What is 'Cyber Conflict?'

POSC 3610 – International Conflict

Steven V. Miller

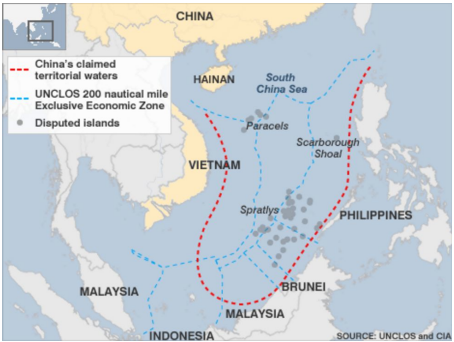
Department of Political Science

CLEMSON UNIVERSITY

Goal for Today

Introduce conflict through so-called 'cyber' capabilities, and what we can say about these patterns so far.

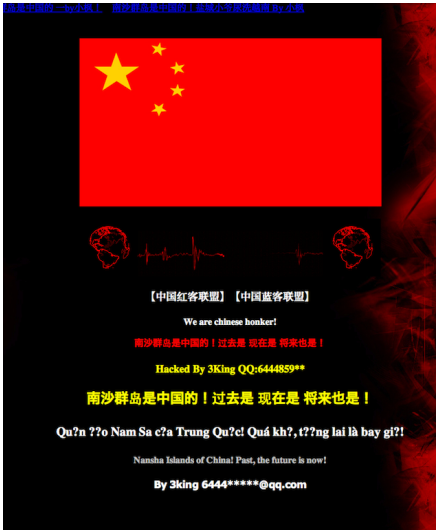
MIC of the Day: Another Spratly Island Confrontation (MIC#4699)



MIC#4699

- *Who*: China v. Vietnam (5 May 2011 - 5 July 2011)
- *Why*: maritime boundary dispute in the South China Sea (Spratly Islands)
- *What happened*:
  - May 2011: China patrol vessel cuts cable on Vietnamese survey boat (in DRV's waters)
  - June 2011: assorted shows of force/vessel chases between both sides
  - July 2011: Chinese soldiers board DRV fishing vessel and assault a crew member.

DCID Cyber Incident of the Day: 209



DCID Cyber Incident #209

- *Who*: China v. Vietnam (3 June 2011 - 6 June 2011)
- *Why*: maritime boundary dispute in the South China Sea (Spratly Islands)
  - A coordinated offensive strike to take down websites/disrupt online activities
- *What happened*:
  - Chinese hackers defaced over 200 Vietnamese websites (~10% of which were government websites)
  - Government websites targeted were non-military, mostly agricultural ministry websites
  - Apparent culprits “3King” and “Xiao Lan” were from “Honker Union”, a hacker collective from Yancheng
  - Hackers also apparently stole some sensitive information from these websites as well.

What is 'Cyber Conflict?'

"Cyber conflict", broadly understood (Valeriano and Manness, 2015) is:

- the use of computational technology
- for malevolent and destructive purposes to
- impact/change diplomatic/military interactions between states

Notice the phenomenon straddles how we might define things like "(militarized, inter-state) confrontations" and "terrorism".

- i.e. there are clear political aims for initiators against targets, including their respective governments.
- However, initiators/targets need not be "official" government actors/forces

Why ‘Cyber?’

The etymology of ‘cyber’ comes from Greek, meaning “governance.”

- Real origin story: rise of ‘cybernetics’ in the 1940s-1960s, studying self-governing systems (e.g. thermostats, cruise control).
- ‘Cyberspace’ first mentioned in 1982 by (SC-born) essayist William Gibson.

Even better origin story:

> *Cyber is such a perfect prefix. Because nobody has any idea what it means, it can be grafted onto any old word to make it seem new, cool — and therefore strange, spooky. [New York magazine, Dec. 23, 1996]*

The Dyadic Cyber Incident and Campaign Dataset (DCID)

