

---

# Emerging Technology + International Security

17.449

Erik Lin-Greenberg

Associate Professor of Political Science

Massachusetts Institute of Technology

---

# Cyber...war?

---

LILY HAY NEWMAN

SECURITY 04.23.2018 08:55 PM

# Atlanta Spent \$2.6M to Recover From a \$52,000 Ransomware Scare

Newman, Lily Hay. "Atlanta Spent \$2.6M to Recover From a \$52,000 Ransomware Scare." *WIRED*, April 23, 2018. © Condé Nast Publications. All rights reserved. This content is excluded from our Creative Commons license. For more information, see <https://ocw.mit.edu/help/faq-fair-use/>.



© Sony Pictures Releasing. All rights reserved. This content is excluded from our Creative Commons license. For more information, see <https://ocw.mit.edu/help/faq-fair-use/>.

The New York Times

## ***‘Dangerous Stuff’: Hackers Tried to Poison Water Supply of Florida Town***

For years, cybersecurity experts have warned of attacks on small municipal systems. In Oldsmar, Fla., the levels of lye were changed and could have sickened residents.



Robles, Frances, and Nicole Perlroth. "Dangerous Stuff: Hackers Tired to Poison Water Supply of Florida Town," *New York Times*, February 8, 2021. © The New York Times Company. All rights reserved. This content is excluded from our Creative Commons license. For more information, see <https://ocw.mit.edu/help/faq-fair-use/>.

# When the screens went black: How NotPetya taught Maersk to rely on resilience – not luck – to mitigate future cyber-attacks

Adam Bannister 09 December 2019 at 12:09 UTC  
Updated: 09 December 2019 at 13:06 UTC

Ransomware Cyber-attacks Maritime



*Serendipity intervened to rescue world's largest shipping conglomerate in 2017*



Courtesy of Official Internet Resources of the President of Russia. Used with permission. License CC BY.



Image courtesy of [the Government of Ukraine](#).  
Source: Wikimedia Commons. This image is in the public domain.



Massachusetts Institute of Technology

Bannister, Adam. "When the screens went black: How NotPetya taught Maersk to rely on resilience—not luck—to mitigate future cyber-attacks." *PortSwigger*, December 9, 2019. © PortSwigger Ltd. All rights reserved. This content is excluded from our Creative Commons license. For more information, see <https://ocw.mit.edu/help/faq-fair-use/>.





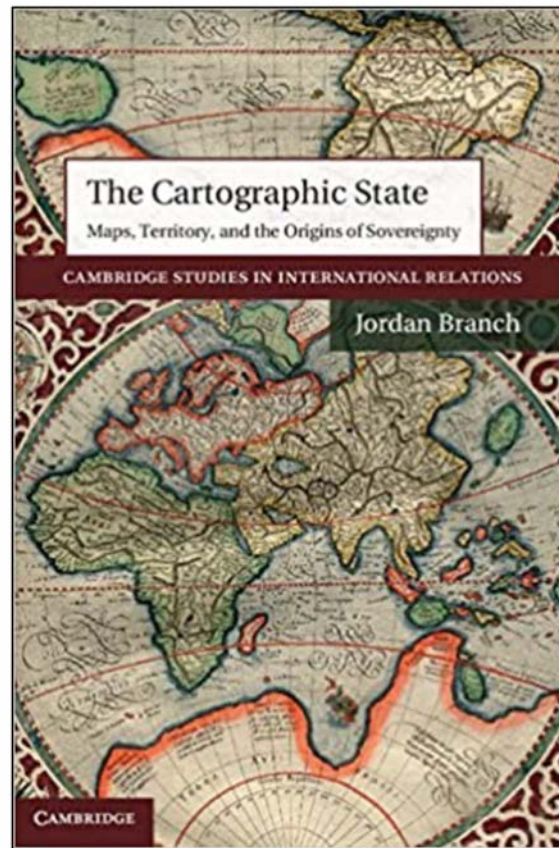
Image courtesy of [USAMHI](#). Source: Wikimedia Commons. This image is in the public domain.



---

# How did we get here?





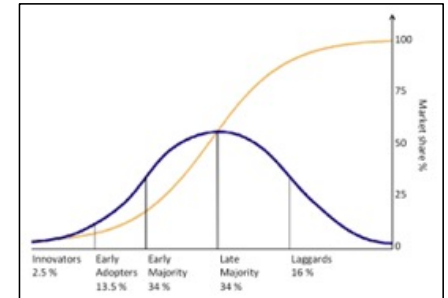
Branch, Jordan. *The Cartographic State: Maps, Territory, and the Origins of Sovereignty*. Cambridge University Press, 2014. © Cambridge University Press. All rights reserved. This content is excluded from our Creative Commons license. For more information, see <https://ocw.mit.edu/help/faq-fair-use/>.

# Views on technology



Image courtesy of [Cover Images/The Ministry of Medium Machine Building of the USSR/Associated Press](#).  
Source: Wikimedia Commons. This image is in the public domain.

Gray, Colin S. *Weapons Don't Make War: Policy, Strategy, & Military Technology*. University of Kansas Press, 1993. © University of Kansas Press. All rights reserved. This content is excluded from our Creative Commons license. For more information, see <https://ocw.mit.edu/help/faq-fair-use/>.



## Techno-determinism

### Strict

Independent causal effect  
Autonomous agent

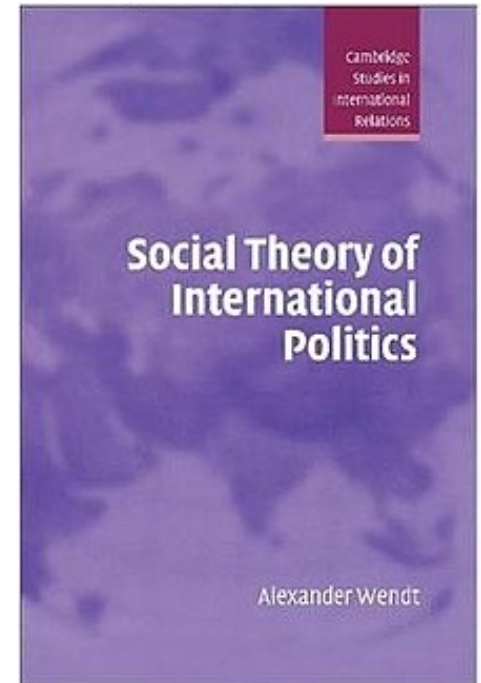
## Socially constructed

### Strict

Social processes shape  
innovation and use

# Paradigms: Constructivism

- Focuses on shared norms and ideals
- Everything is “socially constructed”
- “Anarchy is what you make of it”
- Critique: Who shapes definitions/norms?
- Technology is socially constructed



Wendt, Alexander. *Social Theory of International Politics*. Cambridge University Press, 1999. © Cambridge University Press. All rights reserved. This content is excluded from our Creative Commons license. For more information, see <https://ocw.mit.edu/help/faq-fair-use/>.

