The Motivation and Utility for Covert Action

CS-3113: PRINCIPLES OF CYBER SECURITY

BENJAMIN R. ANDERSON

Basic Concepts

Two Key Questions:

- Why is cyber important to national security?
- Why is the cyber domain inherently asymmetric?

From: *The Decision to Attack: Military and Intelligence Cyber Decision-Making* by Aaron Brantly:

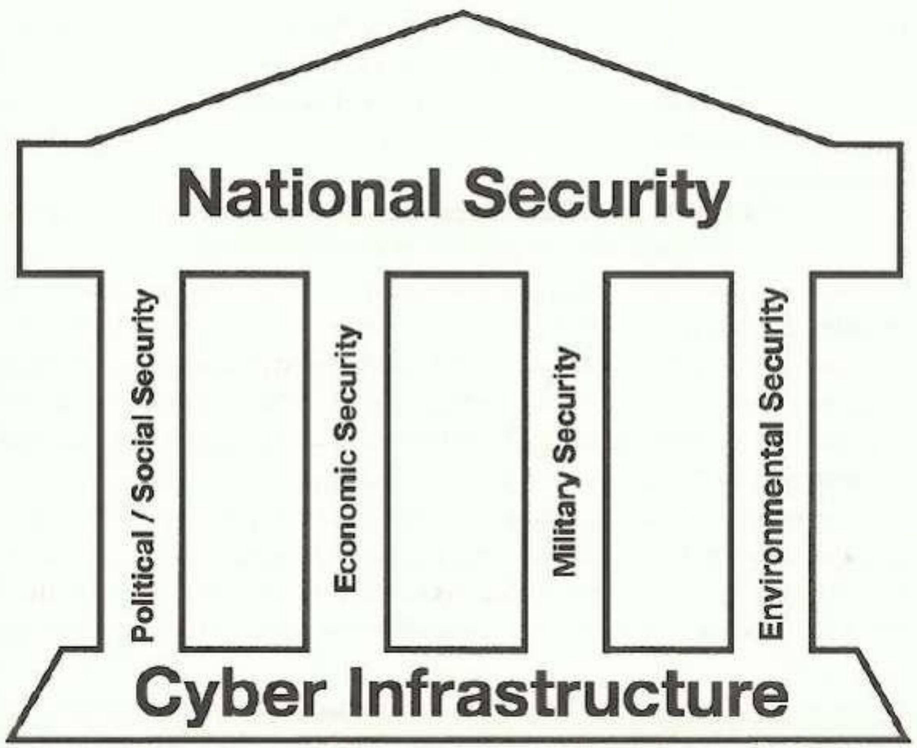
- National security is the maintenance of the survival of the state.
- Cyber is important because it forms a modern infrastructure beneath the pillars supporting national security
- Cyber infrastructure facilitates the connections of individuals, computers, systems, and, at the most basic level, ideas to one another.

The image (from The Decision to Attack) shows the 4 pillars of National Security

- In turn, those rely on the "Cyber Infrastructure" for their operation

Note: As with the previous lesson, this is an important book for this topic, and will be quoted repeatedly in this lesson as well

FIGURE 2.1 The Modern Structure of National Security



The Four Pillars: Political/Social Security

Quotes from *The Decision to Attack* (ch. 2) related to this pillar*:*

- *The realpolitik of the new era is cyberpolitik, in which the actors are no longer just states, and raw power can be countered or fortified by information power.*
  David Rothkopf, "Cyberpolitik"
- *Ideas are the lifeblood of politics and society.*
- *The control of ideas has for millennia been a strategic objective of rulers and later governments alike.*
- *The speed and quality of ideas has significantly increased in the last thirty years. Information communications technologies have facilitated an information revolution that far exceeds the previous information revolutions of the written word, the printing press, the telegraph, the wireless, and television. While the inventions of ARPANET and later TCP/IP protocols were not necessarily intended to facilitate the transference of idea, the connecting of computers has had enormous repercussions.*
- *Daniel Drezner and Henry Farrell reiterate this sentiment when they write of the evolution of a "web of influence" particularly in news and information published within the blogosphere.*
- *We take a lot these things (phones, blogs, social media, the Internet) for granted as just a part of our lives, but think for a second what the impact of these are (or can be). How can we use these to SHAPE or MOLD the "hearts and minds" of people which can then lead them to a desired action.*
- *What is certain is that the communicative capabilities developed in the last thirty years are affecting this pillar of national security.*
- *Because the cyber connection associated with the social and political pillar of national security is not entirely systemically necessary for the operation of social discourse and the dispersion of ideas, it poses a lower level of threat to national security than the other pillars of dependence. However, as cyber becomes more and more ingrained in the development of social and political issues, it will become increasingly important for national security.*

Reference: Aaron Brantly, *The Decision to Attack: Military and Intelligence Cyber Decision-Making, 2018*

