Cyber Strategy:
The Evolving Nature of Cyber Power

Brandon Valeriano
Marine Corps University
Donald Bren Chair of Armed Politics
drbvaler@gmail.com
Enigma v3
The Power of Cyber Weaponry?

- Just how useful are cyber strategies?
- Cyber enabled tools will not replace traditional elements of strategy, statecraft, or leverage.
- Methods thought to be cheap, easy, and fast are no substitute for traditional strategy. Effectiveness is contingent on other factors.
- Innovation in military and diplomatic affairs is rarely revolutionary, instead it is evolutionary process replete with unintended consequences and cascading effects.
Methods and Progress

- Need to avoid the “megafauna” approach to cyber security.
- Large recent history of cyber events
- Empirical analysis of cyber conflicts over the last two decades helps paint a different picture of the efficacy of cyber strategies
- Stories are useful if imbedded and extracted from a large corpus of events
- Cyber actions have yet to achieve “knock out” effects
- Yet, there remains paths to chaos and destruction in the domain.
The Situation and Problem

- Major powers now attempt to employ coercive cyber strategies to gain a position of advantage relative to their rivals.
- Small states and non-state actors attempt to use cyber operations to punch above their weight to maximize their goals.
- These operations seek to achieve effects and compel the enemy to change behavior.
- However, few have uncovered how to measure and understand the effects of cyber conflict and its coercive potential.
- The efficacy of cyber strategies remains an open question.
The Promise of Impact

- 2017 United States *National Security Strategy*: “Cyberattacks offer adversaries low cost and deniable opportunities to seriously damage or disrupt critical infrastructure, cripple American businesses, weaken our Federal networks, and attack the tools and devices that Americans use every day to communicate and conduct business.”

- Cyber revolutionists see lines of code as “potent cyber weapons” that create “strategic instability” (Kello 2013: 8).

- Mazanec (2015: 4): “cyber warfare capabilities are leading to a new [revolution in military affairs] RMA, wherein cyber capabilities will play an increasing desirable role in military conflicts.”
Coercion and Compellence

- Coercion is the use of threats, punishment, or escalation of costs during a crisis or conflict to alter foreign policy behavior.

- Cyber coercion involves digitally exploiting “the power to hurt” and escalating the costs of taking certain actions.

- Compellence vs Deterrence: “a threat intended to make an adversary do something and a threat intended to keep an adversary from doing something” (Schelling 1966)

- Cyber operations shape how rivals manage crises. An actor could compel an adversary short of physical attack or signal the risks of further escalation.
Cyber is not the droids we are looking for...

- Cyber campaigns are neither as revolutionary nor as novel as they seem when evaluated with evidence.
- Restraint: adversaries on the digital front are constrained in their options and are unlikely to engage in cyber conflict because of the normative restrictions, proliferation of cyber weapons, and risk inherent with untested options. (Valeriano and Maness 2015)
- Empirical-based evidence suggests that cyber strategies produce limited coercive effects and actually limit escalation (Valeriano, Jensen, and Maness 2018).
Theory of Cyber Coercion

- We find that the utility of cyber coercion as a form of political warfare optimized for the 21st century lies in ambiguous signaling.
- Covert attempts to demonstrate resolve that rely on sinking costs and raising risks to shape rival behavior
- Disruption: Harassment, probe adversary and signal intent
- Espionage: Manipulate data and perceptions, alter balance of information
- Degrade Operations: Covert efforts to deny and sabotage.
Dyadic Cyber Incidents and Dispute (DCID) Dataset, version 1.1 (Maness, Valeriano, and Jensen 2017) investigate the coercive content of cyber operations by coding operational success and concessions from 2000 to 2014.
Major Findings

- We find that cyber coercion produces only limited concessions. Examining 192 episodes of cyber coercion between rivals, only 5.2 percent achieve compellent success.

- Cyber degradation is more likely to achieve concessions than other forms of cyber strategy. Yet, even this finding is subject to caution. Most of the degradation events evoking concessions involve the United States.

