
Emerging Technology + International Security

17.449

Erik Lin-Greenberg

Associate Professor of Political Science

Massachusetts Institute of Technology

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

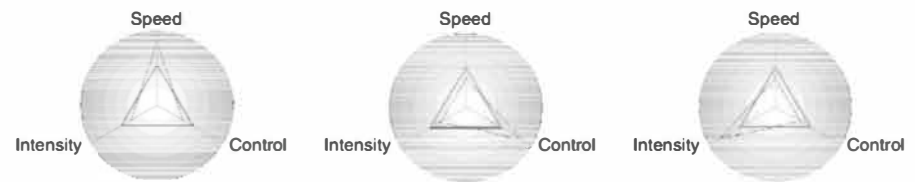
The Myth of Cyberwar?

- 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.

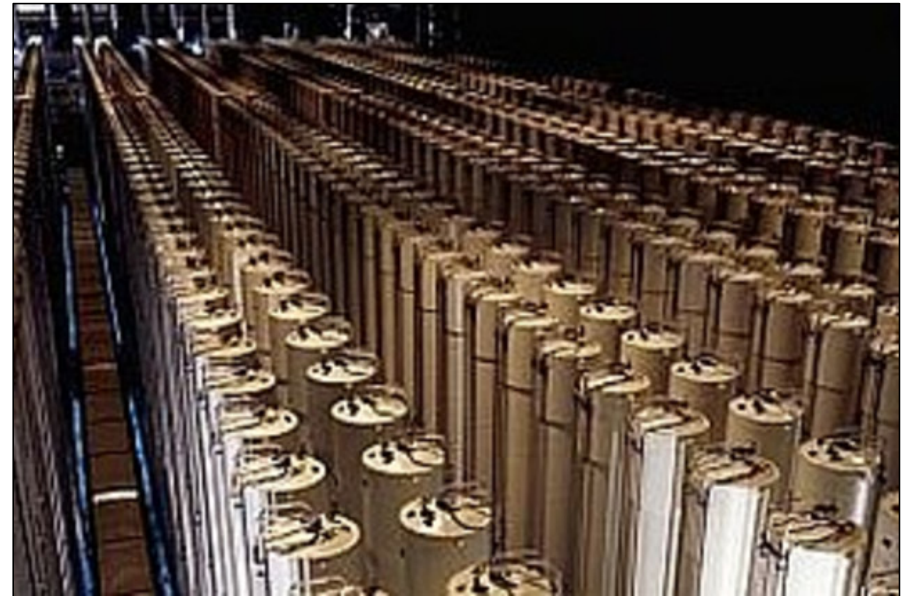


Image courtesy of [the Nuclear Regulatory Commission](#). Source: Wikimedia Commons. License CC BY.

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/>.

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/>.

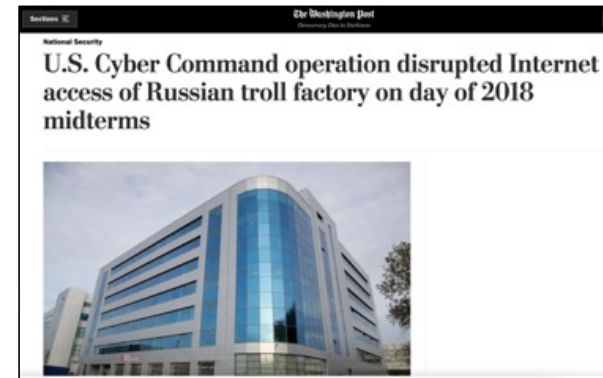
What does this tell us about the conditions under which cyber operations might have greatest effect?

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)



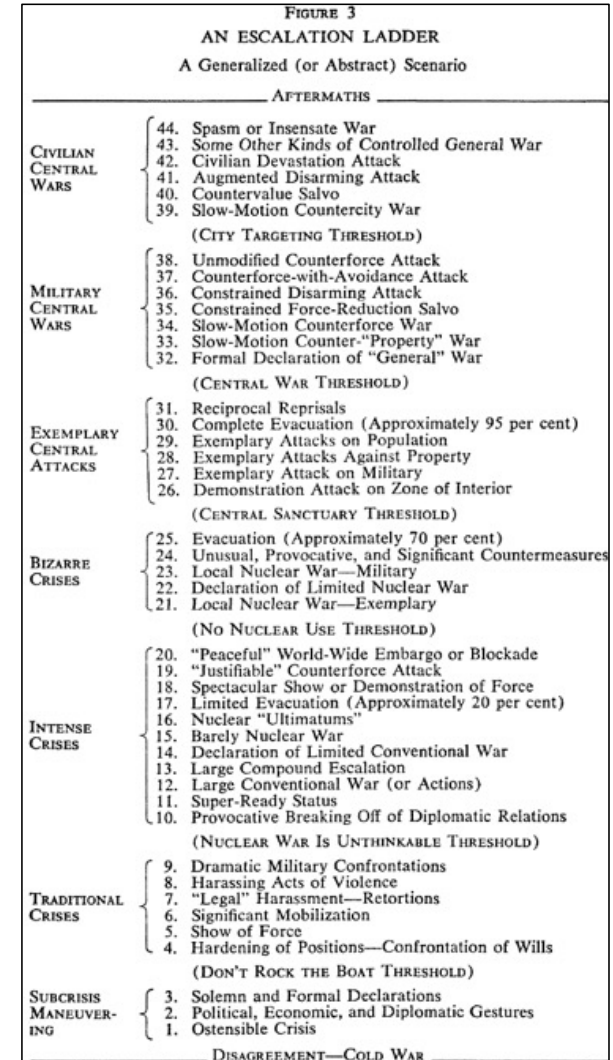
Image courtesy of [the Federal Government of the United States](#).
Source: Wikimedia Commons. This image is in the public domain.



