Cyber Conflict History: Assessing State Responsibility and Other Major Trends

Jason Healey and Karl Grindal, Cyber Conflict Studies Association

Research derived from the book *A Fierce Domain; Conflict in Cyberspace 1986 to 2012,* published in June 2013.

Explorations in Cyber International Relations
Massachusetts Institute of Technology Harvard University
Workshop on
Cyber Security & the Governance Gap
MIT, January 6 and 7, 2014

Problem

Even in its earliest history, cyberspace had disruptions, caused by malicious actors, which have gone beyond being mere technical or criminal problems. These cyber conflicts exist in the overlap of national security and cyberspace, where nations and non-state groups use offensive and defensive cyber capabilities to attack, defend, and spy on each other, typically for political or other national security purposes.

In other areas of national security, newly hired people learn their field through the vicarious experience of those that have gone before. Understanding history is the main way to turn the experience of the past generations into cumulative knowledge, such as by teaching military officers the implications of Gettysburg, Inchon, Trafalgar, or MIG Alley. Yet, the US government and military have almost completely ignored cyber history. Even though major conflicts have occurred in cyber conflict since the mid-1980s, these are largely unknown and untaught, making it far more likely we will continue repeating the same mistakes.

We sought to mine cyber conflict history to develop this vicarious experience and create a narrative of "cyber mindedness" to connect past, present and future cyber cadres. **While historical analysis can address numerous questions, we sought to address one of the common maxims in cyber international relations that cyber threats are not attributable.**

Methods

***Cyber conflict:* When nations and non-state groups use offensive or defensive cyber capabilities to attack, defend, and spy on each other, typically for political or other national security purposes.**

A comparative analysis of major cyber incidents should be grounded in clear definitions and structured classifications. To do this we started with a clear definition of cyber conflict. From this definition we compiled in *A Fierce Domain* a set of case studies on major cyber incidents that had strategic effect to the United States. Case studies were selected based on interviews with historical practitioners and subject matter experts, as well as sources that referred to the incidents as "wake-up" calls (see below). The outline for each case study hoped to address the 1) geopolitical context, 2) adversaries, and 3) attack and aftermath of each incident.

Utilizing this reference material, we now had the ability to look at major trends in US cyber conflict history and to challenge contemporary notions of cyber conflict with a historical analysis. For example, one major theme from these incidents was the critical role of the private-sector in defending against cyber threats. To address the question of national attribution, Jason Healey developed a spectrum of attribution, and then a set of questions for assigning attribution. Based on how case studies completed the questionnaire we could now assign responsibility.

Cyber "Wake-Up Calls"

1. Morris Worm
2. ELIGIBLE RECIEVER and SOLAR SUNRISE
3. MOONLIGHT MAZE
4. Chinese Espionage
5. Estonia and Georgia
6. BUCKSHOT YANKEE
7. OLYMPIC GAMES / Stuxnet

The Research

The Spectrum of State Responsibility

1.State-prohibited. The national government will help stop the third-party attack.
2.State-prohibited-but-inadequate. The national government is cooperative but unable to stop the third-party attack.
3.State-ignored. The national government knows about the third-party attack but is unwilling to take any official action.
4.State-encouraged. Third parties control and conduct the attack, national government encourages them as a matter of policy.
5.State-shaped. Third parties control and conduct the attack, but the state provides some support.
6.State-coordinated. The government coordinates third-party attackers, such as by "suggesting" operational details.
7.State-ordered. The state directs third-party proxies to conduct the attack on its behalf.
8.State-rogue-conducted. Out-of-control elements of cyber forces of the state conduct the attack.
9.State-executed. The state conducts the attack using cyber forces under their direct control.
10.State-integrated. The state attacks using integrated third-party proxies and its own cyber forces.

Analysis of State Responsibility

Analytical Element	Assessment of the Estonian Cyber Attacks of 2007	Assessment of the Georgian Cyber Attacks of 2007	Assessment of the Stuxnet Cyber Attacks
Attack Traced to Nation	Many traced to Russia	Many traced to Russia (and in particular to Russian organized crime)	Not applicable
Attack Traced to State Organization	Some trace to Russian state institutions	No Strong evidence	Not applicable
Attack Tools or Coordination in National Language	In Russian	In Russian	Partial
State Control over the Internet	Partial but growing	Partial but growing	Not applicable
Technically Sophisticated Attack	Not particularly sophisticated	Yes	Highly
Sophisticated Targeting	Not particularly sophisticated	No	Highly
Popular Anger	Strong	Broad anger within Russia	Low
Direct Commercial Benefit	Low	Low (But inconclusive)	Low
Direct Support of Hackers	No evidence	None	Not applicable
Correlation with Public Statements	Comments by both government and individuals	Strong	Very High: US and Israel
Lack of State Cooperation	Russia refused to cooperate	Russia did not cooperate	Possible: US
Cui Bono?	None	Russia	High: US, Israel
Correlation with National Policy	Strong	Very strong	High: US, Israel
Correlation with Physical Forces	Moderate	Very Strong	Moderate: US, Israel

Preliminary Results/Results

Assessment of State Responsibility

Estonia Case Study	High confidence that the attacks on Estonia were at least encouraged by the Russian government
Georgia Case Study	High confidence that the attacks on Georgia were at least ignored by the Russian government; Moderate confidence they were state-shaped or state-coordinated by the Russian government
Stuxnet Case Study	Medium confidence that Stuxnet was a state-executed attack by the United States and/or Israel

Other Lessons & Findings from our Cyber Past

From the history of cyber conflict, key lessons and findings emerge and each of these carries significant policy implications for cyber defenders and policymakers today:

•Cyber conflict has changed only gradually over time; thus, historical lessons derived from past cases are still relevant today (though these are usually ignored).
•The probability and consequence of disruptive cyber conflict have often been hyped, while the real impacts of cyber intrusions have been consistently underappreciated.
•The more strategically significant a cyber conflict is, the more similar it is to conflicts on the land, in the air, and on the sea—with one critical exception.

This critical exception is the role of the private-sector. As the infrastructure of the Internet is privately owned and operated, **governments rarely play a central role in mitigating cyber conflicts.** Rather, a nation's ability to defend themselves has relied on their cooperation with private-sector actors.

The private sector tends to have agility, subject matter expertise and their 'hands-deep' in cyberspace, giving them the decisive role in resolving most serious cyber attacks and conflicts. Governments tend to have staying power, larger resources, and access to other levers of power. Successful Internet governance is built on the strengths of each.

Author and Affiliation

Jason Healey is the director of the Cyber Statecraft Initiative at the Atlantic Council, working to demystify the overlap of traditional national security and cyberspace by focusing on international cooperation, completion, and conflict in cyberspace. He has worked on cyber issues since the 1990s as a policy director at the White House, as executive director at Goldman Sachs Asia, and as a US Air Force intelligence officer. As a widely published expert on cyber conflict and statecraft, he is a board member of Cyber Conflict Studies Association and lecturer at Georgetown University.

Karl Grindal is an associate at Delta Risk LLC where he provides strategic, policy and research services for government clients. Karl is also the project manager for the Cyber Conflict Studies Association (CCSA) history efforts and served as the Associate Editor of *A Fierce Domain.* His academic background includes a Bachelor of Arts in Government from Wesleyan University and a Master of Public Policy degree from Georgetown University.