POLS 429: International Terrorism

Lecture 31 (04.15.2020): Cyber Terrorism

Rotem Dvir

Texas A&M University

rdvir@tamu.edu

Department of Political Science
Spring 2020

Overview

Review

What we covered last meeting?

- How can we explain variations in CT choices of states?
- Strategic: domestic politics and non-optimal CT choices.
- Organizational: intergroup rivalry and SOP's .
- Psychological: risk perception (Obama – Bush).
- Ideological: symbolic power of terrorism, ethnocentrism, authoritarianism.
- Structural: state capacity, regime type.
- Critical: CT as performative act, intended to consolidate state power.

Questions??

What is Cyber Terrorism?

- The threat of cyber-terrorism, definition and scope.
- Definition aspects:
  1. Who is the target. ▸ Target
  2. The objective of wide-scale fear. ▸ GoalFear
  3. Specific elements of terror. ▸ Terror
  4. Examples. ▸ Attacks
- Globalization (structure): easier access to technologies, expanded the pool of supporters and recruits (Cronin 2003).
- *Critical Info Infrastructures (CII)* with high connectivity to the internet.
- Example: cyber-attack on a power grid of a major city.

Cyber-Terrorism: Why?

The appeal of cyber-terrorism (Weimann 2005):

1. Low cost.
2. Potential for anonymity.
3. Wide target list.
4. Ability to execute attacks remotely.
5. Potential for many casualties.

- Also:
  1. Larger extent of damages and/or casualties with no use of explosives or firearms.
  2. 'Easier' to plan and execute simultaneous global attacks.

Cyber-Terrorism: Why?

Theoretical mechanisms: Substitution.

- Substitute less effective tactics (due to CT actions).
- Replace methods countered by defensive measures such as border security or police watch lists.

Theoretical mechanisms: Diversification.

- Expand 'portfolio' to reduce predictability, and force states to extend their defensive capabilities.
- Overcome disadvantages in resources and personnel.
- Usually implemented pre-emptively.
- Evidence for political success (Cronin 2009).

Cyber-Terrorism: Why (Not)?

1. Expertise to execute (complex) operations - terror groups still lack these skills.
2. The effects of cyber-attacks are less grandiose (images of fear and multiple casualties).
3. Effects are rarely immediate, in contrast to explosives.

Cyber Terrorism/attacks

The empirical record by 2020

- As of today $\rightarrow$ no clear cases of cyber-attacks perpetrated by terror groups.
- The vast majority of cyber-attacks are conducted by state actors:
  - Israel/American operation against Iran's nuclear program (Stuxnet).
  - Russia complemented its offensive operations in Estonia and Georgia with cyber-attacks of infrastructure.
  - Most other cases involve stealing information (Uber 2016, White House OPM 2015, DNC 2016).
- StuxnetVirus

Cyber Terrorism/attacks

- Terrorism in cyberspace $\rightarrow$ indirect, complementary to conventional attacks and did not generate direct loss of life.
- 2015: ISIS cell led by Junaid Hussain spread online propaganda and helped recruit the man who opened fire on citizens in Garland, Texas.
- 2017: Palestinian terror operator hacked into the video feed of IDF drones flying missions over Gaza.
- Also hacked into systems that monitors civilian air traffic in Israel's main airport and transportation authority cameras.

Cyber Terrorism/attacks

Alternative methods of using computer technology:

- **(1) Cyber crimes**.
- Finance terror operations and accumulate resources.
- **(2) Information warfare**.
- Recruitment, spreading propaganda.
- Spread misinformation against target population.

Attribution & Credit Claiming

Poznansky and Perkoski (2018)

- Secrecy and anonymity in cyberspace.
- The benefits of secrecy in cyberspace for deterrence and the dynamics of conflict and escalation.
- Not all actors remain anonymous: *SOBH Cyber Jihad, Iran*.
- The logic of credit claiming depends on the objective of the perpetrator of the cyber-attack.
- Nonstate actors (including terror groups): credit claiming for signaling credibility, influencing public opinion and expanding recruitment.
- Relative weakness and lower capacity in cyberspace - credit claiming helps prove their capability.

