POLS 318: Theories of IR

Lecture 26 (11.17.2020): Modern Technology & International Relations

Rotem Dvir

Texas A&M University

rdvir@tamu.edu

Department of Political Science

Fall 2020

Overview

1. Quick review
2. Tech and IR
3. Military Tech: Drones
4. Advanced Weapons Tech
5. Military Tech: Cyber
6. Extra Material

Review

WHAT WE COVERED LAST MEETING?

- Terrorism and elections.
- How terrorism affects voting - Israel, Spain.
- Psychological effects of terrorism.
- Threats, national security and civil liberties.
- CT tools - hard power.
- Indiscriminate and discriminate approach.
- CT tools - soft power.
- Politics of counter-terrorism policies.

Questions?? Email me!

Military technology

OR?

Introduction

Military Technology

- The importance of military power in IR.
- Realism/Neorealism, Deterrence, Coercion.

- How do we use military tools?
- Strategies, deployments, organizational routines.
- Focus on acquisition - why obtain weapons?
- Institutions, leaders, strategic setting.

- Modern technology research → explain behavior.

Study military technology

Limits in Research

- Access to evidence: exposure of technology.
- Uncertainty of the effects on war conduct.

"Solutions"

1. Direct: measure attitudes on using technology.
2. Integrate tools to existing research: drones in war.
3. Apply IR theory to tech: how AI shape BOP?
4. Formal theory: derive expectations and test with limited cases.

Military technology

A path towards escalation?

- Risks of advanced technology. ▸ Officials
- A complementary factor?
- Advanced tools support political and strategic decisions to escalate a conflict.
- How new technology shape war conduct?
  1. Strong causal effect: emphasize 'first-movers' advantage.
  2. Weak intervening role: enable deliberate escalation by states.

Military technology

Escalation types (Talmadge 2019)

- *Vertical*: shift in level of violence.
- Target civilians & military targets.
- Crossing of a threshold: casualties, duration and issue salience.

- *Inadvertent*: wrong estimates, security dilemma.
- Enhance 'first-movers' advantage.

- *Intended*: leverage tech to implement military strategies.
- Amplify the escalation decision.

Military technology and escalation

Aerial bombing in Vietnam (1965-1972)

Military technology and escalation

Aerial bombing in Vietnam (1965-1968)

- Gradual escalation in strategy.
- Targets: industrial → military → infrastructure.
- Technology: a non-factor.
- Failure to destroy targets despite multiple sorties.
- Precision problems.

Military technology and escalation

Aerial bombing in Vietnam (1972)

- Technology advancement: laser guided bombs.
- Enable a 'horizontal' escalation: new type of targets.

Christmas Bombing (December 1972)

Military Drones

Background

- Remote piloted with launch and landing capabilities.
- Repeated use (multiple operations).
- Prevalent tool of counter-terrorism policy.
- The effectiveness puzzle...

Pros of drones

- Efficient → accurate targeting
- Cost-effective: protect soldiers, and civilians.
- Long duration missions.

Military Drones

Cons of drones

- Blowback → inaccurate intelligence.
- Success → good *human* intelligence.
- Cannot prevent terror groups propaganda, recruitment, etc.
- Blowback → criticism by target public.
- Increased radicalization and support for insurgents.
- Damage credibility of host (target state).
- Violation of international laws.

Military Drones

Public views

- Data: US samples.
- Strong public support → cost-effective.
- No need to use 'boots on the ground'.

- Experiments to collect data.
- Terrorism, anger and drones as CT tools.
- International laws violation → lower support.

Military Drones

Proliferation

- Armed drones $\gg$ tactical.
- Regimes and objective of acquiring drones.

Military Drones

Coercion

- How drones affect deterrence or compellence?
- Tech developments → drones as credible weapons.
- Cost-effective and increased precision.
- Enhance coercive power for those who possess the weapon system.

- Escalation dynamics: shooting-down a drone?
- Less likely → no loss of life.

More advanced tools

Artificial Intelligence (AI)

- *(1) Narrow AI*: algorithms execute a specific task.
- *(2) AGI*: machines that self-innovate and learn.
- Growing interest among powerful states.

Advanced technology

Advanced Weapons System

- Advanced weapons → questions about barriers to war, civilian casualties and international laws.
- **AWS**: operate with no human intervention.