Information “Blockades”

In times of civil unrest, one of the first things many government have done is to shut down the internet

- As a recent example, in March 2022, Russia announced it would block Facebook and Twitter
- https://www.theguardian.com/world/2022/mar/04/russia-completely-blocks-access-to-facebook-and-twitter

In addition, in April 2021, Myanmar shut down the internet during a military coup

- https://www.theguardian.com/world/2021/apr/02/myanmar-coup-military-expands-internet-shutdown

Locking down this information is a type of information blockade

- A traditional blockade blocks travel or shipping of supplies
- An information blockade prevents people from accessing information or data
  - This can make it difficult to obtain accurate information
  - Hinders decision making by those affected

Information “Blockades”

From the *Supplementary Human Dimension Meeting* in October 2016: *Information Blockade and Fomenting Terror through Propaganda Must Be Stopped in Turkmenistan*

- *The Internet is prohibitively expensive in Turkmenistan, its speed is deliberately slow, and most importantly, it is subject to total censorship. Access is blocked to all websites that have ever posted critical information about the Turkmen authorities, including the websites of foreign NGOs and Turkmen human rights groups in exile. Virtually all known social media, messengers, and video hosting platforms, such as YouTube, are outlawed. All Internet access is channeled through a sole government-controlled monopolist provider, allowing the authorities to access and read all user correspondence.*
- However, this scenario also shows the length a corrupt or malicious government will go to block access to information
- Specifically, Turkmenistan authorities also worked to destroy communication infrastructure
  - ***Quote***: *In particular, they are advancing an ongoing nationwide campaign to destroy satellite antennas.*
  - ***Quote***: *Countrywide removal of private satellite dishes on the pretext of “improving the look of cities” began in the spring of 2015.*
- If physical destruction is required to block the information, then they will do so

Reference: http://www.osce.org/odihr/278866?download=true

Information “Blockades”

References for the U.S. Army bring up several interesting terms and concepts

From: *FM 3-0: Operations (2008)*:

- ***Information superiority*** *is the operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary’s ability to do the same (JP 3-13)*

The manual also discusses “information actions” after a battle with Taliban forces:

- *7-4: Soldiers gathered evidence and met with the local populace to ensure they understood the situation. The provincial reconstruction team helped the Afghan governor to organize a meeting with the Margah elders to pressure them into cutting ties with the Taliban. The attached psychological operations detachment developed and disseminated sophisticated products, targeting Taliban survivors of the battle. The public affairs officer then organized a press conference on-site in Margah to allow the Afghan governor to tell the story of the security success to local and regional audiences. The joint public affairs team organized a similar event for the international media. The joint commander met with senior commanders of the Pakistani and Afghan military.*

In this case, ensuring this information was provided in various ways resulted in the Pakistani Army increasing cooperation along the border and Margah elders severed ties with the Taliban

Reference: https://army.rotc.umich.edu/public/resources/FM3-0Operations(FEB08).pdf

Information “Blockades”

More from: *FM 3-0: Operations (2008)*:

- *1-34. Joint doctrine defines the information environment as the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information (JP 3-13). The environment shaped by information includes leaders, decisionmakers, individuals, and organizations. The global community’s access and use of data, media, and knowledge systems occurs in the information shaped by the operational environment.*

Reference: https://army.rotc.umich.edu/public/resources/FM3-0Operations(FEB08).pdf

The Four Pillars: Economic Security

From the National Cyber Strategy, September 2018:

- *Protecting America's national security and promoting the prosperity of the American people are my top priorities. Ensuring the security of cyberspace is fundamental to both endeavors. Cyberspace is an integral component of all facets of American life, including our economy and defense. Yet, our private and public entities still struggle to secure their systems, and adversaries have increased the frequency and sophistication of their malicious cyber activities. America created the Internet and shared it with the world. Now, we must make sure to secure and preserve cyberspace for future generations.*
  - President Donald J. Trump

Quotes from *The Decision to Attack* (ch. 2) related to this pillar*:*

- *Cyber has come to undergird modern economics. Modern global economics, according to Thomas Friedman, has been flattened by cyber. This flattening makes it possible for multinational corporations to expand their supply chains with electronic data interchanges (EDIs) around the world, traversing physical borders using the relatively borderless expanse of cyberspace.*
- *Multinational corporations are not the only beneficiaries of this digital revolution; small businesses and individuals are now able to connect and gain access to information and products from around the world.*
  - Consider how many individuals and small businesses can access a global market through websites like Amazon, eBay, and Etsy
  - This global reach would not be possible with interconnected information systems

Reference: Aaron Brantly, *The Decision to Attack: Military and Intelligence Cyber Decision-Making, 2018*