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?

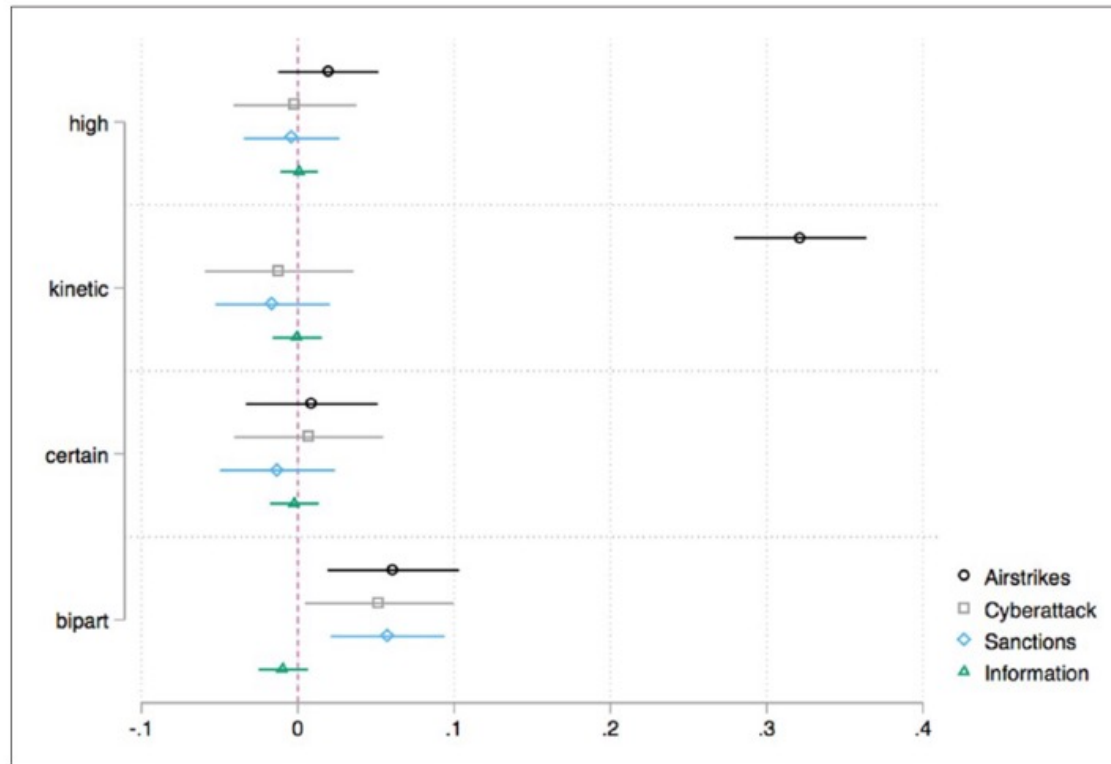
Emerging Technologies + IR

- 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?

