Vengeance and Cyber Conflict

Robert Axelrod

2021

Vengeance

- The drive for vengeance can be powerful.

- Vengeance is often taken with little regard to the cost or consequences, although it feels justified and even rational at the time.

- Thus, the drive for vengeance should taken into account in cyber doctrine, operations, norms and expectations.

Examples

- Cyber examples:
  - ARAMCO after Stuxnet
  - Cyber attacks on Estonia after statue moved
  - Cyber (and other) attacks on Georgia after Russia felt provoked

- Non-cyber examples:
  - A-bomb as vengeance for Pearl Harbor
  - Invasion of Afghanistan as vengeance after 9/11

Implications
for the use of cyber weapons

- To avoid escalation when using cyber weapons,, take care to avoid things that will evoke righteous indignation on the part of the target.

- What evokes vengeance?

An attack can evoke vengeance if:

1. Unprovoked

2. Perfidious attack – underhanded; based on deception; “stab in the back”

3. Disproportionate response

4. Unprecedented (beyond commonly accepted norms)

5. Inappropriate (as response what we did)

6. “Cowardly” in not allowing direct retaliation (like drone strikes); hiding

7. “Cowardly” in not revealing one’s identity

8. Done without warning

9. Insulting

Typical of a Cyber Attack

1. Unprovoked

2. Perfidious: – underhanded; based on deception; “stab in the back”

3. Disproportionate response

4. Unprecedented (beyond commonly accepted norms)

Typical of a Cyber Attack, cont.

5. Inappropriate (as response what we did)

6. "Cowardly" in not allowing direct retaliation (like drone strikes); hiding

7. "Cowardly" in not revealing one's identity

8. Done without warning

9. Insulting

Some Ways to Avoid Evoking Vengeance

Be undetected by target
- But this can backfire if detected

Prevent attribution
- But “false flag” operation is perfidious

Be invisible to public
- Allows face saving non-response

Make “the punishment fit the crime”
- Requires flexible plans

Avoid needless insults