Sandia National Laboratories

SAND2019-8334D

Civilian Cyber Strategic Initiative: Cyber Deterrence

Ryan Jacobson and David Johnson

The CCSI Team: Jeff Apolis, Ben Bonin, Rob Forrest, Michelle Gonzalez, Ann Hammer, John Hinton, Sarah Low, Christopher Mairs, Trisha Miller, Michael Minner, Jason Reinhardt, Nerayo Teclemariam, Eva Uribe, and Lynn Yang

DETERRENCE: The creation of conditions that dissuade an adversary from taking an action because they perceive that the costs exceed the benefits. Includes all elements of state power and influence.

Cybersecurity Is Currently Inadequate

to defend national critical infrastructure like the electrical grid, healthcare networks, financial institutions, water distribution, etc. "Perfect defense" isn't a viable solution – otherwise we wouldn't experience or fear cyberattacks.

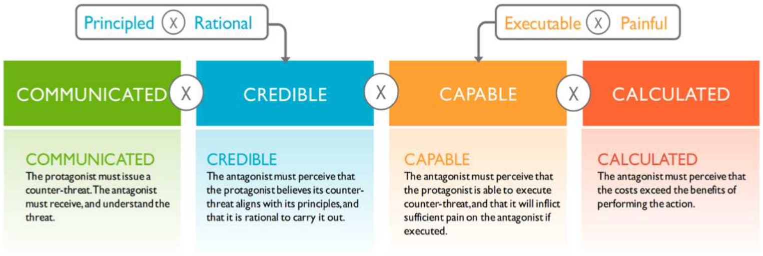
Deterrence Is a Strategy to Consider

especially when confronted with the most severe threats. Abstract & fictional scenarios between "red" and "blue" countries help to illustrate these circumstances and assist us in thinking about possible consequences.

Objectives & Approach

1. Identify usability issues with the deterrence framework previously developed by the CCSI team.
2. Increase theoretical understanding of deterrence metric primitives (primarily *rational* and *executable*).
3. Verify results of prior deterrence scenarios and participate in additional new scenarios to create representative case studies.
4. Discover larger patterns and trends in deterrence measures through a longitudinal study of the history of cyberattacks on the U.S. financial sector.

What Makes an Effective Deterrent Threat?



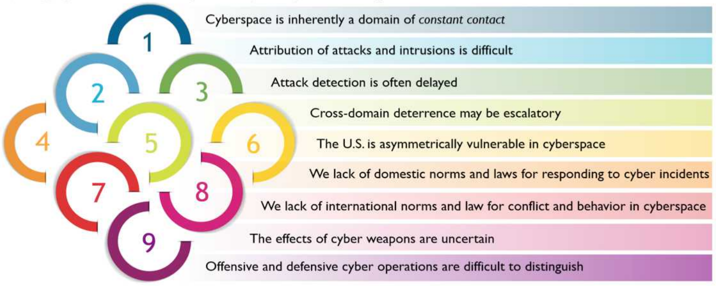
COMMUNICATED: The protagonist must issue a counter-threat. The antagonist must receive, and understand the threat.

CREDIBLE: The antagonist must perceive that the protagonist believes its counter-threat aligns with its principles, and that it is rational to carry it out.

CAPABLE: The antagonist must perceive that the protagonist is able to execute counter-threat, and that it will inflict sufficient pain on the antagonist if executed.

CALCULATED: The antagonist must perceive that the costs exceed the benefits of performing the action.

Challenges Unique to the Cyber Domain



1. Cyberspace is inherently a domain of *constant contact*
2. Attribution of attacks and intrusions is difficult
3. Attack detection is often delayed
4. Cross-domain deterrence may be escalatory
5. The U.S. is asymmetrically vulnerable in cyberspace
6. We lack of domestic norms and laws for responding to cyber incidents
7. We 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

Example Scenario: Cyberattack to Interfere in Elections

Country Red plans to exploit the supply chain for Blue's electronic voting machines to sway the vote for a candidate supportive of Red's economic interests.

Deterrence Action	Deterrent Effective?	Communicated	Principled	Rational	Executable	Painful
Vote verification: distributed ledger technology (each person can verify with a hash or key their vote). **Denial of Victory**	Yes.	Yes. This may have ancillary benefits. Helps increase public's confidence in election integrity.	Yes - this aligns with Blue's principles.	Yes. Would be worth the cost to obtain and deploy this technology. Some challenges: Do you keep all that information in a central database? Is each person required to validate their vote? Government may not have authority/jurisdiction to impose implementation, and it may cost a lot to obtain authority (might fall under executability).	Yes. Blue has the capability to do this - though there is the potential that vendor lock in or existing laws require the use of already purchased machines which do not support this. There also needs to be sufficient time prior to the election to design and implement this technology.	High. Denies Red capability to execute attack.
Threaten legal action against adversaries suspected of working towards seeding the supply chain. **Punishment/ Norms**	Maybe.	Yes. Public or private communication. Requires adequate and accurate communication channels.	Yes.	Yes. The cost of imposing reputation costs (e.g. name and shame) on vendors is low for Blue. Blue is a government, so it should be relatively easy/inexpensive to impose legal consequences. The consequences of carrying out these actions would be low for Blue, and would likely be viewed as worthwhile to bolster deterrence of future supply chain attacks.	Yes. Blue has political mechanisms and cooperation of allies to pursue this.	Medium. Depending on what that legal action is and on who the adversary is. For increased pain, a legal penalty would require large scale or severe economic, reputational, incarceration consequences - must be tailored to specific adversary.
Threaten kinetic attack on Red. **Punishment**	No.	Yes.	No. This conflicts with Blue's adherence to international laws and norms, as well as its own domestic political values.	No. The consequences may include unacceptable kinetic retaliation from Red.	Yes.	High. Kinetic action is inherently painful.

Conclusions

- Deterrence trends more towards punishment as the point of deterrence progresses down the cyber kill chain.
- Pre-judgement of deterrence options is a problem in the current framework.
  - Requiring the analyst to consider the "category" of deterrence prior to brainstorming deterrence options often encourages additional pre-judgement.
- "Executable" often coincides with "Principled" and "Rational" when considering political responses.
- Some options become more rational in combination.

Why U.S. Financial Sector for Focus of Future Work?

- Costs of cyberattacks on financial institutions can vary widely.
- Wide variety of antagonists behind financial attacks.
- Financial institutions are generally more cyber-aware and competent than similarly critical sectors.
- Long history of attacks & public disclosure laws.

Acknowledgements: We especially thank Gio Kao and the Center for Cyber Defenders, and Heidi Ammerlahn and the Division 8000 Energy and Homeland Security leadership for their support.

U.S. DEPARTMENT OF ENERGY

NNSA National Nuclear Security Administration

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.
SAND No. ____________

Sandia National Laboratories

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.