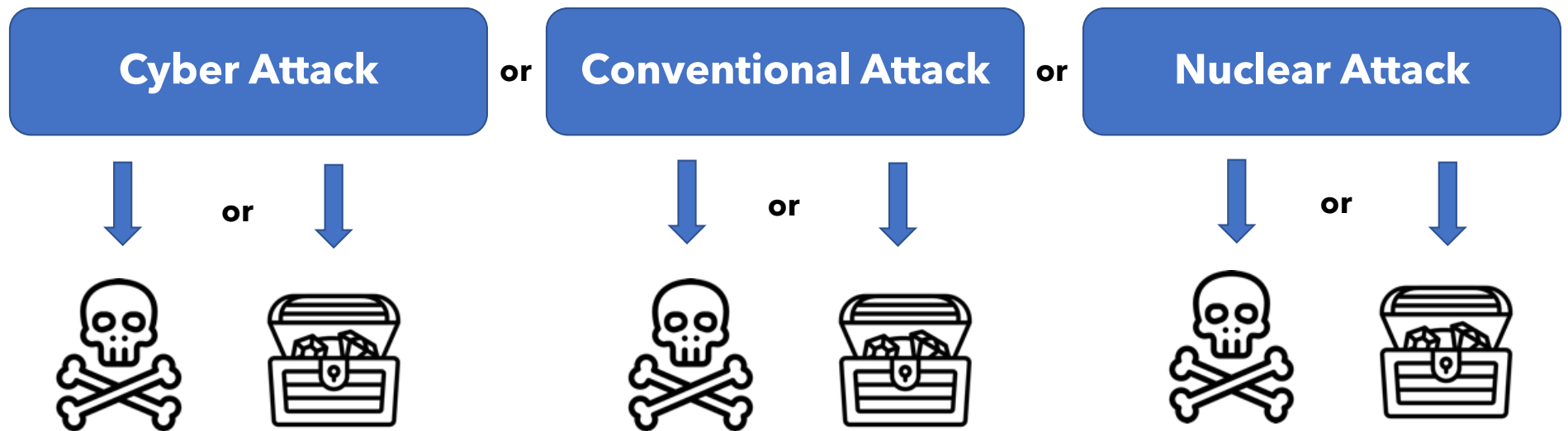
Determinants of Retaliation



Variation in Escalation

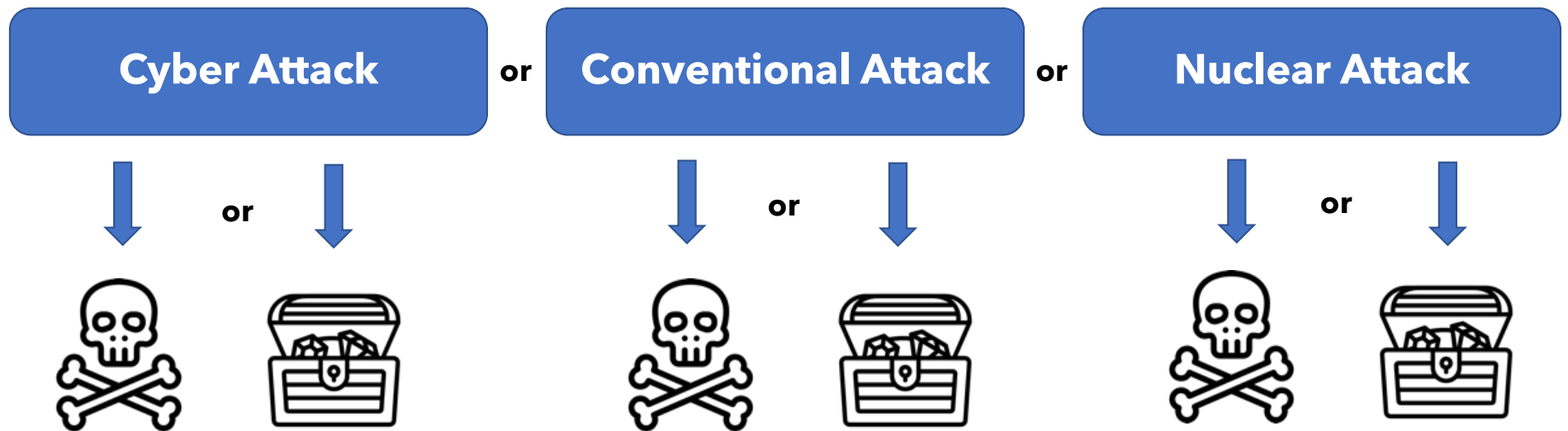
- Kreps and Schneider (2019)
 - RQ: Do cyber and conventional attacks drive the same types of responses?
- Two theoretical escalation pathways
 - Means based ("of a different kind")
 - Effects based
- "Firebreaks" in means based pathway
 - Cold Wars have a nuclear firebreak (or threshold)
 - But, (typically) 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



