetric threats.

7.1 Cyber Deterrence

With 90% of cyberspace networks and infrastructure owned and operated by private industry, deterrence in cyber is developing and evolving internationally.[112] In the U.S., the distributed nature of titles and authorities amongst government entities makes the defense and response to cyber attacks complex.

In 2013, the U.S. released Presidential Policy Directive/PPD-21 focused on Critical Infrastructure Security and Resilience which advances a national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure.[113] The nature of this document focused on a defensive cyber infrastructure for the United States inclusive of both civilian and military networks. Since the release of PPD-21, defensive cyber efforts have been implemented providing a foundation of protections for the U.S. networks (Figure 1).

[112] U.S. Department of Defense, "The Department of Defense Cyber Strategy," http://www.defense.gov/home/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf (April 2015).
[113] U.S. Office of the President, "Presidential Policy Directive – Critical Infrastructure Security and Resilience," https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil (February 12, 2013).

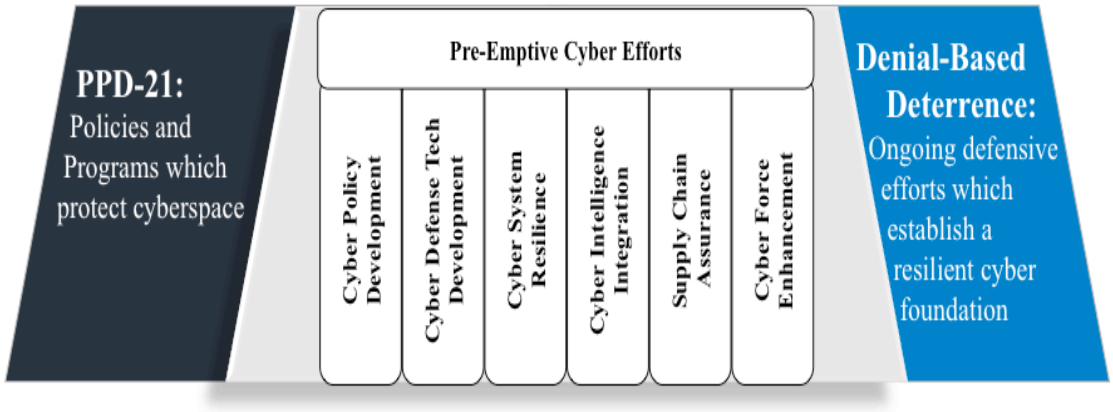

Figure 7.1
Defense/Denial Based Deterrence implemented via PPD-21.[114]

Recognizing that "making oneself invincible" in cyberspace is costly (and complete security cost prohibitive in the current model), the U.S. government is moving toward implementation of defenses via PPD-21 using cost/risk-based decision structure for cyber defenses that may be similar to that discussed by Wyss, et al.[115] In this structure, government decision-makers perform risk-based cost-benefit prioritization of security investments.

A coordinated risk-based, defensive structure thwarts some threats, but the porous nature of the internet and cost of cyber based defense drives a state away from utilizing a purely defensive deterrence structure and drives a state to consider a combined punishment-based/denial-based model (Figure 2). In a Punishment-based Deterrence scenario, the state responds with escalation following a cyber-based attack that is customized based on the attack. Response may include, but is not limited to, criminal action (naming and shaming, fines, incarceration), diplomatic action (demarche), economic sanctions (banking restrictions, trade bans), offensive cyber response (DDOS), coordinated ally response, and kinetic response.

In this model, a cyberattack may see immediate and overwhelming force in retaliation to the attack.

[114] Heather Blackwell, Chrisma Jackson, and Jennifer McCann, An Analytic Framework for United States Cyber Deterrence," Research Project Presentation on April 28, 2015. Harvard Kennedy School Research Paper for National Security Fellows.
[115] Gregory D. Wyss, John P. Hinton, Katherine Dunphy-Guzman, John Clem, John Darby, Consuelo Silva, and Kim Mitchiner, "Risk-Based Cost-Benefit Analysis for Security Assessment Problems," *Security Technology (ICSST)*, 2001 IEEE International Carnahan Conference on Security Technology, San Jose, CA, Oct 5-8, 2010, 286-295.

