# Is 'Cyber Conflict' the Future of Inter-State Conflict?

## POSC 3610 – International Conflict

Steven V. Miller

Department of Political Science

CLEMSON UNIVERSITY

# Goal for Today

*Discuss whether cyber conflict is the future of inter-state confrontations.*

# MIC of the Day: MIC#4535

# MIC#4535

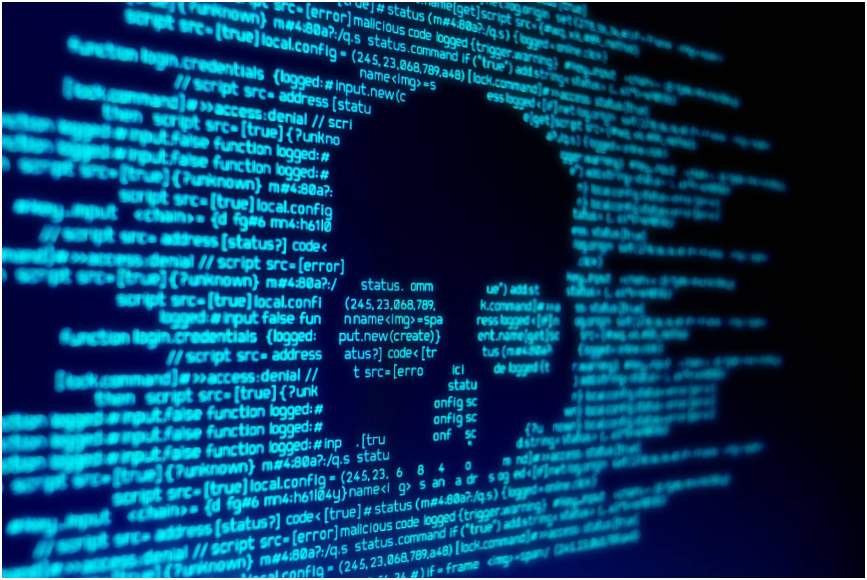
- *Who*: Iran v. United States (Sept. 2006 - 29 Aug. 2007)
- *Why*: Iran's nuclear program
- *What happened*:
  - Sept. 2006: Iran fires on U.S. forces across border
  - 11 Jan. 2007: U.S. seizes Iranian consulate in Iraq, confiscating documents
  - March-April: shows of force by U.S. against Iran

# DCID Cyber Incident of the Day: Stuxnet (#29)

# Stuxnet

- *Who*: U.S. v. Iran (June 1, 2009 - Oct. 1, 2010)
- *Why*: disrupt Iran's nuclear development program
- *What happened*:
  - Preceded by another version of same worm (#27)
  - Malware developers (U.S. + Israel) developed/deployed the so-called "first digital super weapon."
  - A worm spread throughout Iran, targeting nuclear contractors in orbit of Iran's nuclear program.
  - It eventually landed at the Natanz nuclear facility and burned out about 20% of the facilities centrifuges.

# Is ‘Cyber Conflict’ the Future of Conflict?



# The Debate

The debate is typically set up between two camps.

1. Cyber revolutionaries
2. Cyber skeptics

# The Cyber Revolution

Lucas Kello (2013) argues scholars ignore cyber conflict at their own risk.

- Cyber weaponry is expanding the range of possible harms.
- Clear precedent to how else new technology has altered conflict (e.g. tanks, U-boats)
- Technological advances outpace our capacity to understand their harms.
- Cyber capabilities shift balance to offense, further undermining stability.
- Attribution issues pervade this frontier as well.

# *WarGames* (1983)

# *WarGames* (1983)

In this movie, Matthew Broderick:

- Uses his trusty IMSAI 8080 to backdoor through a modem in Sunnyvale, CA to the Cheyenne Mountain Complex
- Triggers a war game (WOPR) that NORAD set up to automate launch control centers
- Cos-plays as the Soviet Union, targeting American cities
- Momentarily convinces NORAD that the Soviets are actually attacking
- Has to trick the computer (otherwise planning a massive response to the Soviets) to learn about no-win situations through tic-tac-toe.
- Induces WOPR to explore no-win scenarios before the launch, thus avoiding the annihilation of all humanity.
- Has a lady friend played by Ally Sheedy (aka the “Basket Case” from *The Breakfast Club*).