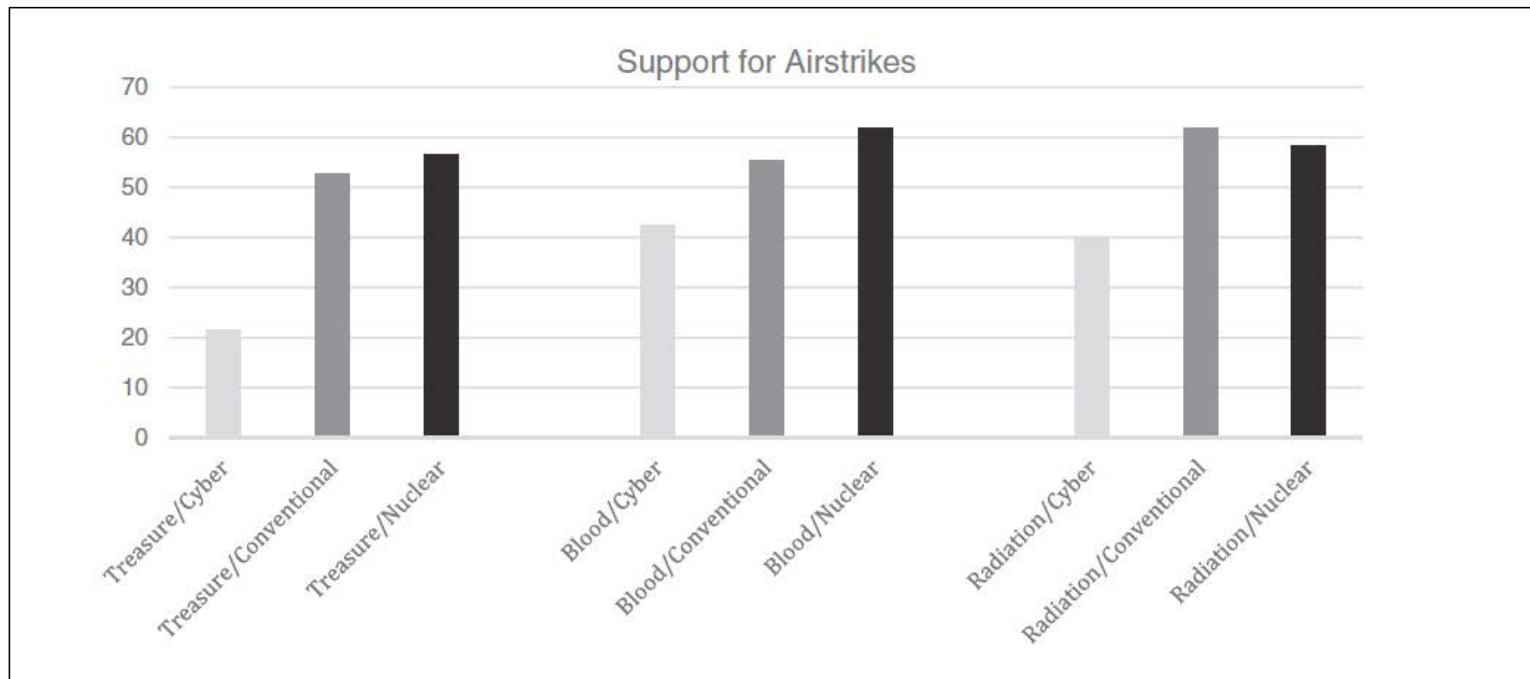
How would you retaliate?

Variation in Escalation



Thoughts on research design?
Sample, Country, Confounders?

Variation in Escalation



Drones

Key Questions

- What is a drone and how did they come to be?
 - International + Domestic Drivers
- How do they change the character of warfare?
 - Borders, battlefields, and combatants
- What are their battlefield consequences?
 - Users: States vs. Non-state Actors
 - Targets: States vs. Non-state actors



Image courtesy of [88 Air Base Wing Public Affairs](#). Source: Wikimedia Commons.
This image is in the public domain.

Concepts: Drones

- Remotely operated military systems
 - Air, land, sea
 - Armed/Unarmed
- Battlefield effects without frontline personnel
 - Earlier technology required battlefield personnel
- Increasingly common (80+ countries)
- Substitutive vs. additive employment



Image courtesy of [Lt. Col. Leslie Pratt / U.S. Air Force](#).
Source: Wikimedia Commons. This image is in the public domain.



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



Image courtesy of [Olivier Dugornay \(IFREMER, Pôle Images, Centre Bretagne - ZI de la Pointe du Diable - CS 10070 - 29280 Plouzané, France\)](#).
Source: Wikimedia Commons. License CC BY.

Image courtesy of [Valder137](#) on Wikimedia Commons. License CC BY.



Kettering Bug, 1918

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



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



Operation Sandstone, 1947-8

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



Project Brass Ring, 1949



Image courtesy of [Tech. Sgt. Emerson Nuñez of the U.S. Air Force](#). Source:Wikimedia Commons.
This image is in the public domain.