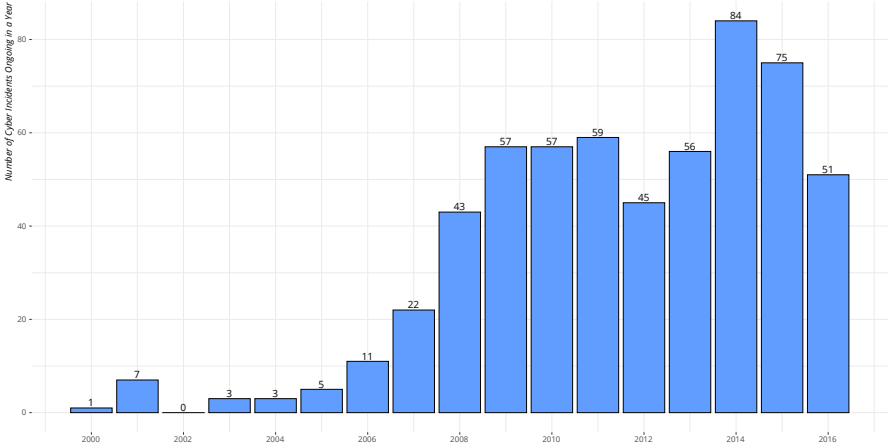
The Dyadic Cyber Incident and Campaign Dataset (DCID) records every instance of dyadic cyber incidents from 2000-2016.

- *Units*: rival dyads (Klein et al., 2006; Thompson, 2001)
- Initiators must be governments or government-sponsored groups.
  - e.g. “Fancy Bear” (i.e. the group that hacked the DNC in 2016) is (from what we know) a GRU outfit.
  - “Berserk Bear” (i.e. the group that hacked the whole damn government from 2019 to 2020) is effectively a state-sponsored (FSB) hacker group, albeit one with a lot of freelancers.
- Targets need not be government actors.

Total number of known cyber incidents: 226

The Number of Ongoing Dyadic Cyber Incidents by Year, 2000-2016

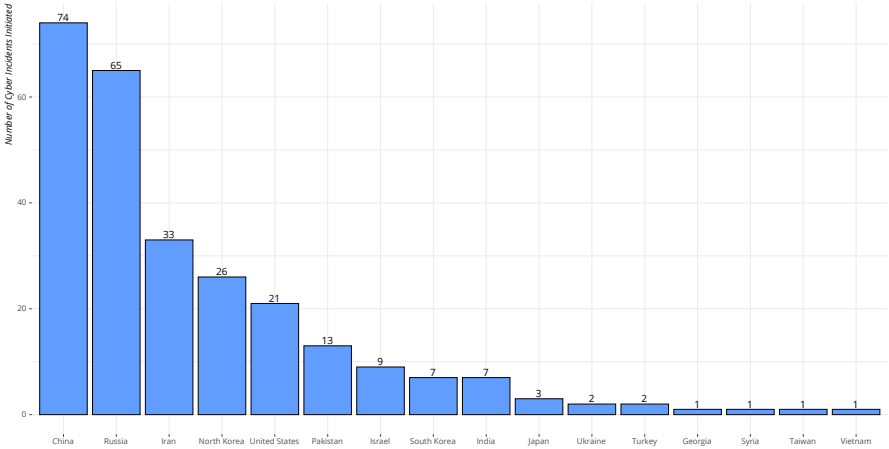
Cyber capabilities have become better developed over time. 2016 had more cyber incidents than 2000-2008 combined.



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

All States Initiating Cyber Incidents, 2000-2016

China and Russia stand out for investing significant energy into cyber attacks. Combined, both are more than 52% of all cyber incidents in the data set.



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

Table 1: The States Most Targeted by Cyber Attacks, 2000-2016

Targeted State	**Number of Cyber Incidents**
United States	82
South Korea	29
India	20
Ukraine	15
Iran	14
Japan	13
Russia	11
Israel	11
Saudi Arabia	7
China	7

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

Table 2: The Dyads with the Most Dyadic Cyber Incidents, 2000-2016

Dyad	Number of Cyber Incidents
US-China	48
US-Russia	26
N Korea-S Korea	22
India-Pakistan	20
US-Iran	20
Iran-Israel	18
Russia-Ukraine	17
China-Japan	8
China-Taiwan	8
S Korea-Japan	8

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

Target Types

Cyber incidents go after one of three groups in a state.

1. Private/non-state (e.g. the Sony hack in 2014 [incident 101])
2. Government/non-military (e.g. China's hack of Vietnam in 2011)
3. Government/military (e.g. Russia momentarily seized the JCS' [unclassified] email system in March 2015 [incident: 19])

The Sony Hack (#101)

The Sony Hack (#101)

On 24 Nov. 2014, a DPRK hacker group ("Guardians of Peace") leaked 100 TBs of Sony's data. Including:

- personal information about employees
- email communication between employees
- Copies of upcoming films/plans for future films

Why: Sony produced *The Interview*, a then forthcoming film about a plot to assassinate Kim Jong-un.