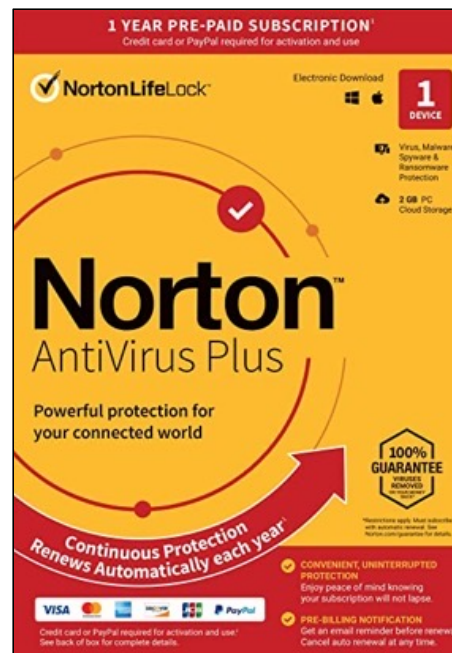
# What's in a Name?

- Examines how metaphors shape practice/behavior
  - What are metaphors? (Foundational Metaphors)
  - How did metaphors become part of “cyber” in U.S?
  - What are the “rhetorical effects” of terminology?
- Metaphor: “understanding/experiencing one kind of thing in terms of another”
  - Reshape thinking, decision-making, and outcomes
  - Create implicit mental models (heuristics!)
  - Often used for hard-to-define concepts

# What's in a Name?



Image courtesy of [mxmstryo](#) on Flickr. License CC BY.



© Gen Digital Inc. All rights reserved. This content is excluded from our Creative Commons license. For more information, see <https://ocw.mit.edu/help/faq-fair-use/>.



© manop / Shutterstock.com. All rights reserved. This content is excluded from our Creative Commons license. For more information, see <https://ocw.mit.edu/help/faq-fair-use/>.

# What's in a Name?



Image courtesy of [the U.S. Navy, Office of Public Relations](#). Source: Wikimedia Commons. This image is in the public domain.



# What's in a Name?

- Cyberspace
  - Arises in early 1980s (William Gibson)
  - What does this term connote?
  - Connection to realist logics of power/influence?

```
override func viewDidLoad() {
    super.viewDidLoad()

    // Latitude and longitude for Golden Gate Bridge
    var latitudeGGB:CLLocationDegrees = 37.817785
    var longitudeGGB:CLLocationDegrees = -122.478590

    // Latitude and longitude degree difference for
    var latDelta:CLLocationDegrees = 0.25
    var lngDelta:CLLocationDegrees = 0.25

    // Set the zoom level for the map based on the previously defined zoom level coordin
    var span:MKCoordinateSpan = MKCoordinateSpan(latitudeDelta: latDelta, longitudeDelta

    // Set the previously defined coordinates as the location
    var location:CLLocationCoordinate2D = CLLocationCoordinate2DMake(latitudeGGB, longit

    // Set the region view to be displayed with the center as 'location', and zoom level
    var region:MKCoordinateRegion = MKCoordinateRegionMake(location, span)

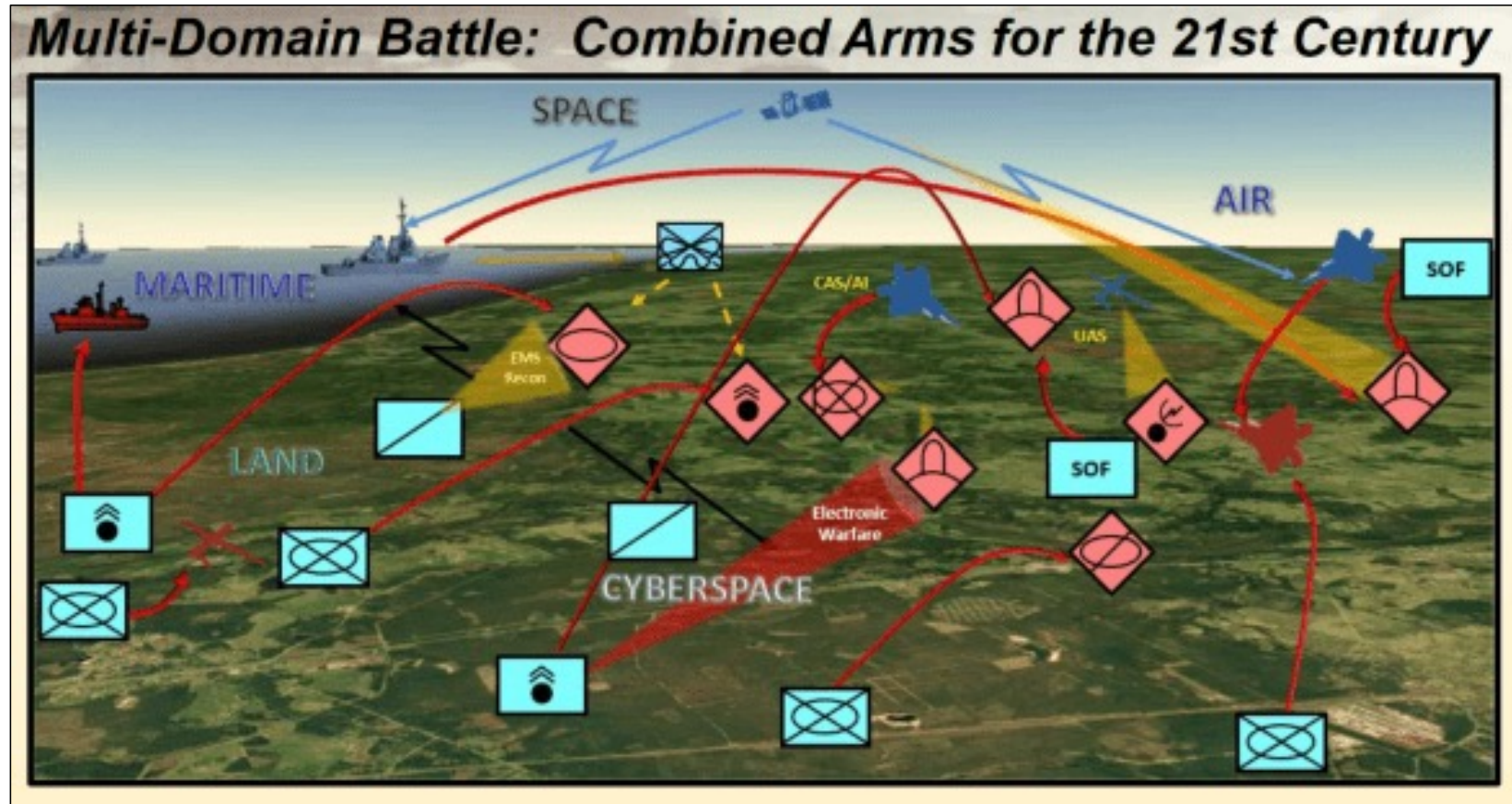
    // Display the region on the particular map object, 'mapView'
    mapView.setRegion(region, animated: true)
```

Meguira, Yonathan. "How many lines of code have you written?" Medium. July 16, 2017.  
© Yonathan Meguira. All rights reserved. This content is excluded from our Creative Commons license. For more information, see <https://ocw.mit.edu/help/faq-fair-use/>.



© National Geographic Maps. All rights reserved. This content is excluded from our Creative Commons license. For more information, see <https://ocw.mit.edu/help/faq-fair-use/>.

# What's in a Name?



Massachusetts Institute of Technology

Woodford, Shawn. "Army And Marine Corps Join Forces To Define Multi-Domain Battle Concept." The Dupuy Institute. February 3, 2017. © The Dupuy Institute. All rights reserved. This content is excluded from our Creative Commons license. For more information, see <https://ocw.mit.edu/help/faq-fair-use/>.