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

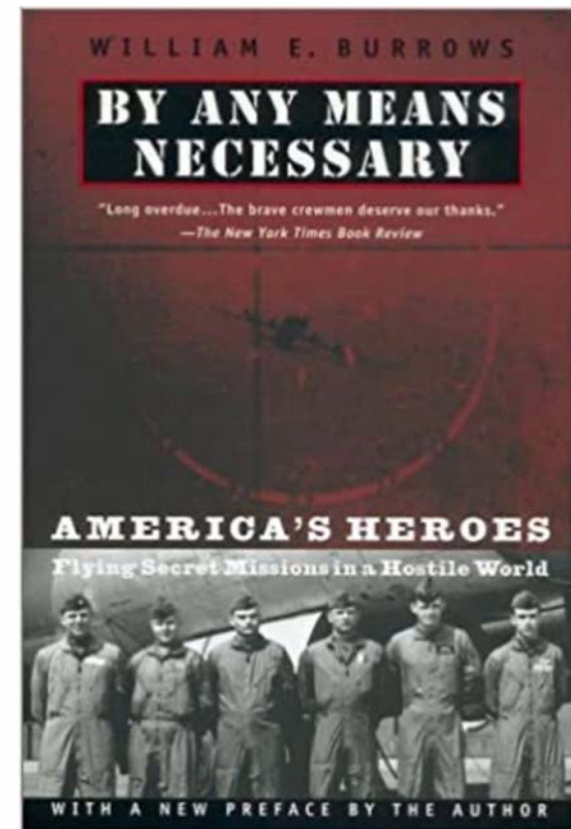
Image courtesy of [USGOV-PD](#). Source: Wikimedia Commons. This image is in the public domain.



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



Image courtesy of [Larry Bessel of the Los Angeles Times](#). Source: Wikimedia Commons. License CC BY.



Burrows, William E. *By Any Means Necessary*. Plume, 2002.
© Plume. All rights reserved. This content is excluded from our Creative Commons license. For more information, see <https://ocw.mit.edu/help/faq-fair-use/>.



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



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



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



Image courtesy of [Ken LaRock of the United States Air Force](#). This image is in the public domain.

Reconnaissance Drone - Korea (U)

(S) On 14 Dec 72, the Joint Chiefs of Staff directed that collection requirements for the COMBAT DAWN high-altitude drone signal intelligence (SIGINT) collection mission at Osan AB, Korea be increased from 30 hours per month to 60 hours per month and that an assessment be made of the adequacy of the 60 hour coverage rate not later than 6 months after the start of the expanded coverage.⁸ SAC initiated the 60 hours per month collection rate on 1 Jan 73. The assessment by the Defense Intelligence Agency and the National Security Agency is expected soon after 30 Jun 73. Meanwhile, the

6. CSAF memo for JCS, CSAFM 291-72, 21 Dec 1972.

7. JCS memo for CSAF, (SM-251-73), 22 May 1973, CORONET DOCTOR (U).

8. JCS 2010/441, 7 Dec 72.

TOP SECRET

This image is in the public domain.

This image is in the public domain.

Approved For Release 2000/04/17 : CIA-RDP78B04560A006100010022-7

SECRET

NPIC/R-194/67

NO FOREIGN DISSEM



TOP SECRET

HANDLE VIA

Approved For Release 2003/09/30 : CIA-RDP79B01709A000100060004-2

TAGBOARD

File: TAGBOARD

25X1A

THE JOINT CHIEFS OF STAFF
WASHINGTON, D.C. 20301

5 March 1971

MEMORANDUM FOR THE HOLDERS OF THE SPECIAL OVERFLIGHT SUPPLEMENT

Subject: TAGBOARD Mission D-550 Resume

1. (TS/) The D-21 (TAGBOARD) drone reconnaissance mission scheduled for the month of March 1971 was executed on 5 March. The drone launched from the B-52 mothership on schedule at 05/0356Z and flew the preset route (attached) over South China exactly as programmed. Recovery package ejection occurred on time at 05/0530Z and was sighted by the JC-130 recovery aircraft at 05/0531Z. Because of probable air pickup chute failure; aerial recovery was not possible and the package impacted in the water 10 nm northwest of the predicted impact point at 05/0558Z. This malfunction differed from the failure on the previous mission in that the package apparently experienced a retarded if not soft landing, transmitted required telemetry signals, and floated for approximately one hour. The destroyer, USS McMorris, the back-up recovery ship, steamed to the splash down point and had visual sighting at 05/0700Z. Telemetry was lost at 05/0655Z and the destroyer reported loss of visual contact and unsuccessful boarding attempt at 05/0714Z due to extremely rough seas. The recovery destroyer remains in the impact area; however, the recovery package is assumed sunk in approximately 2100 fathoms of water.

This image is in the public domain.