Advanced technology

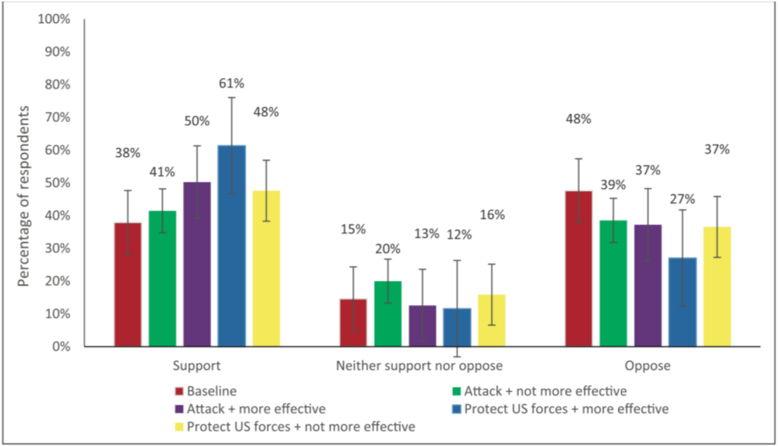
AWS and public opinion (Horowitz 2016)

- No human - a problem?
- Normative and legal concerns.
- Contextual factors matter:
  1. Casualty aversion.
  2. Military utility.
  3. Adversary use.

Does public opinion matter?

- Formulation of international law.
- Public averse → immoral weapons systems.
- NGO pressure industry and affects development.

Advanced technology and public opinion



Cyber Technology

Introduction

- 'Weaponizing' computer tech and networks.
- Not conventional instruments of war.
- Attacks may seem as criminal acts: a digital bank robbery.
- Powerful intelligence tool: stealing information.
- Target private companies (records, private information of employees).
- Target national government - spread propaganda.
- 'Conventional' usage → target military networks, air defense systems.

Cyber Technology

A weapon of war - the threat from cyber tech

- A game changing technology?
- Evidence: Russia (Estonia and Georgia)
- Define cyber conflict: narrow or broad.

- Expand the conflict beyond the battlefield.
- Second-order effects.
  - Damage national computer network.
  - Economic costs from hacking.

- The attribution problem.

Cyber Technology

A threat? When?

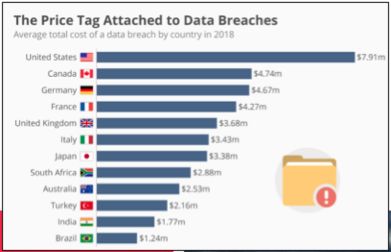
- Overall - limited effect on warfare and escalation (2001-2014).

- When can cyber tools make an impact?
- 2016 US presidential elections: shake confidence in democratic system.
- Method of espionage and intelligence.
- Attack economic and soft targets.

- 'Easy' attacks? not so fast...
- Skills and expertise.
- Operational capacity and resources.

Cyber Technology

Public views of cyber threats



Cyber Technology

The 'User Error' problem

- Computer users drive success and costs of cyber attacks.
- Prevention → safer online practices by users.
- Human failure → weakness exploited by perpetrators.

- Why can't we act safer online? **Low knowledge**
- But why?
- Most attacks → data breach of private sector and government.
- No personal damage.
- No 'Cyber pearl harbor'.

Cyber Technology

Public views of cyber threats (Kostyuk and Wayne 2020)

- Test public views of cyber threats.
- Personal threat → Do citizens engage in safer online behavior?
- Support extended government action?

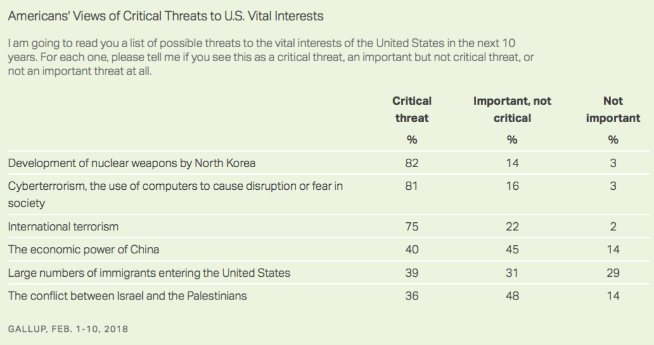
Findings

1. Low levels of knowledge.
2. Concern about personal security. ▸ Personal
3. Personal threat: express willingness to act safer (no evidence).
4. Support for defensive/preventing policies. ▸ ResponsePolicies

Cyber Technology

Cyber attacks by Terrorists?

- The problem? No evidence for attacks.
- Low levels of cyber knowledge.
- However...



Americans' Views of Critical Threats to U.S. Vital Interests

I am going to read you a list of possible threats to the vital interests of the United States in the next 10 years. For each one, please tell me if you see this as a critical threat, an important but not critical threat, or not an important threat at all.