- The group demanded Sony withdraw the film, threatening terror attacks against cinemas that showed it.

What happened:

- Sony withdrew *The Interview* and cancelled all premieres.
- Sony lost about $35 million on IT repairs, and ate about $30 million on the film.

Table 3: Targets of Dyadic Cyber Incidents, 2000-2016

Target Type	**Number of Cyber Incidents**
Private/non-state	85
Government (Non-military)	132
Government (Military)	49

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

Cyber Objectives

Analogous to terrorism, different cyber incidents carry different cyber objectives.

1. Disruption
2. Short-term espionage
3. Long-term espionage
4. Degradation

The Lockheed F-35 Hack (#66)

Table 4: Objective Types of Dyadic Cyber Incidents, 2000-2016

Objective Type	**Number of Cyber Incidents**
Disruption	86
Short-term Espionage	80
Long-term Espionage	65
Degradation	35

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

Cyber Methods

1. Vandalism
2. DDoS attacks
3. Network intrusion
4. Network infiltration
    - 4.1 Logic bombs
    - 4.2 Viruses
    - 4.3 Worms
    - 4.4 Keystroke logging

Table 5: The Methods of Dyadic Cyber Incidents, 2000-2016

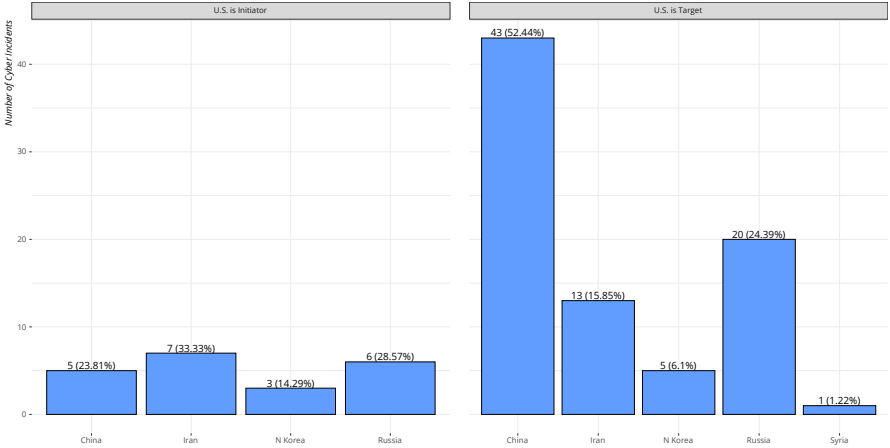
Method Type	**Number of Cyber Incidents**
Vandalism	28
DDoS Attacks	46
Network Intrusion	144
Network Infiltration (Logic Bombs)	7
Network Infiltration (Viruses)	24
Network Infiltration (Worms)	9
Network Infiltration (Keystroke Logging)	8

Note:

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

The Dyadic Nature of U.S. Cyber Incidents by Initiator and Target, 2000-2016

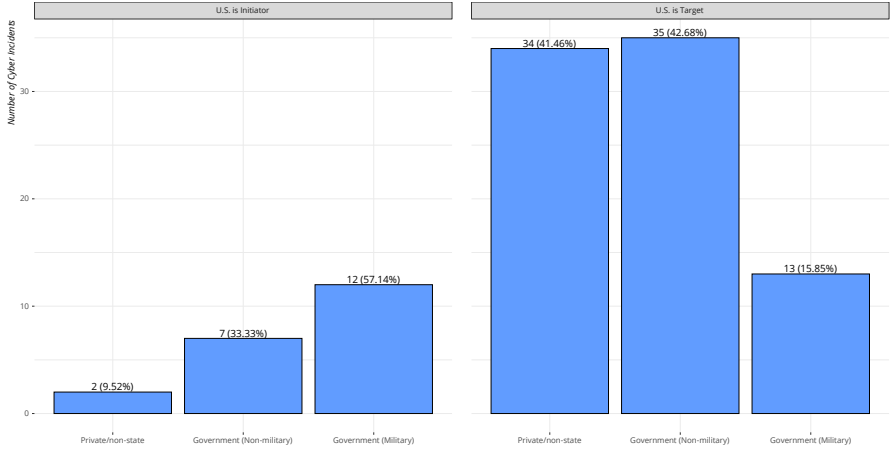
The U.S. is the target of 36% of incidents in the whole data set, most of which are initiated by China.