NPIC L-9926

NPIC BASE 36

1967



Massachusetts Institute of Technology

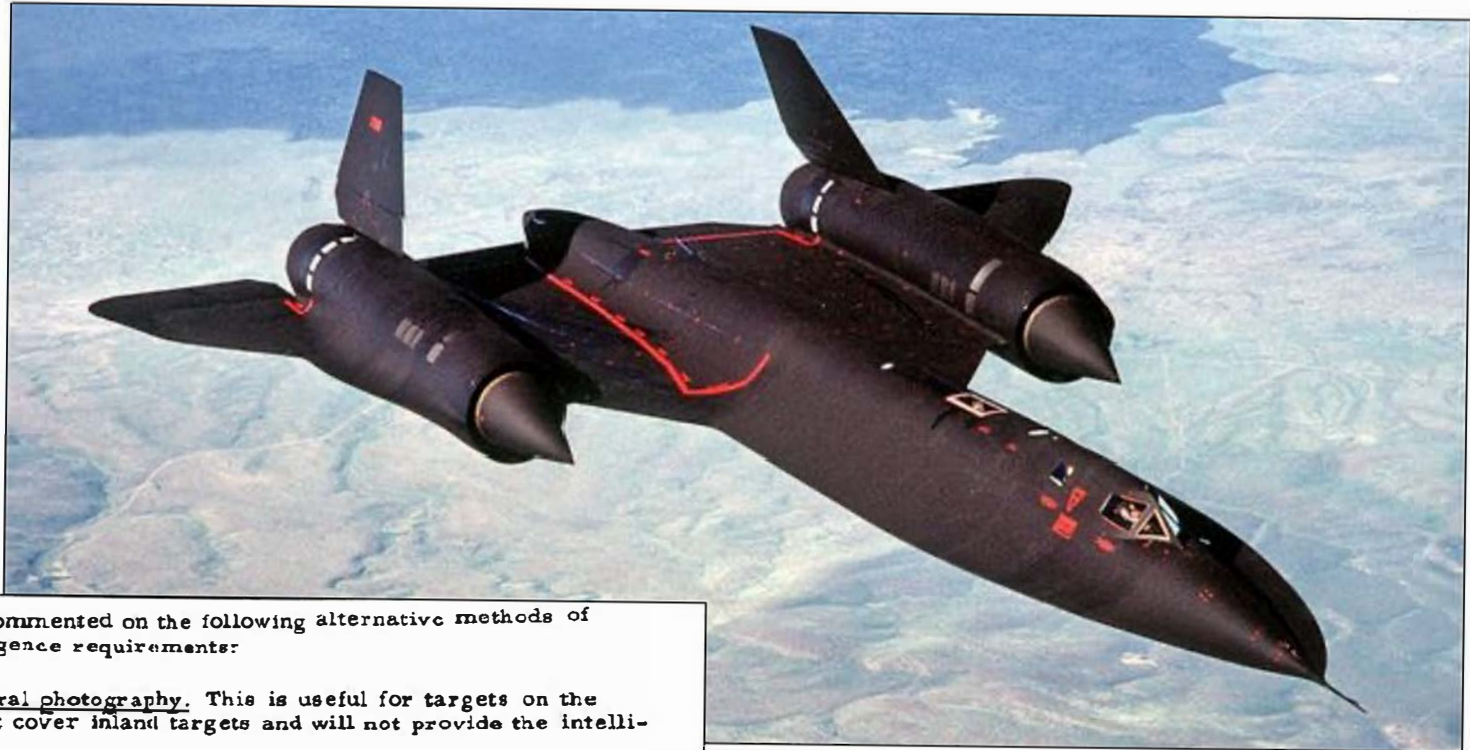
Image courtesy of [the CIA](#). Source: Wikimedia Commons. This image is in the public domain.



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



Image courtesy of [PHC Lawrence B. Foster of the U.S. Navy](#).
Source: Wikimedia Commons. This image is in the public domain.



Director McCone commented on the following alternative methods of fulfilling our intelligence requirements:

(1) Peripheral photography. This is useful for targets on the coast but it does not cover inland targets and will not provide the intelligence we require.

(2) Drones. They do not produce as good coverage as the U-2. They are more vulnerable. The shooting down of a drone would call for a different response by the U.S. because no pilot is involved.

Image courtesy of [TSgt. Michael Haggerty / U.S. Air Force](#). Source: Wikimedia Commons. This image is in the public domain.

This image is in the public domain.