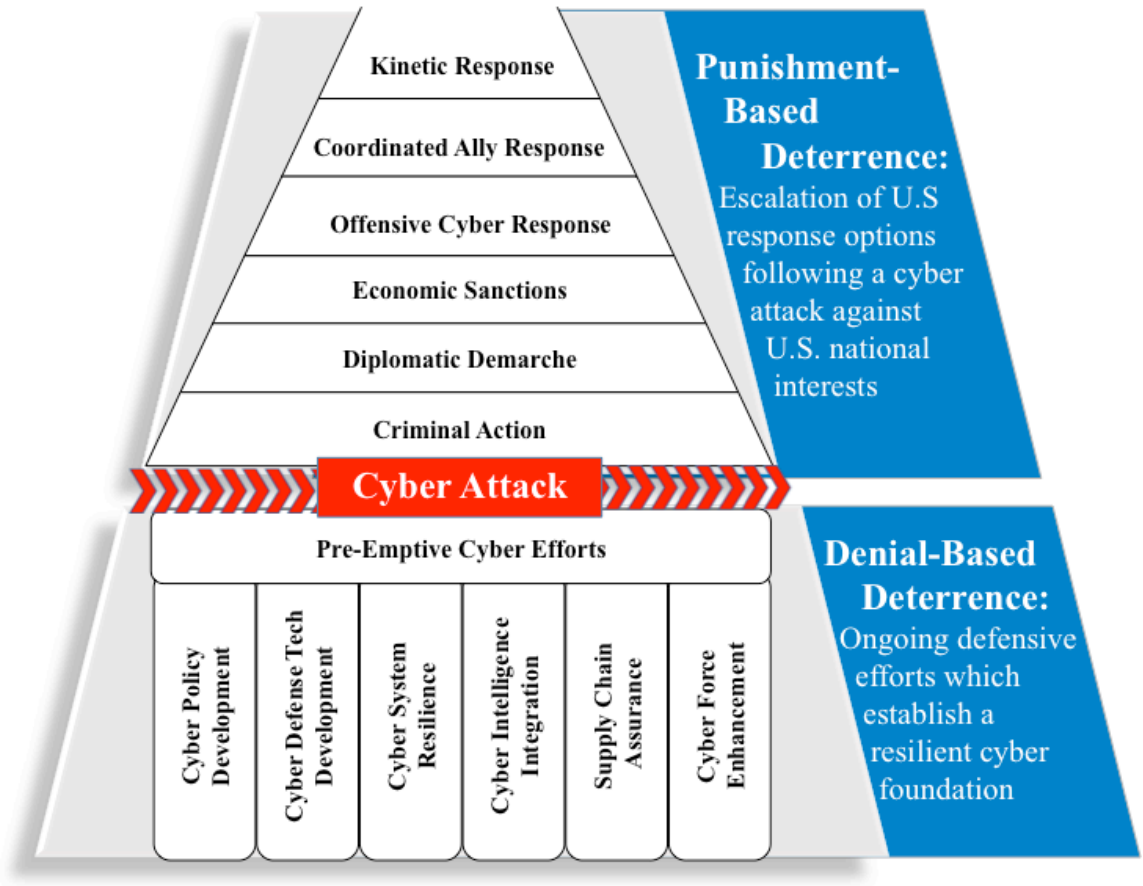

Figure 7.2
Combined Punishment/Denial Framework for Cyber Deterrence

7.2 International Demonstrations of Force or Deterrence: International Examples

The notion of the extension of deterrence to cyber has been discussed academically, but discussions at the state level have been limited. Based on recent attacks/ responses as well as media reports, U.S., Russia and China appear to be building their attack/response profiles.

In the U.S., several recent incidents and reports confirm responses and demonstrations of force may be highlighted. In 2012, the U.S. Marines confirmed the use of cyberattacks in Afghanistan including use of tools to "get inside his (enemy) nets, infect his command-and-control, and in fact defend myself against his almost constant incursions to get inside my wire, to affect my operations."[116] Late in 2014, international headlines were filled with the news related to the North Korean attacks on Sony Pictures Entertainment. In response for those attacks, the U.S reportedly is leading a criminal investigation, diplomatic demarche, diplomatic sanctions, offensive cyber attacks, and international coordination (with China).[117] In the spring of 2015, President Obama and Prime