# What's in a Name?

- Cyberspace as a "domain"
  - Incorporated into military doctrine → consolidation over time
  - Export "terrestrial" terms into cyber realm → fit with military ideas
    - "Cyber fires"; "Cyber targets"; "cyber weapons"



Image courtesy of [Richard Watt/MOD](#). Source: Wikimedia Commons. This file is licensed under the Open Government Licence version 1.0.



Image courtesy of [George Johnson, Aviation Section, U.S. Army Signal Corps](#). Source: Wikimedia Commons. This image is in the public domain.



Image courtesy of [Mass Communication Specialist 3rd Class Scott A. Raegen of the U.S. Navy](#). Source: Wikimedia Commons. This image is in the public domain.

# What's in a Name?

- Cyberspace as a "domain"
  - Incorporated into military doctrine → consolidation over time
  - Export "terrestrial" terms into cyber realm → fit with military ideas
    - "Cyber fires"; "Cyber targets"; "cyber weapons"

```
override func viewDidLoad() {
    super.viewDidLoad()

    // Latitude and longitude for Golden Gate Bridge
    var latitudeGGB:CLLocationDegrees = 37.817785
    var longitudeGGB:CLLocationDegrees = -122.478590

    // Latitude and longitude degree difference for
    var latDelta:CLLocationDegrees = 0.25
    var lngDelta:CLLocationDegrees = 0.25

    // Set the zoom level for the map based on the previously defined zoom level coordin
    var span:MKCoordinateSpan = MKCoordinateSpan(latitudeDelta: latDelta, longitudeDelta

    // Set the previously defined coordinates as the location
    var location:CLLocationCoordinate2D = CLLocationCoordinate2DMake(latitudeGGB, longit

    // Set the region view to be displayed with the center as 'location', and zoom level
    var region:MKCoordinateRegion = MKCoordinateRegionMake(location, span)

    // Display the region on the particular map object, 'mapView'
    mapView.setRegion(region, animated: true)
```

Meguira, Yonathan. "How many lines of code have you written?" Medium. July 16, 2017. © Yonathan Meguira . All rights reserved. This content is excluded from our Creative Commons license. For more information, see <https://ocw.mit.edu/help/faq-fair-use/>.



# What's in a Name?

- Metaphors have a real world effect
  - Is there a problem with cyber "militarization"?
- Militarization of cyberspace
  - Concepts of operations/"**defend forward**" (2019)
- Bureaucratic battles/organizational change
  - RMA logic at play?
  - Within and across services



# What's in a Name?

- Air Force attempts to become lead service in cyber domain
  - Parallels with space, key to command and control, long range strike

2008 (Not activated)



2009- 2018



2018 -2019



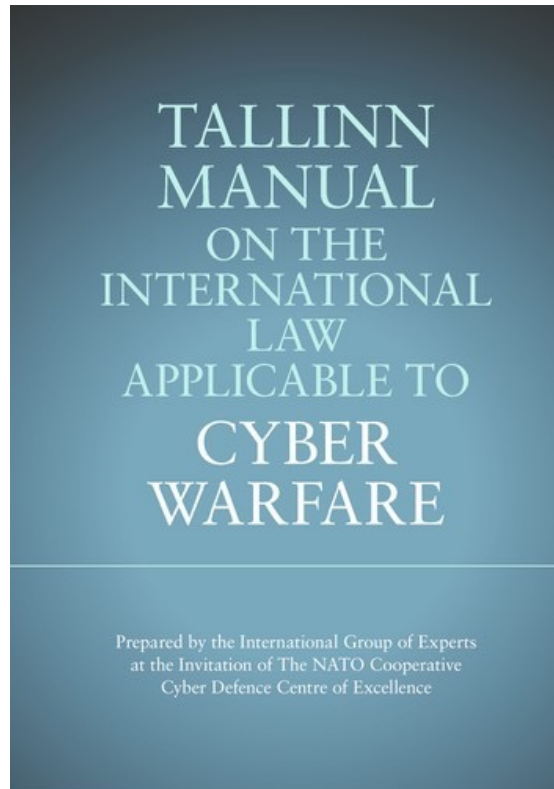
2019 -Present



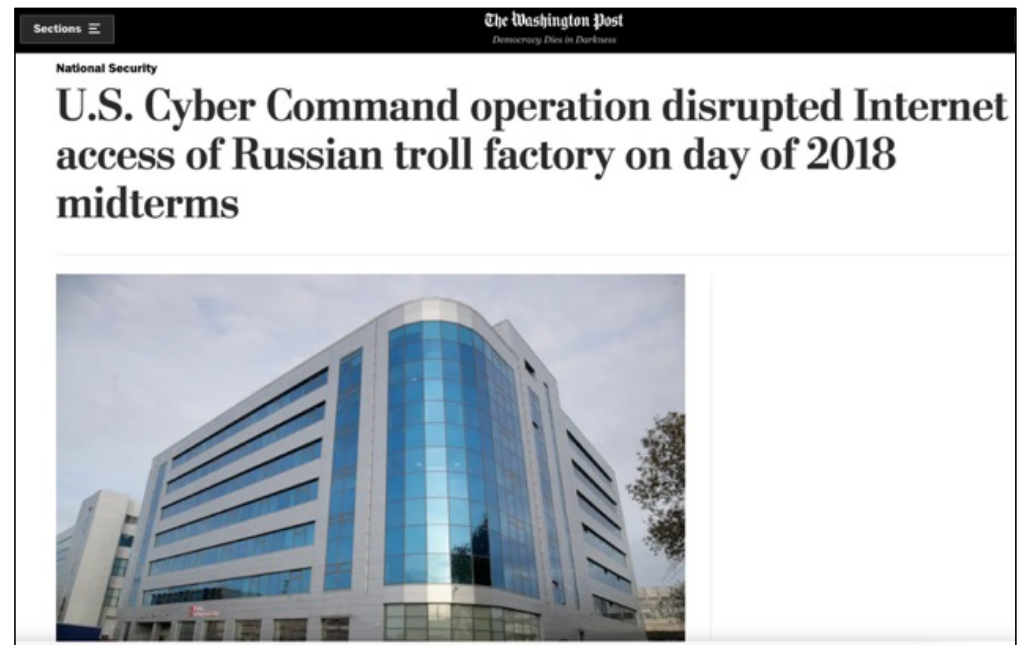
Credit for these images are on page 54.



# What's in a Name?



Schmitt, Michael N., ed. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge University Press, 2013. © Cambridge University Press. All rights reserved. This content is excluded from our Creative Commons license. For more information, see <https://ocw.mit.edu/help/faq-fair-use/>.



Nakashima, Ellen. "U.S. Cyber Command operation disrupted Internet access of Russian troll factory on day of 2018 midterms," *Washington Post*, February 26, 2019. © Nash Holdings. All rights reserved. This content is excluded from our Creative Commons license. For more information, see <https://ocw.mit.edu/help/faq-fair-use/>.