# *WarGames* (1983)

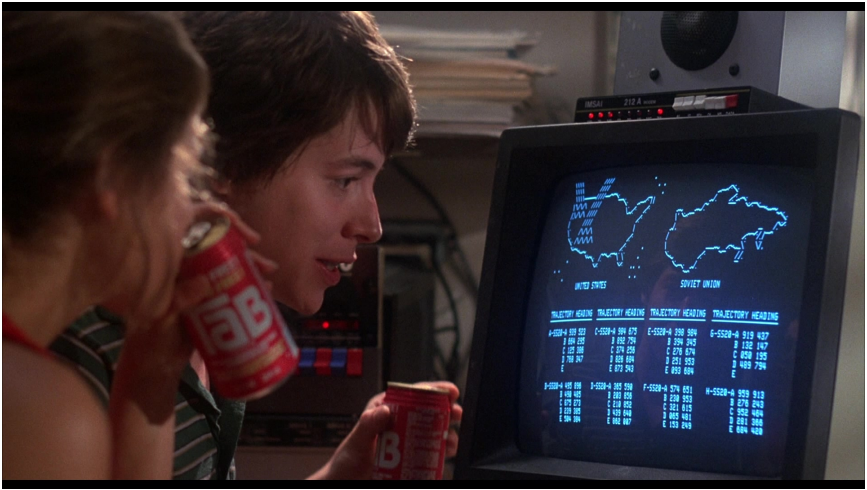

In response to this movie, Ronald Reagan set up the first national task force (NSDD-145) to explore American cyber vulnerabilities.

# Cyber Skepticism

Cyber skeptics dismiss the revolutionary claims here.

- Cyber may be a new domain of conflict, but conflict is still the domain of soldiers on the field.
- We may see (and are seeing more of it), but don't expect it to fundamentally transform conflict processes between states.

# Why Not?


UNITED STATES
SOVIET UNION
TRAJECTORY HEADING
TRAJECTORY HEADING
TRAJECTORY HEADING
TRAJECTORY HEADING

# Cyber Conflict Has Limited Utility

Think of the classic understanding of coercion (Schelling, 1980).

- Compellence: target does something it otherwise wouldn't.
- Deterrence: target doesn't do something it wants to do.
- For both: initiating state signals rewards/punishments to alter target behavior.

The cyber domain doesn't map neatly to this domain.

- Initiator threats lack credibility/reassurance
- Initiating states don't typically tether threats to policy.

We've seen some change in behavior here (i.e. *Solarium*, recent threats from the U.S.)

- But the difficulty is real, as is the lack of utility.

Table 1: Concessionary Behavioral Changes from Cyber Incidents, 2000-2016

| **Cyber Incident Outcome** | **N** |
|---|---|
| No Concessionary Behavioral Change | 254 |
| Concessionary Behavioral Change | 12 |

*Note:*

Data: Dyadic Cyber Incident and Campaign Dataset (DCID), v. 1.5.

# Cyber Offense Depends on a Failure of Cyber Defense

Stuxnet's sophistication belies the kind of cyber incidents we typically see.

- Very few incidents are degradation efforts.
- Relatively few incidents infiltrate networks.

"The best offense is a good defense."

# The OPM Hack (#88)

# Cyber Conflict Has Had Limited Impact

Again, Stuxnet is an anomaly.

- Very few incidents involve physical damage like that.
- There has yet to be a fatality associated with cyber conflict.
- It's difficult to conjure plausible (i.e. non-sci-fi) paths toward it.

# DCID's Severity Scale

1. Probing/packet sniffing
2. Harassment, propaganda, nuisance
3. Stealing critical information
4. Widespread network intrusion
5. Critical infiltration, destruction
6. Critical infiltration, widespread destruction
7. Minimal death (e.g. hacking a car or pacemaker)
8. Critical economic disruption (e.g. shutting down the NYSE)
9. Critical infrastructure shutdown (e.g. power grid hack)
10. Massive death (e.g. Ferris Bueller doesn't save the day)

Table 2: The Severity of Cyber Incidents, 2000-2016

| **Severity Scale** | **Example** | **N** |
|---|---|---|
| Probing/packet sniffing | Operation SnowMan | 9 |
| Harassment, propaganda, nuisance | Las Vegas Sands Hack | 92 |
| Stealing critical information | Spratly island dispute | 97 |
| Widespread network intrustion | 2016 presidential election hack(s) | 53 |
| Critical infiltration, destruction | Stuxnet | 12 |
| Critical infiltration, widespread destruction | Left of Launch | 3 |

*Note:*

Data: Dyadic Cyber Incident and Campaign Dataset (DCID), v. 1.5.

# Conclusion

There are plenty of good reasons to be interested in the trajectory of cyber conflict.

- New technology
- Information/misinformation
- Repressive tool

But do not expect a cyber war to come.

- Cyber conflict is still connected to conflict.
- Cyber aims are typically limited.
- Cyber offense has limited effect.

# Table of Contents