[116] Raphael Satter, "U.S. General: We hacked the enemy in Afghanistan," *Associated Press* August 24, 2012 on USA Today, http://usatoday30.usatoday.com/news/military/story/2012-08-24/afghan-cyberattack/57295168/1.
[117] David Robb, "Sony Hack: A Timeline," *Deadline.com*, http://deadline.com/2014/12/sony-hack-timeline-any-pascal-the-interview-north-korea-1201325501/(accessed December 19, 2014); Jim Acosta and kevin Liptak, "U.S. Slaps New Sanctions on North Korea after Sony Hack," *CNN.com*, http://www.cnn.com/2015/01/02/politics/new-sanctions-for-north-korea-after-sony-hack/index.html(accessed March 7,

Minister Cameron announced a cooperative cyber alliance and "joint war games" with the U.K.[118]

Coordinated cyberattacks on Estonia, originating from Russia, in 2007 disrupted the communications and operations of the banks, parliament, ministries, newspapers, and TV in the state.[119] These attacks were a clear demonstration of offensive capability and force. Following these attacks in 2013, Russia announced the creation of a Cyber Army including the establishment of a Cyber Defence Centre citing a "need to gather intelligence as with traditional espionage; the ability to disrupt communications to hamper conventional forces, and also the ability to deliver cyber-assaults on critical infrastructure – including the banking sector…".[120]

China has had an active government cyber program restricting internal access to parts of the larger internet, nicknamed the "Great Firewall of China," for years, but most recent reports in a March 2015 PLA publication openly discuss specialized units devoted to wage war on computer networks. The units include:

- Specialized military forces - fighting offensively and defensively on networks.
- Experts from civil society organizations - Ministry of State Security (equivalent to China's CIA), and the Ministry of Public Security (equivalent to the FBI) – who are authorized to conduct military leadership network operations.
- External entities - non-government entities (state-sponsored hackers) mobilized for network warfare operations.[121]

Following the March publication, the new DDoS tool, nicknamed "The Great Cannon", was hijacking traffic to (and presumably from) individually IP addresses whereas restricting users from accessing those addresses on the net. "Where the Great Firewall was a tool for largely passive censorship – preventing access to material and providing the Chinese state with the ability to spy on its residents – the Great Cannon provides the ability to effectively rewrite the internet on the fly."[122]

As we look across the world, the build-up and leveraging of cyber as a platform is being leveraged internationally amongst the major powers: U.S. Russia, and China. Acts demonstrating the three "Cs": demonstrations of technology/joint war games (Capability), defining clear lines of attack (Clarity), and the willingness of governments to respond via use of force (Credibility) draw new meaning and extension to the use of deterrence theory.

2015); Mike Chinoy, "A Cyber Conflict with North Korea is 'Dangerous Uncharted Territory'," *CNN.com,* http://www.cnn.com/2014/12/23/world/asia/north-korea-cyber-conflict-chinoy-qa/index.html (accessed March 7, 2015); Nicole Perlroth and David E. Sanger, "North Koreas Loses its Link to the Internet," *The New York Times* December 22, 2014, http://www.nytimes.com/2014/12/23/world/asia/attack-is-suspected-as-north-korean-internet-collapses.html.

[118] U.S. Office of the President, "FACT SHEET: U.S.-United Kingdom Cybersecurity Cooperation," *Office of the Press Secretary* January 16, 2015, https://www.whitehouse.gov/the-press-office/2015/01/16/fact-sheet-us-united-kingdom-cybersecurity-cooperation.

[119] Charles Clover, "Kremlin-backed group behind Estonia cyber blitz," *Financial Times* March 11, 2009, http://www.ft.com/cms/s/0/57536d5a-0ddc-11de-8ea3-0000779fd2ac.html.

[120] Eugene Gerden, "$500 million for new Russian cyber army," *SC Magazine* November 6, 2014, http://www.scmagazineuk.com/500-million-for-new-russian-cyber-army/article/381720/.

[121] Mohit Kumar, "China finally admits it has Army of Hackers," *The Hacker News* March 19, 2015, http://thehackernews.com/2015/03/china-cyber-army.html.

[122] Alex Hern, ""Great Cannon of China" turns internet users in to weapon of cyberwar," *The Guardian* April 13, 2015, http://www.theguardian.com/technology/2015/apr/13/great-cannon-china-internet-users-weapon-cyberwar.