# What's in a Name?

- Branch makes strong claims, but we run into the **fundamental problem of causal inference**
- Counterfactual analysis
  - What if it wasn't viewed as a "cyberspace domain"
  - What if it were an "eco-system" instead?

```
override fun viewDisland() {
    super.viewDisland()

    // Latitude and longitude for Golden Gate Bridge
    var latitudeGGB:CLLocationDegrees = 37.817782
    var longitudeGGB:CLLocationDegrees = -122.478598

    // Latitude and longitude degree difference for
    var latDelta:CLLocationDegrees = 8.25
    var lngDelta:CLLocationDegrees = 8.25

    // Set the zoom level for the map based on the previously defined zoom level coordis
    var span:MKCoordinateSpan = MKCoordinateSpan(latitudeDelta: latDelta, longitudeDelta: lngDelta)

    // Set the previously defined coordinates as the location
    var location:CLLocationCoordinate2D = CLLocationCoordinate2DMake(latitudeGGB, longitudeGGB)

    // Set the region view to be displayed with the center as 'location', and zoom level
    var region:MKCoordinateRegion = MKCoordinateRegionMake(location, span)

    // Display the region on the particular map object, 'mapView'
    mapView.setRegion(region, animated: true)
}
```

Meguira, Yonathan. "How many lines of code have you written?" Medium. July 16, 2017. © Yonathan Meguira. All rights reserved. This content is excluded from our Creative Commons license. For more information, see <https://ocw.mit.edu/help/faq-fair-use/>.



Massachusetts Institute of Technology



Image courtesy of [the U.S. Department of Homeland Security](#). Source: Wikimedia Commons. This image is in the public domain.

# But what is cyber war?



Healey, Jason. "Cyber Effects in Warfare: Categorizing the Where, What, and Why." *Texas National Security Review* 7, no. 4 (2024): 37-50. © University of Texas Press. All rights reserved. This content is excluded from our Creative Commons license. For more information, see <https://ocw.mit.edu/help/faq-fair-use/>.

---

**Prior to hostilities**

**During hostilities (but not on front lines)**

**During hostilities (on the battlefield)**

---

**Prior to hostilitie**

**During hostilities (n front lines)**

**During h (on the battlefield)**

**Are these distinctions clear cut?**

---

# Some implications...



# Legal Challenges

- Who responds to cyber threats?
  - Government agencies (which ones?)
  - Private firms?
- Title 50 vs. Title 10 Authorities
  - Title 50: Covert action
  - Title 10: Traditional military activity
  - Different under international/domestic law
    - Differing levels of oversight
  - Line is fuzzy...and getting fuzzier
    - "Tug of war" between actors



Image courtesy of [the United States Cyber Command](#).  
Source: Wikimedia Commons. This image is in the public domain.



Image courtesy of [the United States Government](#).  
Source: Wikimedia Commons. This image is in the public domain.



Nakashima, Ellen. "U.S. military cyber operation to attack ISIS last year sparked heated debate over alerting allies," *Washington Post*, May 8, 2017. © Nash Holdings. All rights reserved. This content is excluded from our Creative Commons license. For more information, see <https://ocw.mit.edu/help/faq-fair-use/>.

# Legal Challenges



You have intelligence authorities, Title 50, and you have military authorities, Title 10. Well, what does the commander of Cyber Command do? Does he get to pick and choose between them? You need some way to say, “This kind of thing is military, you have to use the military decision chain,” versus, “this kind of thing is intelligence, you have to use the intelligence decision chain.” I’m not sure they’ve worked through all of that.

Dr. James Lewis, CSIS

© Source unknown. All rights reserved. This content is excluded from our Creative Commons license. For more information, see <https://ocw.mit.edu/help/faq-fair-use/>.

Image courtesy of [the National Security Agency](#). Source: Wikimedia Commons. This image is in the public domain.



Massachusetts Institute of Technology

# Legal Challenges

- Hacking Back?
  - Introduction of Active Cyber Defense Certainty (ACDC) Act
  - Never emerged from committee (multiple times)
- ACDC Act allows for private-sector cyber defense
  - Allows for beacons to track pilfered data ("GPS for data")
  - Potentially allows for destruction/locking up of stolen data
    - Limited ACDMs: Attribute, Disrupt, Monitor
    - List of prohibitions: *Can't impact defense/government computers*
- Would ACDC Act enable violations of existing law?
  - Computer Fraud and Abuse Act
- What are the **political** implications
  - Principal-agent problems?
  - Who are actors here?



Image courtesy of [Aranami](#) on Flickr. License CC BY.



© Michigan State University. All rights reserved.  
This content is excluded from our Creative Commons license. For more information, see <https://ocw.mit.edu/help/faq-fair-use/>.

---

# **Is this all overblown?**

# The Myth of Cyberwar

Erik Gartzke

Bringing War in Cyberspace  
Back Down to Earth

A blitz of media, punditry, and official pronouncements raise the specter of war on the internet. Future conflicts may well take place in cyberspace, where victory or defeat could be determined in mere “nanoseconds.”<sup>1</sup> Secretary of Defense Leon Panetta has even warned of a “cyber-Pearl Harbor.”<sup>2</sup> Nor are fears of cyberwar abstract speculation. Events such as the denial of service attacks against Estonian and Georgian government websites, the Stuxnet worm designed to disable Iranian nuclear centrifuges, and the recent hacking of U.S. military computer networks seem to indicate that the era of cyberwar has already arrived.

Cyberwar can be viewed as the most recent phase in the ongoing revolution in military affairs.<sup>3</sup> This time, however, the threat is said to be directed at the sophisticated technological civilizations of the West, rather than at desert insurgents or the leaders of rogue states with arsenals of inferior second world military hardware. Joseph Nye expresses this emerging consensus, “Dependence on complex cyber systems for support of military and economic activities creates new vulnerabilities in large states that can be exploited by nonstate actors.”<sup>4</sup> Following this logic, the United States appears destined to be “the

---

*Erik Gartzke is Associate Professor of Political Science at the University of California, San Diego, and Professor of Government at the University of Essex.*

The author thanks Susan Aaronson, Tai Ming Cheung, Peter Cowhey, Peter Dombrowski, Eugene Gholz, Florian Grunert, Jeffrey Kwong, Jon Lindsay, John Mueller, and Heather Roff and the anonymous reviewers for comments and encouragement. Oliver Davies provided valuable research assistance.

1. Dan Kuehl, quoted by Grace Chng, “Cyber War: One Strike, and You’re Out,” *Sunday Times* (Singapore), July 18, 2010.
2. Elisabeth Bumiller and Thom Shanker, “Panetta Warns of Dire Threat of Cyberattack,” *New York Times*, October 11, 2012.
3. On the revolution in military affairs (RMA), see Alvin and Heidi Toffler, *War and Anti-War: Survival at the Dawn of the 21st Century* (Boston: Little, Brown, 1993); Andrew F. Krepinevich, “Cavalry to Computer: The Pattern of Military Revolutions,” *National Interest*, No. 37 (Fall 1994), pp. 30–42; Andrew F. Krepinevich, *The Military-Technical Revolution: A Preliminary Assessment* (Washington, D.C.: Center for Strategic and Budgetary Assessments, 2002); Eliot A. Cohen, “A Revolution in Warfare,” *Foreign Affairs*, Vol. 75, No. 2 (March/April 1996), pp. 37–54; Richard Hundley, *Past Revolutions, Future Transformations: What Can the History of Revolutions in Military Affairs Tell Us about Transforming the U.S. Military?* (Santa Monica, Calif.: RAND, 1999); Michael O’Hanlon, “Why China Cannot Conquer Taiwan,” *International Security*, Vol. 25, No. 2 (Fall 2000), pp. 51–86; and Michael G. Vickers and Robert C. Martinage, *The Revolution in War* (Washington, D.C.: Center for Strategic and Budgetary Assessments, 2004). For criticism of the RMA, see Stephen Biddle, “Assessing Theories of Future Warfare,” *Security Studies*, Vol. 88, No. 1 (Autumn 1998), pp. 1–74.
4. Joseph Nye, “Cyber Power” (Cambridge, Mass.: Belfer Center for Science and International Affairs, Harvard Kennedy School, May 2010), p. 4.