Attribution & Credit Claiming

Poznansky and Perkoski (2018)

- The question of **attribution**.
- Forensics are complex and may take months.
- Terror groups $\rightarrow$ disadvantage from a structural perspective.
- Credit claiming in cyber-attacks is very appealing proposition.
- A strategic perspective: credibility and signaling resolve by 'announcing' the attacks.

Attribution & Credit Claiming

Poznansky and Perkoski (2018)

- Early cyber-attacks $\rightarrow$ inconvenience rather than actual damage.
- After establishing a 'track record' $\rightarrow$ large scale attacks targeting critical infrastructure.
- Successful cyber operations:
  1. Signal resolve and credibility.
  2. Enlarge the pool of recruits.
- Global reach of technology, credit claiming enhance publicity and attract recruits and supporters.

Attribution & Credit Claiming

Poznansky and Perkoski (2018)

- Credit claiming is less logical and anonymity is better: cyber-crimes (stealing funds).
- Why remain anonymous:
  1. Not revealing their identity may allow similar operations in the future, securing more steady source of funding.
  2. Prevent target from suspecting that a (kinetic) attack is looming.

Public View of Cyber-Terrorism

- How does cyber terrorism affects public perceptions?
- Research is very limited; most scholars focus on perpetrators' motivation to employ these measures.
- Recent studies employ experimental designs in the larger context of cyber attacks.

Kostyuk and Wayne (2020)

- How the public reacts to cyber-threats? Are there differences in terms of threat perceptions when the threats have personal effects?
- Risk perception and public understanding of cyber threats.

Public View of Cyber-Terrorism

Kostyuk and Wayne (2020)

- The basic argument: public understanding is very low.
- Why?
  1. Low exposure $\rightarrow$ most attacks target governments or large corporations (data breaches and information theft).
  2. Less debate on cyber threats (compared to other national security threats).
- Threat is not personal, and does not require too much of an investment in protection.
- The psychological aspect: cyber operations do not elicit the same emotional response as conventional terrorism.

Public View of Cyber-Terrorism

Kostyuk and Wayne (2020)

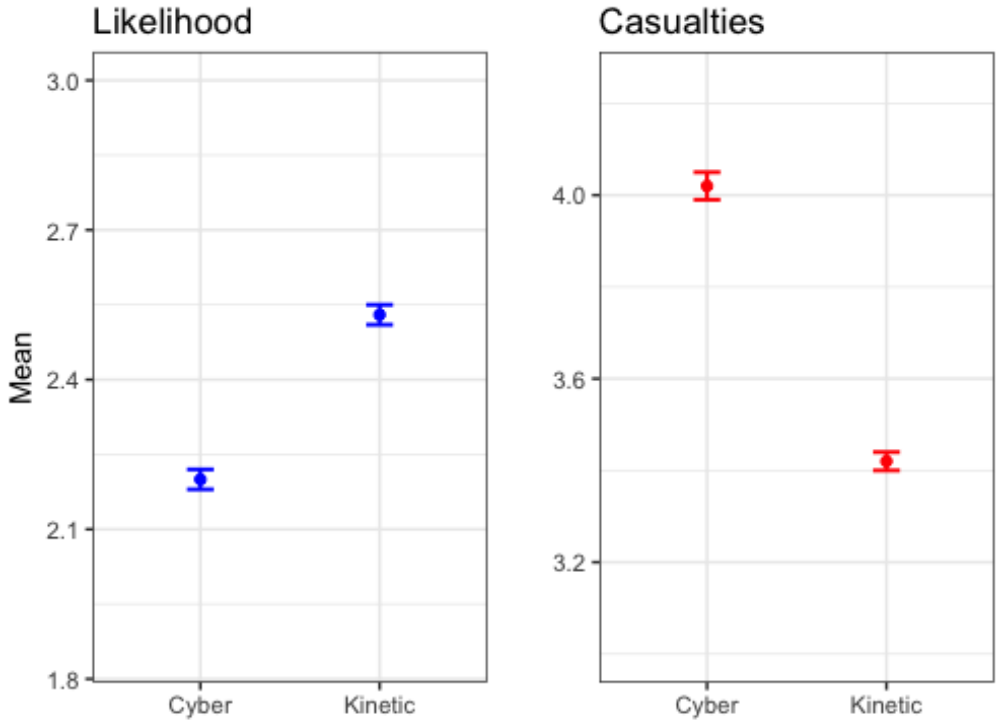
- A cyber-attack with personal ramifications should heighten risk perceptions.
- Increase support for government' investment in prevention and increase propensity to engage in safer cyber behavior.
- Findings from experiments:
  1. Limited public knowledge of cyber terminology and events.
  2. A personal cyber attack triggers higher degree of threat about future attack, more than a national threat. ▸ ThreatCyber
  3. Policy support is higher for those exposed to threats, regardless of its type (personal or national).
  4. Exposure to personal threat increase individuals' propensity to engage in safer cyber behavior (although no *actual* behavior).