References

Acosta, Jim and Kevin Liptak. 2015. U.S. Slaps New Sanctions on North Korea after Sony Hack. *CNN.com*. Accessed March 7, 2015, http://www.cnn.com/2015/01/02/politics/new-sanctions-for-north-korea-after-sony-hack/index.html.

Allison, Graham T. 2004. *Nuclear terrorism: the ultimate preventable catastrophe*. New York: Times Books/Henry Holt.

Allison, Graham. 2014. Interview with Heather Blackwell, Chrisma Jackson, and Jennifer McCann Personal interview. Harvard Kennedy School, Cambridge, MA, November 4.

Blackwell, Heather, Chrisma Jackson, and Jennifer McCann. 2015. An Analytic Framework for United States Cyber Deterrence. Research Project Presentation on April 28. Harvard Kennedy School Research Paper for National Security Fellows.

Brodie, Bernard. 1959. *Strategy in the missile age*. Princeton, N.J.: Princeton University Press.

Chinoy, Mike. 2015. A Cyber Conflict with North Korea Is 'Dangerous Uncharted Territory'. *CNN.com*. Accessed March 7, 2015. http://www.cnn.com/2014/12/23/world/asia/north-korea-cyber-conflict-chinoy-qa/index.html.

Charles Clover, "Kremlin-backed group behind Estonia cyber blitz," *Financial Times* March 11, 2009, http://www.ft.com/cms/s/0/57536d5a-0ddc-11de-8ea3-0000779fd2ac.html.

Gerden, Eugene. 2014. $500 million for new Russian cyber army. *SC Magazine* November 6. http://www.scmagazineuk.com/500-million-for-new-russian-cyber-army/article/381720/.

Hern, Alex. 2015. "Great Cannon of China" turns internet users in to weapon of cyberwar. *The Guardian* April 13. http://www.theguardian.com/technology/2015/apr/13/great-cannon-china-internet-users-weapon-cyberwar.

Kumar, Mohit. 2015. China finally admits it has Army of Hackers. *The Hacker News* March 19. http://thehackernews.com/2015/03/china-cyber-army.html.

Parrish, Karen. 2013. Official describes Evolution of Space Deterrence. *American Forces Press Service*. U.S. Department of Defense. http://www.defense.gov/news/newsarticle.aspx?id=120818.

Perlroth, Nicole and David E. Sanger. 2014. North Korea Loses Its Link to the Internet. *The New York Times*. December 22. http://www.nytimes.com/2014/12/23/world/asia/attack-is-suspected-as-north-korean-internet-collapses.html.

Robb, David. 2014. Sony Hack: A Timeline. *Deadline.com*. Accessed December 19, 2014, http://deadline.com/2014/12/sony-hack-timeline-any-pascal-the-interview-north-korea-1201325501/.

Satter, Raphael. 2012. U.S. general: We hacked the enemy in Afghanistan. *Associated Press*. USA Today. http://usatoday30.usatoday.com/news/military/story/2012-08-24/afghan-cyberattack/57295168/1.

Schelling, Thomas C. 1966. *Arms and influence*. New Haven: Yale University Press.
Tzu, Sun, *The Art of War*, Trans. Lionel Giles, 2009, file:///Users/User/Downloads/taowde.pdf.

U.S. Department of Defense. 2015. The Department of Defense Cyber Strategy. Department of Defense: April. http://www.defense.gov/home/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

U.S. Office of the President. 2013. Presidential Policy Directive -- Critical Infrastructure Security and Resilience. February, 12. https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

U.S. Office of the President. 2015. FACT SHEET: U.S.-United Kingdom Cybersecurity Cooperation. *Office of the Press Secretary*, January 16. https://www.whitehouse.gov/the-press-office/2015/01/16/fact-sheet-us-united-kingdom-cybersecurity-cooperation.

Wyss, Gregory D., John P. Hinton, Katherine Dunphy-Guzman, John Clem, John Darby, Consuelo Silva, and Kim Mitchiner. 2011. Risk-Based Cost-Benefit Analysis for Security Assessment Problems. Security Technology (ICSST), 2001 IEEE International Carnahan Conference on Security Technology, San Jose, CA, Oct 5-8, 2010, 286-295.