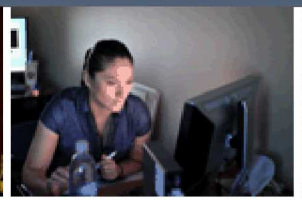
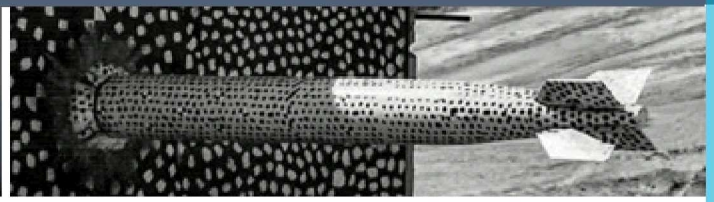
SAND2019-10000C

The Civilian Cyber Strategic Initiative

Briefing to Sandia-UC Davis Research Partnership Symposium

13 August 2019

PRESENTED BY

Michael Minner

Civilian Cyber Strategic Initiative

Jeffrey J. Apolis, Benjamin J. Bonin, Ruby Booth, Rob Forrest, Ann Hammer, John P. Hinton, Ryan Jacobson, David Johnson, Christopher Mairs, Trisha Miller, Michael Minner, Nerayo Teclemariam, Eva C. Uribe, Lynn Yang

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

We cannot solely rely on 'perfect defense' in cyberspace

Global civilian IT and control systems infrastructures are foundational to U.S. economic and political health, as well as to soft power projection abroad. Adversaries (nation states, non-state actors, and criminal organizations) are using increasingly sophisticated technical capabilities to disrupt or manipulate these systems.

Some [attacks] are tailored to achieve very tactical goals while others are implemented for strategic purpose, including the possibility of a crippling cyberattack against our critical infrastructure."
-Dan Coats, Director of National Intelligence

Foreign actors are reconnoitering and developing access to U.S. critical infrastructure systems, which might be quickly exploited for disruption if an adversary's intent became hostile"
–James Clapper, Former Director of National Intelligence

Anticipating and reacting to the latest cyber threat is a ceaseless endeavor that requires ever more resources and manpower. This approach to cybersecurity is not efficient, effective, nor sustainable in light of escalating cyber threat capabilities. We must recognize today's realities: resources are limited, and cyber threats continue to outpace our best defenses.
– 2018 DOE Multiyear Plan for Energy Sector Cybersecurity

The unfortunate reality is that, for at least the coming five to ten years, the offensive cyber capabilities of our most capable potential adversaries are likely to far exceed the United States' ability to defend and adequately strengthen the resilience of its critical infrastructures.
– Defense Science Board Taskforce on Cyber Deterrence (2017)

Deterrence of cyber adversaries is U.S. policy

National Security Strategy (2017)

Priority actions include "deter and disrupt malicious cyber actors."

National Cyber Strategy (2018)

Strengthen U.S.'s ability "to deter and if necessary punish those who use cyber tools for malicious purposes."

Sec. *1636 of the Defense Authorization Act (2019)*

The U.S. should "deter if possible, and respond to when necessary" all cyber attacks and activities that target vital U.S. interests.

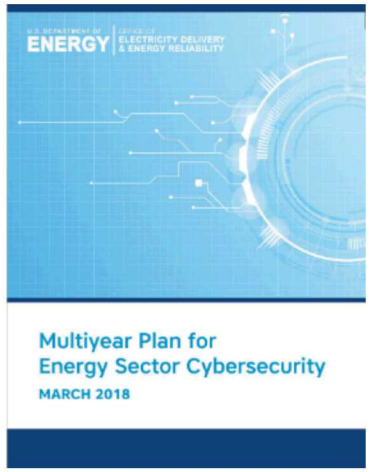
U.S. CYBERCOM Command Vision (2018)

"Adversaries operate continuously below the threshold of armed conflict to weaken our institutions and gain strategic advantages."

Recommendations to the President on Deterring Cyber Adversaries (2018)

Desired end states of U.S. cyber deterrence efforts will be:

1. A continued absence of cyber attacks that constitute a use of force
2. Reduction in destructive, disruptive, or destabilizing cyber activities against U.S. interests below the threshold of the use of force



What is deterrence?

Deterrence involves creating conditions that dissuade adversaries from taking unwanted actions, because they perceive that the costs exceed the benefits.

- Involves the entire spectrum of government and private sector influence and power.

- **Deterrence by punishment**
  Perception of unacceptable costs
- **Deterrence by denial**
  perception of insufficient benefits

What makes deterrence counterthreats effective?

A distillation of deterrence theory literature shows how deterrence counterthreats fail. An effective deterrence counterthreat must have all of the following components:

COMMUNICATED	X	CREDIBLE Principled X Rational	X	CAPABLE Executable X Painful (Costly)	X	CALCULATED
The protagonist's counterthreat must be communicated to the antagonist, and the antagonist must observe and understand this communication in the way that the protagonist intended.		The antagonist must perceive that the protagonist's counterthreat aligns with the protagonist's principles, and that it is rational for the protagonist to carry out the counterthreat.		The antagonist must perceive that the protagonist is able to execute the counterthreat, and that the counterthreat will inflict sufficient pain or cost on the antagonist if executed. The antagonist must perceive that the protagonist is capable of influencing the antagonist's cost/benefit analysis.		The antagonist must consider the counterthreat and its implications when choosing a course of action, and must act rationally.

What makes deterrence counterthreats effective?

	COMMUNICATED	X	CREDIBLE Principled X Rational	X	CAPABLE Executable X Painful (Costly)	X	CALCULATED
	The protagonist's counterthreat must be communicated to the antagonist, and the antagonist must observe and understand this communication in the way that the protagonist intended.		The antagonist must perceive that the protagonist's counterthreat aligns with the protagonist's principles, and that it is rational for the protagonist to carry out the counterthreat.		The antagonist must perceive that the protagonist is able to execute the counterthreat, and that the counterthreat will inflict sufficient pain or cost on the antagonist if executed. The antagonist must perceive that the protagonist is capable of influencing the antagonist's cost/benefit analysis.		The antagonist must consider the counterthreat and its implications when choosing a course of action, and must act rationally.
Reasons for Failure	- The adversary misinterprets the counterthreat		- Uncontrolled or uncertain effects - Cost is prohibitive to Blue		- Inability to rapidly attribute with confidence - Lack of rapid detection - Repeated use of the same tools - Inability to understand adversary motivation		- The adversary is not rational, i.e. adversary is reckless
Potential R&D	- Reveal obfuscation tactics - Identify actions through proxies		- Counter "low and slow" operations - Intelligence or Anticipatory Science		- Hardening defenses, e.g. improved moving target defense - Model adversary behavior or decision-making		- Reverse engineer adversary malware

Deterrence of cyber adversaries presents unique challenges

1. Cyberspace is inherently a domain of *constant contact*
2. Attribution of attacks and intrusions is difficult
3. Detection of attacks and intrusions is often delayed
4. Cross-domain deterrence may be escalatory
5. The U.S. is asymmetrically vulnerable in cyberspace
6. There is a lack of domestic norms and laws for responding to cyber incidents
7. There is a lack of international norms and law for conflict and behavior in cyberspace
8. The effects of cyber weapons are uncertain
9. Offensive and defensive cyber operations are difficult to distinguish