# The Subversive Trilemma

Lennart Maschmeyer

## Why Cyber Operations Fall Short of Expectations

For three decades, states have engaged in cyber conflict, yet the strategic utility of cyber operations remains unclear. Strategic utility refers to measurable contributions toward a state's political goals or shifts in the balance of power.<sup>1</sup> Similar to the 1920s–1940s air power debates, scholars have expected new technology to revolutionize conflict and provide independent utility.<sup>2</sup> When warplanes first emerged, some experts predicted the end of conventional warfare because airplanes were able “to strike mortal blows to the heart of the enemy at lightning speed.”<sup>3</sup> Similarly, when the World Wide Web gained popularity in the 1990s, some analysts predicted a future of cyberwar in which “neither mass nor mobility but information” would become decisive.<sup>4</sup> Subsequent theorizing envisioned strategic cyber strikes similar to strategic aerial attacks, shaping fears of a “cyber Pearl Harbor.”<sup>5</sup> There is, however, a key difference between the two.

Lennart Maschmeyer is a senior researcher at the Center for Security Studies at ETH Zürich.

The author thanks Ronald Deibert, Jesse Driscoll, Nadiya Kostyuk, Gabrielle Lim, Jon Lindsay, Louis Pauly, Irene Poetranto, Max Smeets, Lucan Way, the team at the Citizen Lab at the University of Toronto, the team at the Center for Security Studies at ETH Zürich (especially Alexander Bollfrass, Myriam Dunn Cavelty, Mauro Gilli, Enzo Nussio, and Andreas Wenger), as well as the anonymous reviewers for their helpful comments on earlier drafts of this article. He is also grateful to Lesia Bidochko, Daria Goriacheva, Oksana Grechko, and Mariya Green for research assistance. The author is also indebted to Olga Paschuk for her interpretation services in Ukraine. Finally, the author thanks Lisa Maschmeyer for designing figure 1. The online appendix for this article is available at [doi.org/10.7910/DVN/LZ65MC](https://doi.org/10.7910/DVN/LZ65MC).

1. Robert A. Pape, *Bombing to Win: Air Power and Coercion in War* (New York: Cornell University Press, 1996), p. 57.

2. See, for example, Winn Schwartzau, *Information Warfare: Cyberterrorism: Protecting Your Personal Security in the Electronic Age*, 2nd ed. (New York: Thunder's Mouth, 1996); Dima Adamsky and Kjell Inge Bjerga, “Introduction to the Information-Technology Revolution in Military Affairs,” *Journal of Strategic Studies*, Vol. 33, No. 4 (2010), pp. 463–468, [doi.org/10.1080/01402390.2010.489700](https://doi.org/10.1080/01402390.2010.489700); Lucas Kello, “The Meaning of the Cyber Revolution: Perils to Theory and Statecraft,” *International Security*, Vol. 38, No. 2 (Fall 2013), pp. 7–40, [doi.org/10.1162/ISEC\\_a\\_00138](https://doi.org/10.1162/ISEC_a_00138); and Jacquelyn Schneider, “The Capability/Vulnerability Paradox and Military Revolutions: Implications for Computing, Cyber, and the Onset of War,” *Journal of Strategic Studies*, Vol. 42, No. 6 (2019), pp. 841–863, [doi.org/10.1080/01402390.2019.1627209](https://doi.org/10.1080/01402390.2019.1627209).

3. Giulio Douhet, *The Command of the Air*, trans. Dino Ferrari (Washington, D.C.: Office of Air Force History, 1983), p. 15.

4. John Arquilla and David Ronfeldt, “Cyberwar Is Coming!” *Comparative Strategy*, Vol. 12, No. 2 (1993), pp. 141–165, [doi.org/10.1080/01495939308402915](https://doi.org/10.1080/01495939308402915).

5. James P. Farwell and Rafal Rohozinski, “Stuxnet and the Future of Cyber War,” *Survival*, Vol. 53, No. 1 (2011), pp. 23–40, [doi.org/10.1080/00396338.2011.555586](https://doi.org/10.1080/00396338.2011.555586); Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do about It* (New York: HarperCollins, 2010); and James J. Wirtz, “The Cyber Pearl Harbor,” in Emily O. Goldman and John Arquilla, eds., *Cyber Analogies* (Monterey, Calif.: Naval Postgraduate School, 2014).



---

**"Inferior to terrestrial wars...[cyber is] not likely to serve as final arbiter."**

---

**"Not even useful as an isolated instrument  
of coercive foreign policy."**

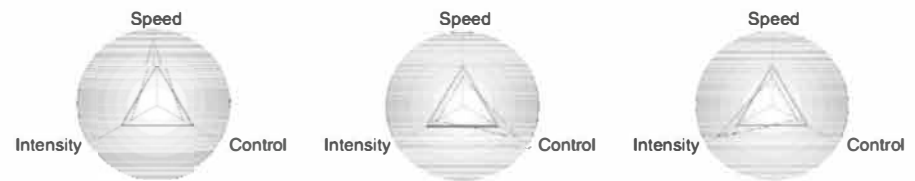
---

# The Myth of Cyberwar?

- Deterrence + coercion is difficult in cyberspace
  - Attribution is challenging
  - Use it and Lose it capabilities
  - Temporary effects
- Military operations have political goals
  - Can't hold territory
  - Cyber must operate alongside military force
    - Gartzke references Stuxnet...valid comparison?
- What do we think of these claims



Figure 1. The Subversive Trilemma



NOTE: In each diagram, the dotted triangle shows how increasing one of these three variables tends to decrease the others compared with a given state in which all are balanced, which is represented by the solid triangle.

Maschmeyer, Lennart. Figure 1: The Subversive Trilemma. From "The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations." *International Security* 46, no. 2 (2021): 51–90. © The President and Fellows of Harvard College and the Massachusetts Institute of Technology. Used with permission.

# Battlefield Effects?

- Kostyuk and Zhukov use data from Syria and Ukraine (pre-2022)
- Timing of cyber actions is independent of ground combat
  - Examine thousands of cyber operations by both government/anti-government forces
- No strategic interaction between “cyber warriors”
  - Independent campaigns

# The Myth of Cyberwar?



© Sony Pictures Releasing. All rights reserved. This content is excluded from our Creative Commons license. For more information, see <https://ocw.mit.edu/help/faq-fair-use/>.

# The Myth of Cyberwar?



Image courtesy of [the U.S. Navy, Office of Public Relations](#). Source: Wikimedia Commons. This image is in the public domain.