Public View of Cyber-Terrorism

Conventional vs. Cyber Terrorism

- Does the public comprehend the threat of cyber-terror and distinguish cyber from conventional threats?
- Motivation → public polls data (2016-2018). ▸ Gallup
- Public cyber threat perception: media discussions and low actual exposure.
- Main 'gaps': in perception, when we explore questions of likelihood and expected costs.

Conventional vs. Cyber Terrorism



- Likelihood for cyber is lower, costs is higher.
- Costs: media, elite emphasize "potential" damages.
- Threat perceptions are dominated by likelihood: behavior does not change.

Recommended readings

More studies on Cyber-Terrorism:

1. Kenney, Michael. "Cyber-terrorism in a post-stuxnet world." *Orbis*, Vol. 59, no. 1 (2015): 111-128.
2. Weimann, Gabriel. "Cyberterrorism: The sum of all fears?." *Studies in Conflict & Terrorism*, Vol. 28, no. 2 (2005): 129-149.
3. Gross, Michael L., Daphna Canetti, and Dana R. Vashdi. "Cyberterrorism: its effects on psychological well-being, public confidence and political attitudes." *Journal of Cybersecurity*, Vol. 3, no. 1 (2017): 49-58.

Defining Cyber Terrorism

Aspects of definition: Target

"**unlawful attacks and threats of attack against computers, networks, and the information stored therein** when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss...attacks against critical infrastructures...depending on their impact

Defining Cyber Terrorism

Aspects of definition: Objective - Fear

"unlawful attacks and threats of attack against computers, networks, and the information stored therein when **done to intimidate or coerce a government or its people in furtherance of political or social objectives**. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss...attacks against critical infrastructures...depending on their impact.

Defining Cyber Terrorism

Aspects of definition: Fit cyber category

"unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. **Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear**. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss...attacks against critical infrastructures...depending on their impact.