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

The Target Type of U.S. Cyber Incidents, whether U.S. is Initiator or Target (2000-2016)

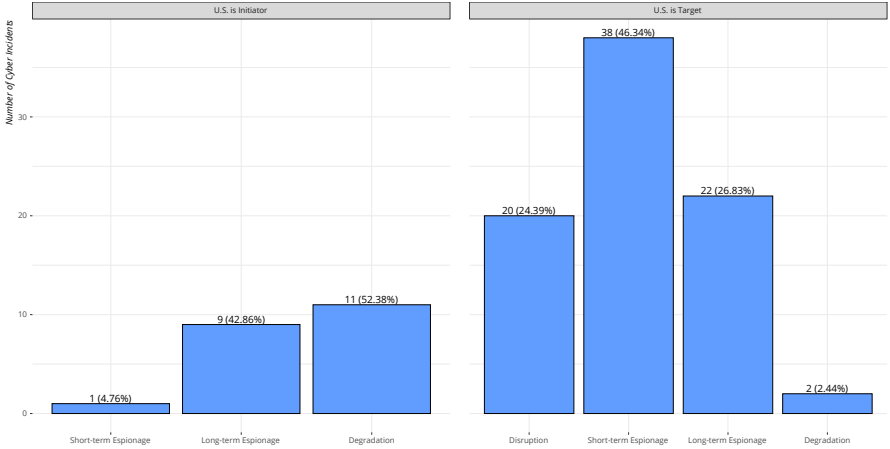
The U.S. cyber capabailities go after the military of the target. By contrast, U.S. rivals have typically attacked private or non-military actors in the United States.



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

The Objective Type of U.S. Cyber Incidents, whether U.S. is Initiator or Target (2000-2016)

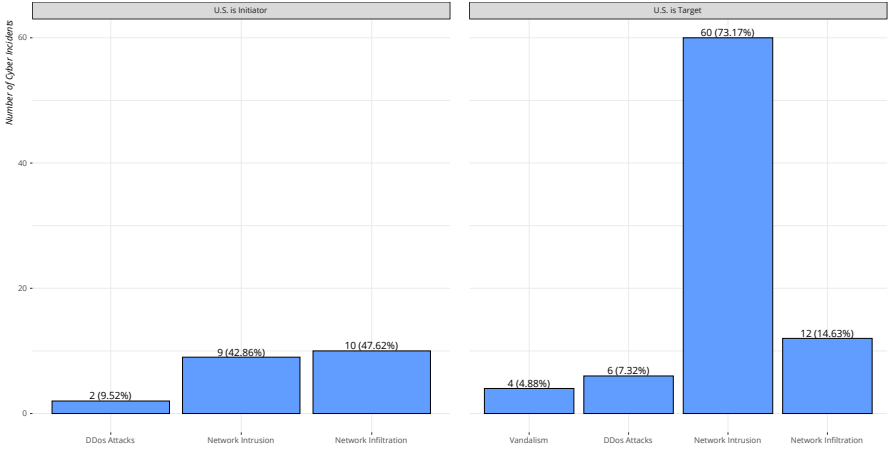
The U.S. cyber capabailities often focus on degrading the capacity of the target (e.g. Stuxnet). Almost 75% of the time, the U.S. itself is targeted in espionage campaigns.



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

The Method of U.S. Cyber Incidents, whether U.S. is Initiator or Target (2000-2016)

American cyber sophistication allows for greater focus on more complicated attacks. Other states, by contrast, focus on trojans and 'backdoors' to gain access to a target's network.



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

Conclusion

- Cyber incidents emerged as tools for weaker (but still sophisticated) states to signal dissatisfaction with rivals.
- Cyber aims are often limited, as are the cyber methods.

Table of Contents

Introduction

The Dyadic Cyber Incident and Campaign Dataset (DCID)

What Does 'Cyber Conflict' Look Like?

The U.S. and Cyber Conflict

Conclusion