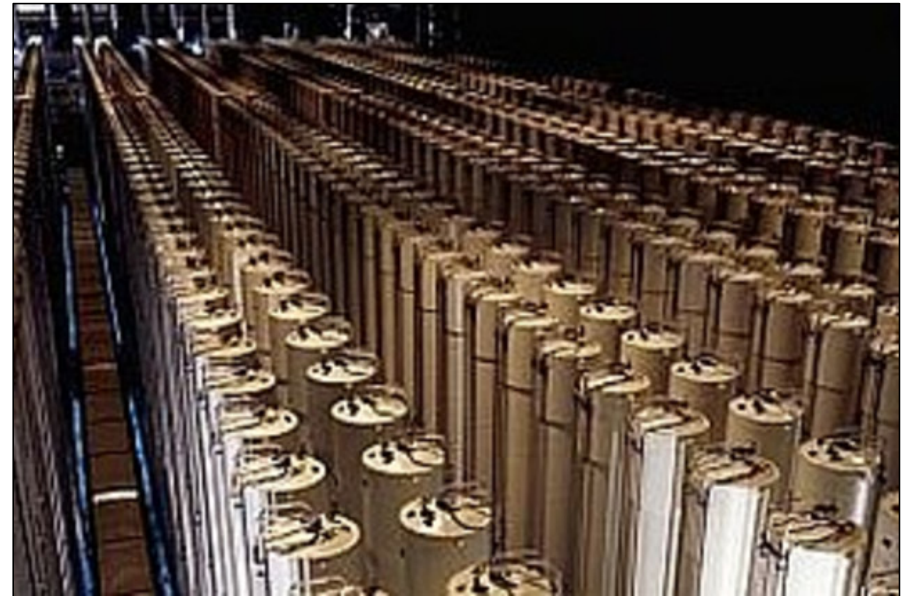


Image courtesy of [the Nuclear Regulatory Commission](#). Source: Wikimedia Commons. License CC BY.



Massachusetts Institute of Technology



# The Myth of Cyberwar?

The New York Times

## *Trump Inherits a Secret Cyberwar Against North Korean Missiles*



Sanger, David E. and William J. Broad. "Trump Inherits a Secret Cyberwar Against North Korean Missiles," *New York Times*, March 4, 2017. © The New York Times Company. All rights reserved. This content is excluded from our Creative Commons license. For more information, see <https://ocw.mit.edu/help/faq-fair-use/>.



# Escalation in the Cyber Domain

World News | Europe

## NATO Warns Use of Article 5 Over Cyber Attack, Members Pledge Spending Increase

June 2017

"NATO Warns Use of Article 5 Over Cyber Attack, Members Pledge Spending Increase," *Haaretz*, June 28, 2017. © Haaretz Daily Newspaper Ltd. All rights reserved. This content is excluded from our Creative Commons license. For more information, see <https://ocw.mit.edu/help/faq-fair-use/>.

## *U.S. Had Cyberattack Plan if Iran Nuclear Dispute Led to Conflict*



By David E. Sanger and Mark Mazzetti

Sanger, David E., and Mark Mazzetti. "U.S. Had Cyberattack Plan if Iran Nuclear Dispute Led to Conflict," *New York Times*, February 16, 2016. © The New York Times Company. All rights reserved. This content is excluded from our Creative Commons license. For more information, see <https://ocw.mit.edu/help/faq-fair-use/>.



Massachusetts Institute of Technology

The New York Times

## Pentagon Suggests Countering Devastating Cyberattacks With Nuclear Arms

WOTR  
warontherocks.com



The Nuclear Posture Review was written at the Pentagon and is being reviewed by the White House. Charles Dharapak/Associated Press

Sanger, David E., and William J. Broad. "Pentagon Suggests Countering Devastating Cyberattacks With Nuclear Arms," *New York Times*, January 16, 2018. © The New York Times Company. All rights reserved. This content is excluded from our Creative Commons license. For more information, see <https://ocw.mit.edu/help/faq-fair-use/>.

---

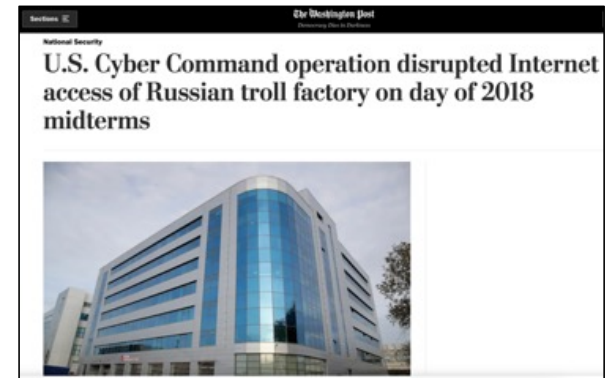
**What does this tell us about the conditions under which cyber operations might have greatest effect?**

# Concepts: Escalation

- Increase in intensity or scope of conflict
  - Vertical or horizontal (Morgan et al 2008; Smoke 1977)
  - Escalation ladder? (Kahn 1968)
  - Wormhole?
- Thresholds: “dividing lines”
  - “New action” vs. “More of the same” (Schelling 1967)
- Action-reaction process
  - Interaction dictates escalation (Carson 2018)
  - Context dependent (Smoke 1977)
- Crises
  - Heightened likelihood of hostilities (Brecher 1993)



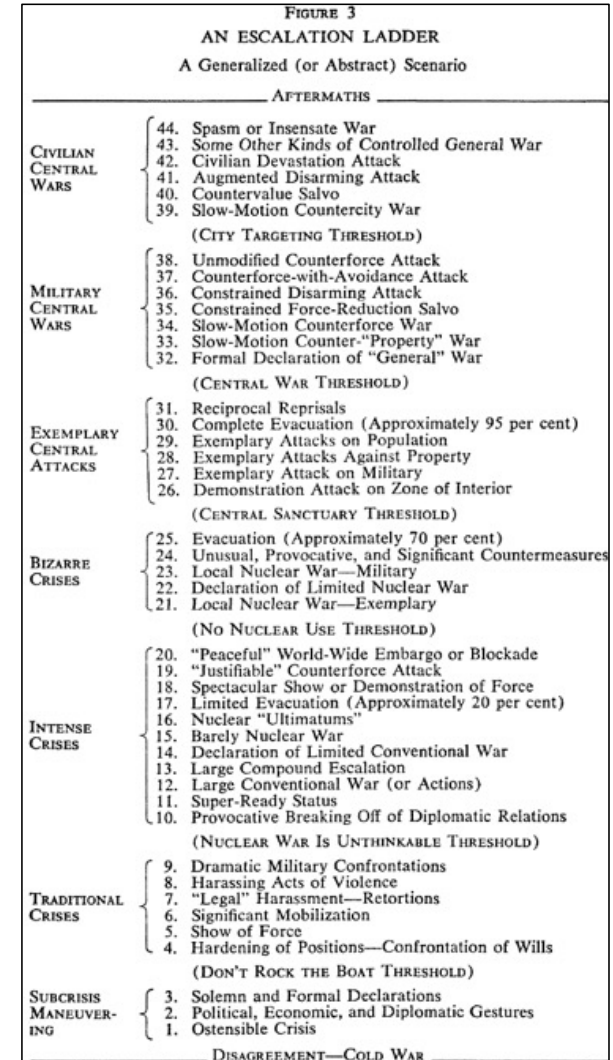
Image courtesy of [the Federal Government of the United States](#).  
Source: Wikimedia Commons. This image is in the public domain.



Nakashima, Ellen. "U.S. Cyber Command operation disrupted Internet access of Russian troll factory on day of 2018 midterms," *Washington Post*, February 26, 2019. © Nash Holdings. All rights reserved. This content is excluded from our Creative Commons license. For more information, see <https://ocw.mit.edu/help/faq-fair-use/>.

# Concepts: Escalation

- Escalation control: Low rungs on ladder
- Not a total absence of hostilities
  - Backstage activity (Carson 2018)
  - Stability-Instability Paradox (Snyder 1961)
  - US, Israel military doctrines (IDF 2016)
- Where does cyber fit on the escalation ladder?



