SAND2021-12283PE

Sandia National Laboratories

Exceptional service in the national interest

Understanding the Cyber Conflict Landscape

Dr Ruby E. Booth

October 4th 2021

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and 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.

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.

Truths About Cyber Conflict?

Common Cyber Conflict Myths

Myth	Reality
You can't kill people with cyberattacks.	Cyberattacks to critical infrastructure, healthcare, etc. could result in destabilization and many deaths
Cyber deterrence isn't possible. or Cyber deterrence is working.	Cyber deterrence likely functions differently above and below the threshold of armed conflict. Also, discussions of cyber deterrence must include clarity on what you are trying to deter.

Vast Asymmetries

"The unfortunately 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)

Goal States

1. “A continued absence of cyber attacks that constitute a use of force” (No cyber Pearl Harbor)
2. “Reduction in destructive, disruptive, or destabilizing cyber activities against U.S. interests below the threshold of the use of force” (No death by 1000 cuts)

   --National Security Council's Recommendations to the President on Deterring Cyber Adversaries (2018)

3. Global strategic stability

Deterrence of cyber adversaries presents unique challenges

1. Cyberspace is a domain of *constant contact* (many actors interacting with unprecedented speed, remoteness, and scale)
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
10. Greater potential for technological surprise that rapidly alters conflict asymmetries
11. Greater tension in the reveal/conceal dilemma (defense is relatively easy)

Common Unhelpful Categories

Script Kiddies:

Attackers who use tools developed by others

Cybercriminals:

Attackers who hack for profit

Hacktivists:

Attackers who hack for an “ethical” ideology

APT:

Nation state level actors with vast resources who attack for strategic advantage

Understanding Attackers

- Resource level
- Motivation
- Strategic Goal
- Tactical Goal
- Intensity/Commitment
- Number of outsiders/insiders
- Expected system knowledge
- Resource level
- Vulnerability to retailiation

Sample Range of Tools

Tools can be built, borrowed, or bought.

More sophisticated actors are more likely to have many tools available to them.

A less sophisticated tool is not necessarily less damaging to the systems against which it is deployed.

Tools can escape into the “wild.”

Questions?