Table 3.3: Degradation Cyber Incidents that produce Concessions

<table>
<thead>
<tr>
<th>Initiator</th>
<th>Target</th>
<th>Name</th>
<th>Start date</th>
<th>Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>U.S.</td>
<td>China</td>
<td>Cisco Raider</td>
<td>2/29/2006</td>
<td>Keystroke &amp; Botnet</td>
</tr>
<tr>
<td>U.S.</td>
<td>China &amp; North Korea</td>
<td>Boxing Rumble</td>
<td>1/1/2008</td>
<td>Botnet</td>
</tr>
<tr>
<td>U.S.</td>
<td>Russia</td>
<td>Buckshot Yankee</td>
<td>11/26/2008</td>
<td>Virus &amp; Botnet</td>
</tr>
<tr>
<td>U.S. and Israel</td>
<td>Iran</td>
<td>Stuxnet</td>
<td>6/1/2009</td>
<td>Worm</td>
</tr>
<tr>
<td>U.S.</td>
<td>China</td>
<td>Arrow Eclipse</td>
<td>5/27/2007</td>
<td>Keystroke &amp; Worm</td>
</tr>
<tr>
<td>U.S.</td>
<td>China</td>
<td>NSA Fourth Party</td>
<td>7/1/2009</td>
<td>Keystroke &amp; Worm</td>
</tr>
<tr>
<td>U.S.</td>
<td>China</td>
<td>Shotgiant</td>
<td>3/10/2010</td>
<td>Trojan</td>
</tr>
</tbody>
</table>
Major Findings

- Neither past cyber incidents nor a state’s latent cyber power are empirically associated with concessions. Military and economic power appear to be better explanatory factors than cyber operations.

- Even when cyber exchanges between rivals escalate, they remain limited in scope outside of ongoing military conflict (Russia-Georgia 2008, Russia-Ukraine 2014).

Table 3.12: Escalation Hazards as a Result of Cyber Operations

<table>
<thead>
<tr>
<th></th>
<th>Cyber Escalation odds-ratio (Coefficient)</th>
<th>Diplomatic Escalation odds-ratio (Coefficient)</th>
<th>Economic Escalation odds-ratio (Coefficient)</th>
<th>Military Escalation odds-ratio (Coefficient)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Past Cyber</td>
<td>11.892** (2.746)</td>
<td>.789 (-.237)</td>
<td>1.502 (.407)</td>
<td>1.490 (.399)</td>
</tr>
<tr>
<td>Regime Type</td>
<td>5.587 (1.720)</td>
<td>.666 (-.407)</td>
<td>4.190 (1.433)</td>
<td>.820 (-.199)</td>
</tr>
<tr>
<td>Cyber Capacity</td>
<td>1.060 (.059)</td>
<td>1.513 (.414)</td>
<td>.894 (-.112)</td>
<td>1.092 (.088)</td>
</tr>
<tr>
<td>CINC</td>
<td>.935 (-.067)</td>
<td>1.106 (.101)</td>
<td>.987 (-.013)</td>
<td>.979 (-.022)</td>
</tr>
<tr>
<td>Military Power</td>
<td>1.003 (.003)</td>
<td>1.101 (.012)</td>
<td>.999 (-.001)</td>
<td>.998 (-.002)</td>
</tr>
<tr>
<td>Economic Power</td>
<td>.969** (-.048)</td>
<td>.926** (-.077)</td>
<td>1.000 (.000)</td>
<td>1.010 (.010)</td>
</tr>
</tbody>
</table>

***p<.01, **p<.05, *p<.10
N=384
Country Specific Results: Russia

- Russia is a diminished power that has a corrupt political system, a flailing economy, and limitations on military spending.

- Its cyber strategy of disruption and disinformation is a cheaper way to seek out its political goals in the international system.

- Overblown view of impact, the Russia election hack of 2016 was neither cheap nor very effective, but it was noticeable and insidious
Country Specific Results: China

- China is the rising great power that is attempting to bridge the gap economically, militarily, and technologically with its status quo competitor, the United States.

- Its strategy of digital espionage that steals technological secrets of the more advanced Western powers as well as Japan is an attempt to hasten this goal of parity with the U.S.

- New moves focused on protecting interests and preventing internal revolt.
Country Specific Results: U.S.

- The United States has technological superiority over both Russia and China.
- It will use its major cyber capabilities sparingly so as not to give its adversaries access to its superior capabilities.
- Precision strike complex dominates strategy
The Cyber Challenge

อม Unpacking the strategic logic of cyber conflict as a new means of coercing political opponents demands that we understand the realities and limits of this innovation.

❑ We urge caution. States seeking to leverage cyber actions to achieve decisive effects are likely to be disappointed.

❑ Digital effects have been slow emerge and tend to amplify rather than replace traditional instruments of power.
The Call to Action

- Problem of Threat Inflation
- Unappreciated strategic risks: cascades, blowback, one shot weapons, untested
- Need for Empirical research to back up dramatic claims
- Understand the process of Modern Political Warfare
- The true challenge in our midst, cyber repression.
Questions/Comments?