Massachusetts Institute of Technology



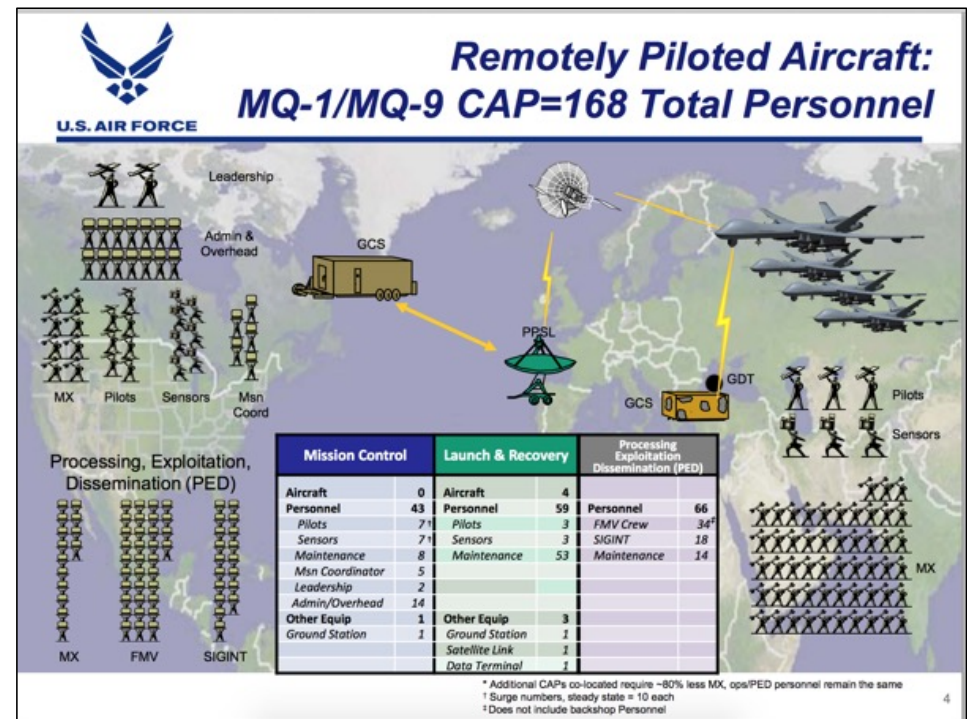
Image courtesy of [the White House Photographic Office](#). Source: Wikimedia Commons. This image is in the public domain.



From "The Post-INF Treaty Crisis: Background and Next Steps." *Arms Control Today* 11, no. 8 (2019). © Arms Control Association. All rights reserved. This content is excluded from our Creative Commons license. For more information, see <https://ocw.mit.edu/help/faq-fair-use/>.



Gettinger, Dan. "Drone Geography: Mapping a System of Intelligence." February 19, 2015. © The Center for the Study of the Drone at Bard College. All rights reserved. This content is excluded from our Creative Commons license. For more information, see <https://ocw.mit.edu/help/faq-fair-use/>.



Gettinger, Dan. "Drone Geography: Mapping a System of Intelligence." February 19, 2015. © The Center for the Study of the Drone at Bard College. 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 U.S. Air Force](#). Source: Wikimedia Commons. This image is in the public domain.



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



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



Image courtesy of [Tech. Sgt. Sabrina Johnson of the U.S. Air Force](#). Source: Wikimedia Commons. This image is in the public domain.

Battlefield Consequences

The New York Times

What We Know About Iran Shooting Down a U.S. Drone

The two countries disagree about where the drone was shot down: over international waters or in Iranian airspace.



Cooper, Helene. "What We Know About Iran Shooting Down a U.S. Drone," *New York Times*, June 20, 2019. © 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/>.

Do Drones Fail or Succeed?



Image courtesy of [New America Foundation](#). Source: Wikimedia Commons. License CC BY.



Image courtesy of [World Economic Forum](#) on Flickr. License CC BY-NC-SA.

Drones: Succeed

- Low risk, Low cost alternative
 - Alternatives are risky
 - Delegating to allies: Operational + Intelligence Risk
 - Ground forces/Inhabited Assets
- Perceived as less of an affront than other methods
 - Can reduce civilian casualties (maybe?)
 - Signature strikes are problematic
- What to do with detainees?
- Based on logic of leadership decapitation
 - Personalization of warfare
 - Eliminates top leaders = confusion (maybe?)
 - Changes insurgent behavior (radio silence, conduct of operations)

Drones: Fail

- Attractive, but ineffective option
 - Vulnerable assets
 - Don't solve root cause of issues
 - Don't collect intelligence
- What are strategic goals
 - Tactical solution vs. Strategic goals
- Provides propaganda that can drive recruitment
 - Backlash (e.g. May 2010 Times Square attack)
- Does decapitation work?
 - Groups like al-Qaeda might survive decapitation
 - Groups can adapt