Kahn, Herman. "Figure 3: An Escalation Ladder." From *On Escalation: Metaphors and Scenarios*. Routledge, 2009. © Routledge. All rights reserved. This content is excluded from our Creative Commons license. For more information, see <https://ocw.mit.edu/help/faq-fair-use/>.

---

# **How should we study whether cyber warfare is escalatory?**

---

# Emerging Technologies + IR

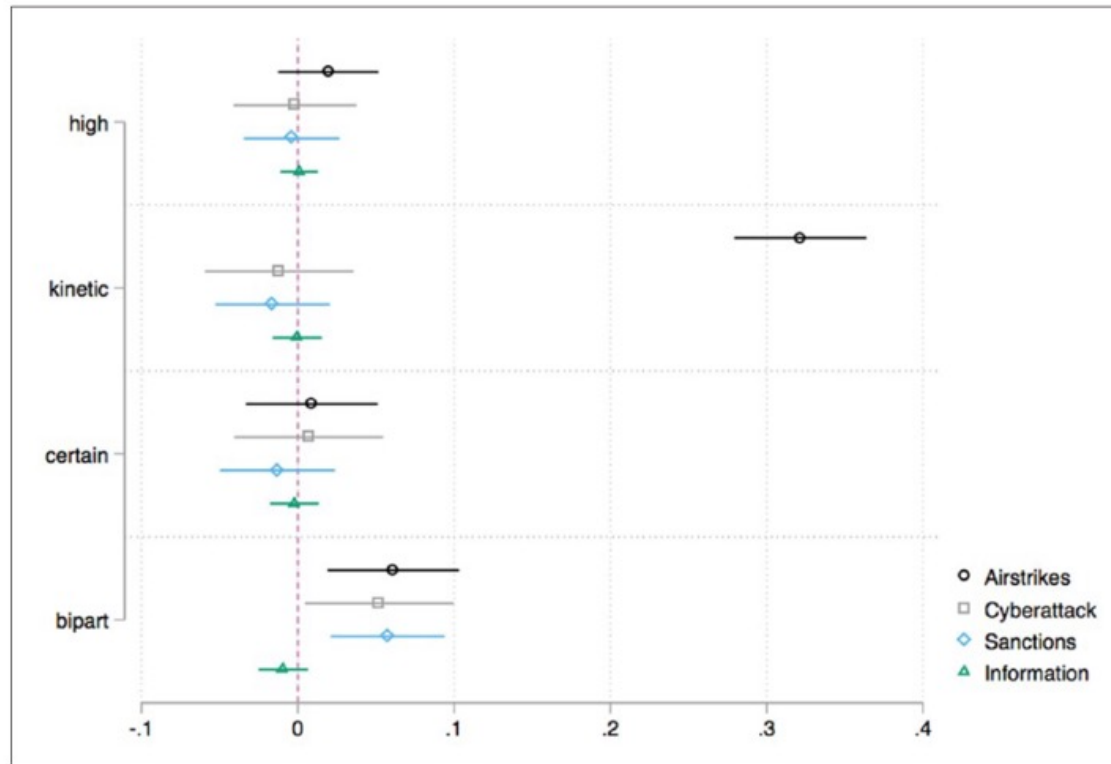
- Confront the fundamental problem of causal inference



# Determinants of Retaliation

- Kreps and Das (2017)
  - RQ: What affects public support for retaliation following a cyber attack?
- Driving Factors:
  - Kinetic vs. Non-kinetic (H1a)
    - Banks vs. Nuclear infrastructure
  - Scale (H1b)
    - \$3B vs. \$30B / hundreds vs. thousands
  - Certainty of attribution (H2)
    - Probably vs. almost certainly (Russia)
  - Elite consensus on attribution (H3)
    - Bipartisan support vs. w/o bipartisan support
- What are our expectations for each of these factors?

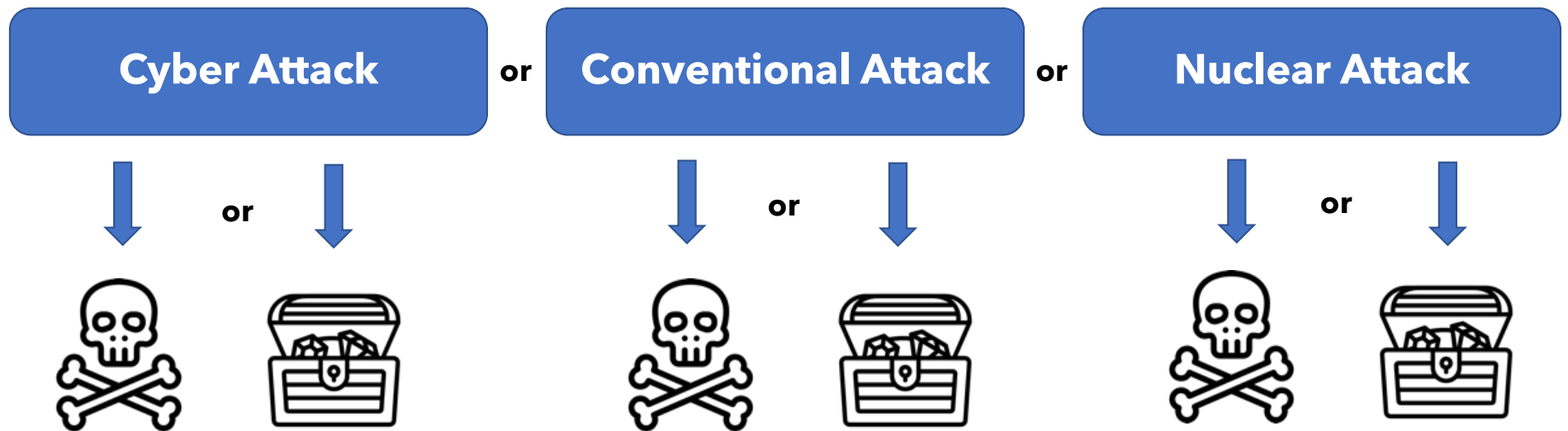
# Determinants of Retaliation



# Variation in Escalation

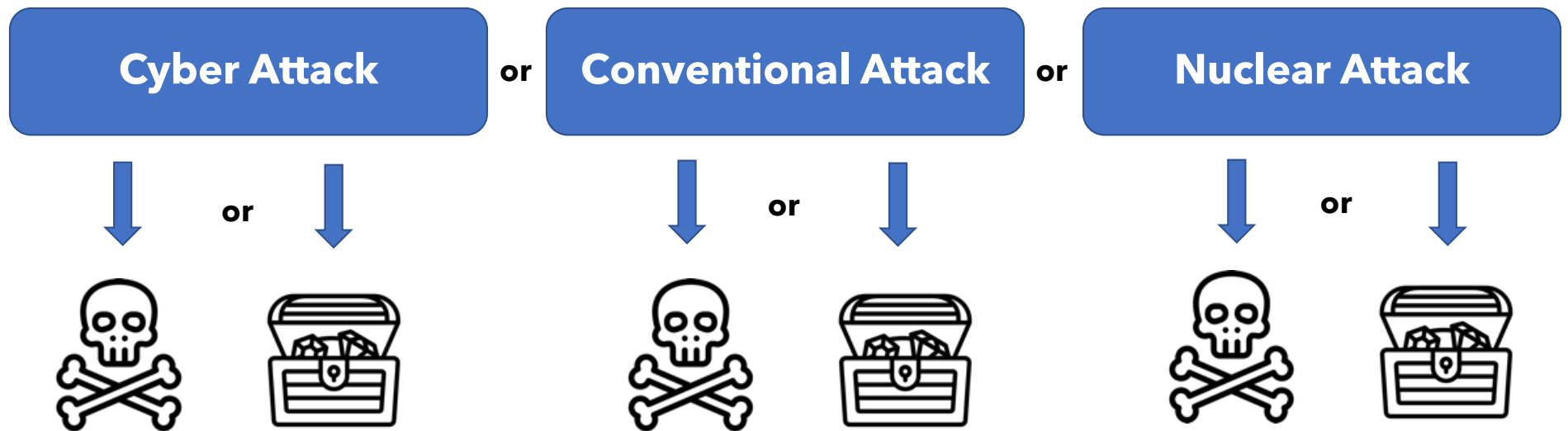
- Kreps and Schneider (2019)
  - RQ: Do cyber and conventional attacks drive the same types of responses?
- Two theoretical escalation pathways
  - Means based ("of a different kind")
  - Effects based
- "Firebreaks" in means based pathway
  - Cold Wars have a nuclear firebreak (or threshold)
  - But, (typically) difference in nuke vs. conventional effects
- So how should we set up this experiment?
  - What should we manipulate?
  - Who should our sample (respondents) be?