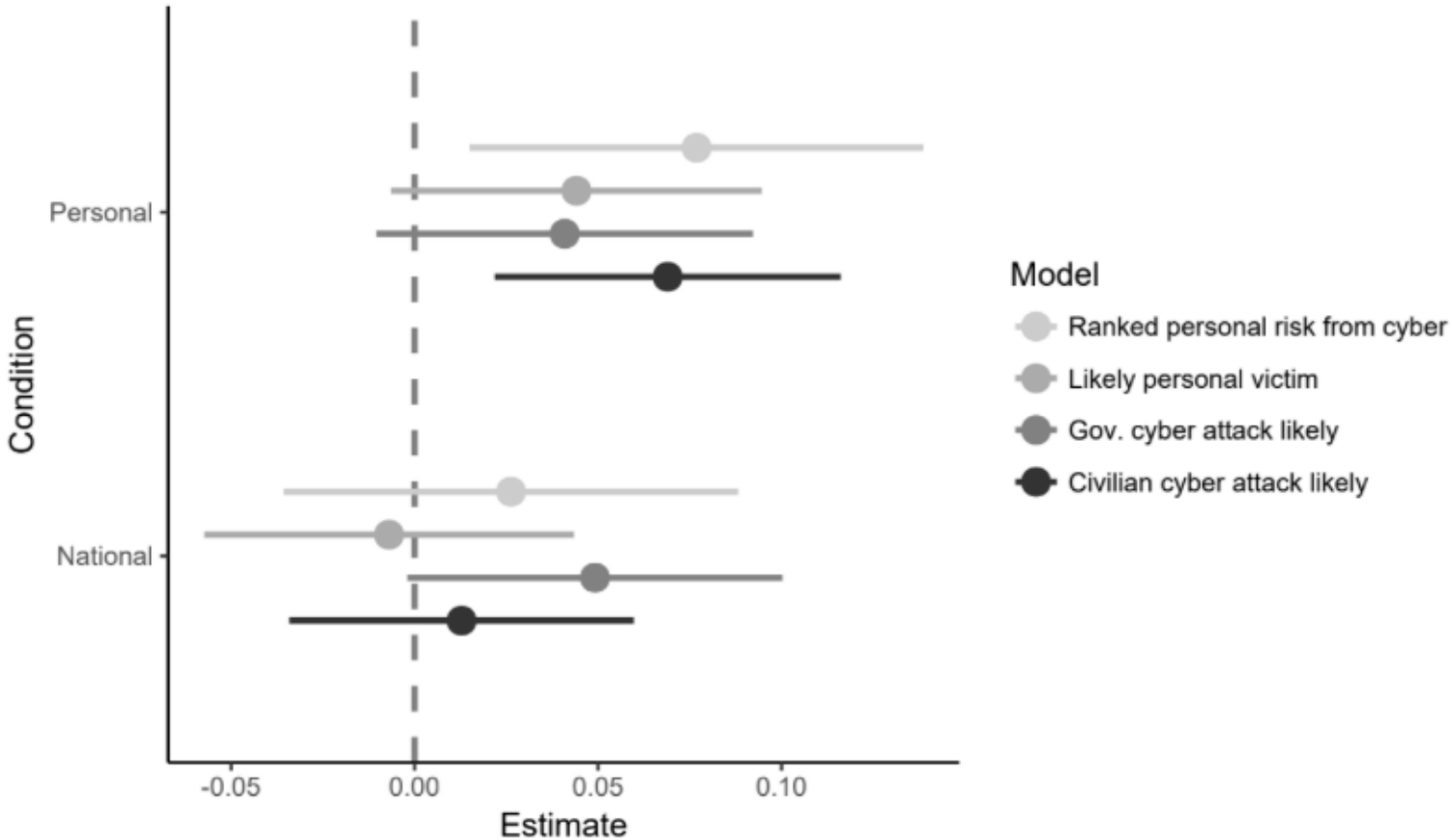
Defining Cyber Terrorism

Aspects of definition: Examples

"unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. **Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss...attacks against critical infrastructures...depending on their impact**.

Cyber Attacks: Threat Perception

Figure 2: Changes in Perceived Cybesecurity Risk



Public Opinion - Gallup 2016

	% Critical threat	% Important but not critical threat
International terrorism	79	18
Development of nuclear weapons by Iran	75	18
Cyberterrorism, the use of computers to cause disruption or fear in society	73	22
The spread of infectious diseases throughout the world	63	33
The conflict in Syria	58	32
The military power of North Korea	58	29