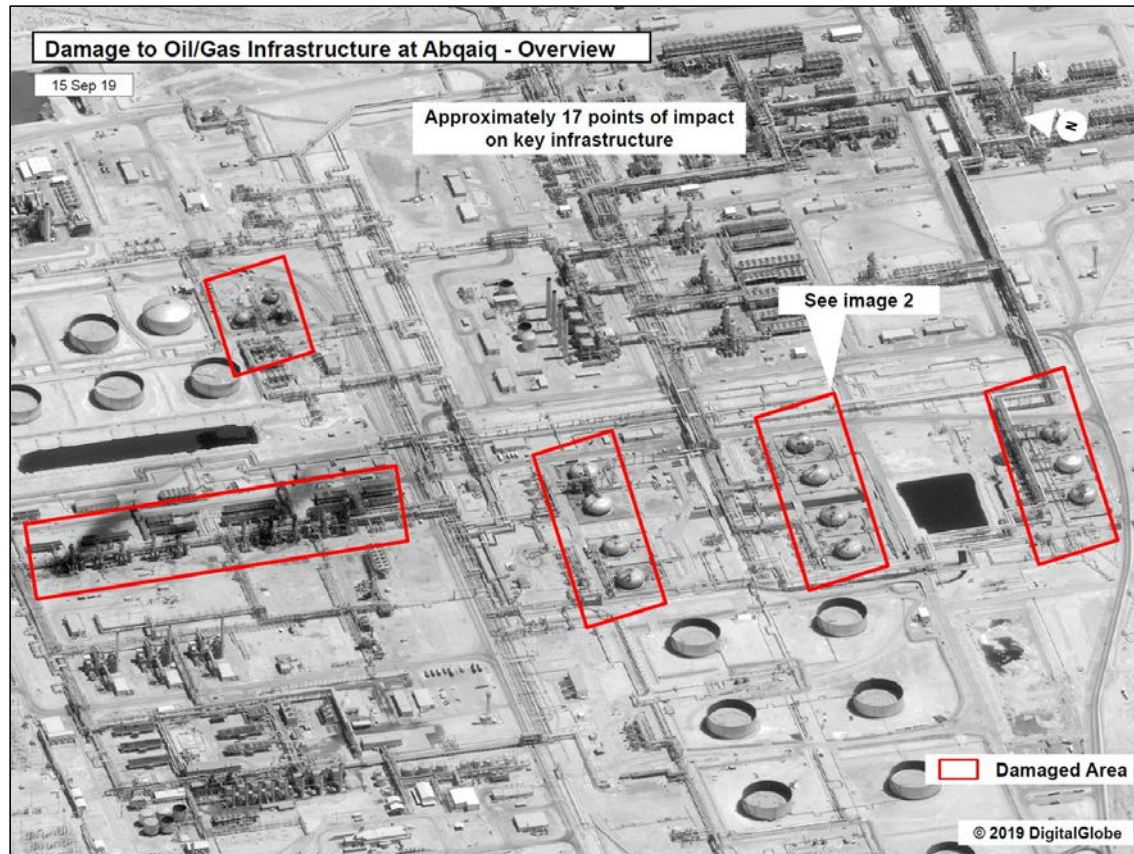
1. It is possible to know the intention and the mission of the drone by using the Russian-made "sky grabber" device to infiltrate the drone's waves and the frequencies. The device is available in the market for \$2,595 and the one who operates it should be a computer know-how.
2. Using devices that broadcast frequencies or pack of frequencies to disconnect the contacts and confuse the frequencies used to control the drone. The Mujahideen have had successful experiments using the Russian-made "Racal."
3. Spreading the reflective pieces of glass on a car or on the roof of the building.
4. Placing a group of skilled snipers to hunt the drone, especially the reconnaissance ones because they fly low, about six kilometres or less.
5. Jamming of and confusing of electronic communication using the ordinary water-lifting dynamo fitted with a 30-metre copper pole.
6. Jamming of and confusing of electronic communication using old equipment and keeping them 24-hour running because of their strong frequencies and it is possible using simple ideas of deception of equipment to attract the electronic waves devices similar to that used by the Yugoslav army when they used the microwave (oven) in attracting and confusing the Nato missiles fitted with electromagnetic searching

From "Al-Qaeda's 22 tips for dodging drone attacks: the list in full," *The Telegraph*, February 21, 2013. © Telegraph Media Group. All rights reserved. This content is excluded from our Creative Commons license. For more information, see <https://ocw.mit.edu/help/faq-fair-use/>.



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

Drone Use by Non-State Actors



Massachusetts Institute of Technology

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

Drone Use by Non-State Actors



© Scripps Media, 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/>.



© X Corp. 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 do drones affect crisis escalation?



Image courtesy of [Lt. Col. Leslie Pratt / U.S. Air Force](#). Source: Wikimedia Commons. This image is in the public domain.

Wargames

Simulations of decision-making events that immerse **human players** in **interactive scenarios**

Experimental Wargames

Create “control” and “treatment” games



Image courtesy of [the U.S. Air Force Museum](https://www.afm.museum/). Source: Wikimedia Commons. This image is in the public domain.



Image courtesy of the U.S. Air Force. This image is in the public domain.

Teams develop a response plan

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



0%
Launch Retaliatory Strikes

25%
Recover Wreckage

Image courtesy of the U.S. Air Force. This image is in the public domain.



100%
Launch Retaliatory Strikes

67%
Recover Wreckage/Remains

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



"Where do you bury the survivors"

"Good thing...there is no pilot being dragged along."

"avoid escalation....control the escalation ladder"

Limited desire to deter or punish

Image courtesy of the U.S. Air Force. This image is in the public domain.



"The gloves are off!"

"If they shot our service members, we retaliate."

"Getting the bodies is what we do."

Greater risk acceptance + escalation to deter future attacks and punish rival

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>.