# Variation in Escalation



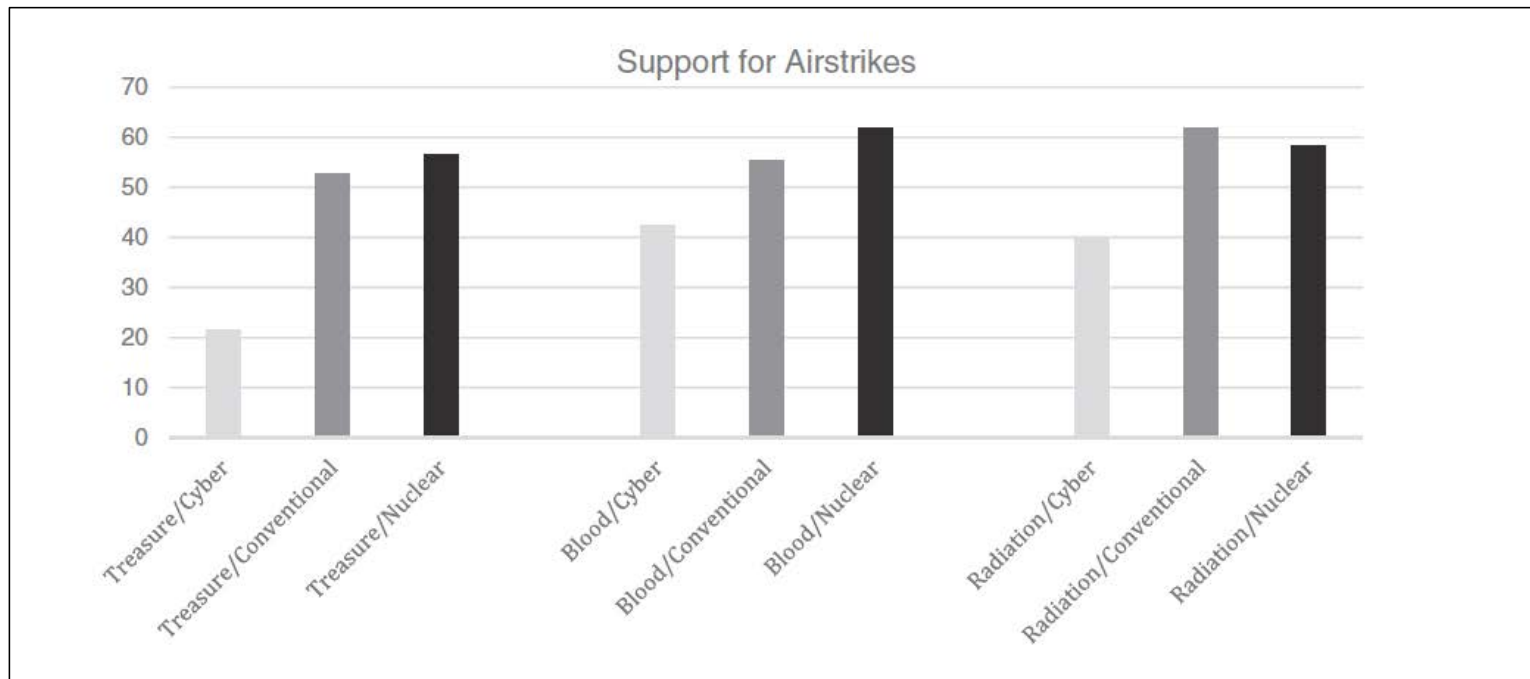
**How would you retaliate?**

# Variation in Escalation



**Thoughts on research design?**  
**Sample, Country, Confounders?**

# Variation in Escalation





## Credits for the images on page 19

Seal of the United States Cyber Command. Image courtesy of [the United States Cyber Command](#). Source: Wikimedia Commons. This image is in the public domain.

United States Tenth Fleet seal. Image courtesy of [the U.S. Navy](#). Source: Wikimedia Commons. This image is in the public domain.

Emblem of the 16th Air Force of the United States Air Force. Image courtesy of [the U.S. Air Force](#). Source: Wikimedia Commons. This image is in the public domain.

United States Army Cyber Command Shoulder Sleeve Insignia. Image courtesy of [the U.S. Army Institute of Heraldry](#). Source: Wikimedia Commons. This image is in the public domain.

Deputy Chief of Staff for Intelligence, Surveillance, Reconnaissance, and Cyber Effects Operations of the United States Air Force emblem. Image courtesy of [the U.S. Air Force](#). Source: Wikimedia Commons. This image is in the public domain.

US Army Cyber Branch Insignia. Image courtesy of [the U.S. Army Institute of Heraldry](#). Source: Wikimedia Commons. This image is in the public domain.

Information Dominance Corps breast insignia. Image courtesy of [N2/N6C111](#). Source: Wikimedia Commons. This image is in the public domain.

New Air Force cyberspace badge. Image courtesy of [the U.S. Air Force](#). This image is in the public domain.

Emblem of Air Force Cyber Command (Provisional) of the United States Air Force. Image courtesy of [the U.S. Air Force](#). Source: Wikimedia Commons. This image is in the public domain.

Emblem of Air Force Space Command of the United States Air Force. Image courtesy of [the U.S. Air Force](#). Source: Wikimedia Commons. This image is in the public domain.

Emblem of the 24th Air Force of the United States Air Force. Image courtesy of [the U.S. Army Institute of Heraldry](#). Source: Wikimedia Commons. This image is in the public domain.

Emblem of the USAF Air Combat Command. Image courtesy of [the U.S. Army](#). Source: Wikimedia Commons. This image is in the public domain.

Emblem of the 16th Air Force of the United States Air Force. Image courtesy of [the U.S. Air Force](#). Source: Wikimedia Commons. This image is in the public domain.

Logo for United States Air Force Cyber Command (AFCYBER). Image courtesy of [afcyber.af.mil, VRIN 180405-F-ZZ999-0002.PNG](#). Source: Wikimedia Commons. This image is in the public domain.

MIT OpenCourseWare  
<https://ocw.mit.edu>

17.449 Emerging Technology and International Security  
Fall 2024

For information about citing these materials or our Terms of Use, visit: <https://ocw.mit.edu/terms>.