	Critical threat	**Important, not critical**	**Not important**
	%	**%**	**%**
Development of nuclear weapons by North Korea	82	14	3
Cyberterrorism, the use of computers to cause disruption or fear in society	81	16	3
International terrorism	75	22	2
The economic power of China	40	45	14
Large numbers of immigrants entering the United States	39	31	29
The conflict between Israel and the Palestinians	36	48	14

GALLUP, FEB. 1-10, 2018

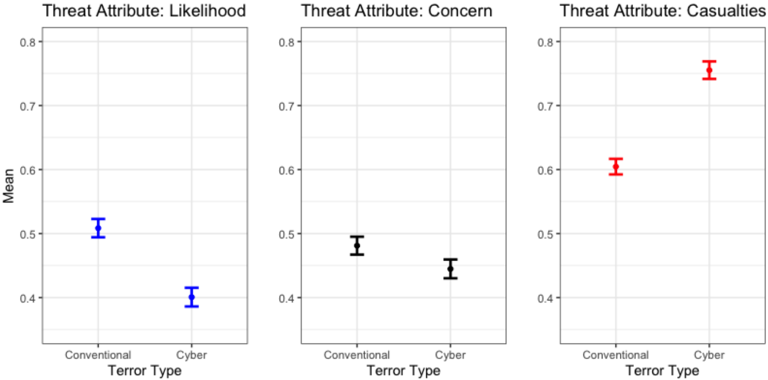
Cyber Terrorism

Public opinion of complex issues

- Public surveys questions - general.
- "How concern are you of threat...?"
- "What is the most important threat?"
- Unpack perceptions:
  - Likelihood: cyber low, conventional high.
  - Costs: cyber high, conventional low.
- Why gaps? exposure to threat and technical knowledge.

Cyber Terrorism

Public opinion of complex issues



Recommended readings

More studies on modern technology and IR:

1. Schneider, Jacquelyn. (2019) "The capability/vulnerability paradox and military revolutions: Implications for computing, cyber, and the onset of war." *Journal of Strategic Studies 42*, 6, 841-863.
2. Horowitz, Michael C. (2018). "Artificial intelligence, international competition, and the balance of power." *Texas national security review*.
3. Volpe, Tristan A. (2019). "Dual-use distinguishability: How 3D-printing shapes the security dilemma for nuclear programs." *Journal of Strategic Studies 42*, 6, 814-840.

Escalation risks

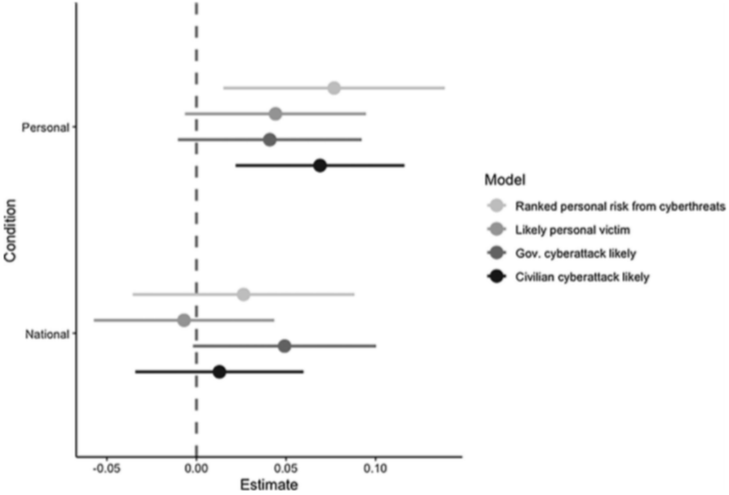
Center for a new American security:

New technologies, particularly cyber and robotics, are changing the way deterrence and escalation operate between the United States and other actors in potentially dangerous ways.

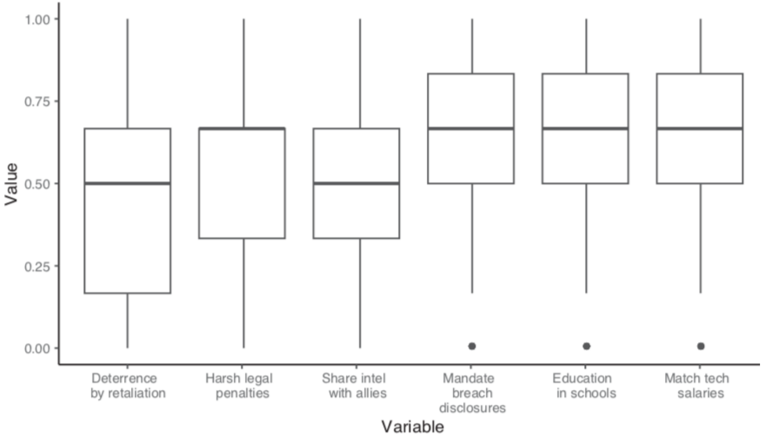
US Defense undersecretary:

Emerging new military capabilities – cyber, space, missile defense, long-range strike, and ... autonomous systems – are increasing uncertainties associated with strategic stability and creating potential slippery slopes of escalation.

Personal Concern from Cyber-attack



Government response to cyber-attack


Value
Deterrence by retaliation
Harsh legal penalties
Share intel with allies
Mandate breach disclosures
Education in schools
Match tech salaries
Variable