The Four Pillars: Economic Security

More quotes from *The Decision to Attack* (ch. 2) related to this pillar*:*

- *No longer are markets isolated from one another; they directly impact one another. The disruption of supply chains by natural disasters can cause ripple effects through entire industries.*
  - This can be seen today, where disruptions from Covid-related shutdowns or military operations can impact businesses literally on the other side of the world
- *Central banks are no longer fully able to control domestic markets. Part of this is clearly due to globalization, but globalization is largely due to information communications technology.*
  - This is evident in the arbitrage markets
  - ***Abritrage***: The simultaneous purchase and sale of the same asset in different markets in order to profit from tiny differences in the asset's listed price
  - Global information systems allow someone to buy a commodity – wheat, copper, gold, oil, etc. – in the U.S. (for example) and seconds later sell it for a profit in Germany (for example)

John McCarthy and his colleagues assert global finance and economics are based on the trust of domestic and international stakeholders. This trust is predicated on the security of the information contained within the economic systems and financial networks. If this information were to be violated, modified, or destroyed, the consequences would be significant and could lead to significant drops in market capitalization or revenues, as was demonstrated in the Target Corporation data breach of 2013.

Criminal cyber exploits are not new. The scale and cascading corporate and societal ramifications of these attacks are growing in leaps in bounds. The first-order effects on a company victimized by a serious cyber exploit can be run in the billions of dollars due to pos hoc security efforts, emergency marketing, legal and regulatory costs, and stock devaluation.

Reference: Aaron Brantly, *The Decision to Attack: Military and Intelligence Cyber Decision-Making, 2018*

The Four Pillars: Economic Security

We have seen major attacks against corporations, resulting in large financial impacts

- In 2013, the “Target breach” resulted in approximately 110 million customers having their personal and financial data compromised
  - https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/
- The breach is estimated to have directly cost over $250 million dollars
- Target also reported a net loss of $2.6 billion, when it had a $350 million profit the previous quarter (for a shift of $3 billion in total)
- https://www.bankinfosecurity.com/target-breach-costs-162-million-a-7951

Overall, this had a huge impact on the entire retail industry, with many companies accelerating their adoption of secure point-of-sale terminals

From *The Decision to Attack:*

- *Corporations can presently participate in Department of Homeland Security information-sharing activities within the constraints of ensuring security for proprietary corporate assets and strategies, consumer privacy, and corporate integrity. Although it might be beneficial in the short run to avoid reporting a potential vulnerability or breach, the cascading effects across corporations and financial entities can make a problem in one company directly relevant to other corporations.*

UTSA/CIAS is heavily involved in the information sharing function

Cyber Espionage

Read the article: *Cyber Espionage Is Reaching Crisis Levels* by Kappos and Passman, December 12, 2015

- https://fortune.com/2015/12/12/cybersecruity-amsc-cyber-espionage/
- Note the scale of the problem:
  - *One study puts the cost of cybercrime at $24 billion to $120 billion in the U.S. and up to $1 trillion globally.*
  - This is from 7 years ago – and is probably much higher in 2022

Read the article: Cyber Espionage by Alexexander Gillis

- https://www.techtarget.com/searchsecurity/definition/cyber-espionage
- Note that the SolarWinds attack is attributed to the Russian hacking group Cozy Bear

The Four Pillars: Military Security

Quotes from *The Decision to Attack* (ch. 2) related to this pillar*:*

- *Military security refers to the defense of the state against potential adversaries. Douglas Dearth writes, **'advanced militaries rely more than ever in modern times upon the civil national, and increasingly international transnational infrastructures**.' This reliance on infrastructures of both a civilian and military nature create well-known vulnerabilities for the military security pillar. The increased communication and efficiency of the battlefield designed to reduce or eliminate what Clausewitz called the 'fog of war' and ever more networked military planning, logistics, human resources, acquisition, and command and control uses of ICTs and their related technologies have fed into a cycle of perpetual vulnerability development that the U.S. government has only recently started to address through the creation of U.S. Cyber Command and the various branch commands associated with cyber.*
- ***Emphasis (bold text) is my edit***
- *…the increasing reliance of modern militaries on information communications technologies has created the modern principle of command and control warfare (C2W). C2W is largely traced back to the first Gulf War, which is often referred to as the first information war. C2W is an important concept of war and has affected the way in which wars are conducted.*

There are many trade-offs with depending on civilian information and infrastructures in war fighting

- Far less expensive than deploying a military-specific infrastructure
- Utilizing existing resources is much faster than building new infrastructure
- However, this means the military is dependent on the civilian systems – and their defenses
- Backup systems can help mitigate this risk

Command and Control (C2) Warfare is a subset of Information Warfare

Reference: Aaron Brantly, *The Decision to Attack: Military and Intelligence Cyber Decision-Making, 2018*

C2Warfare

From: *What is Information Warfare?* by Col. Andrew Borden, USAF:

- ***Information Warfare:*** is any action to Deny, Exploit, Corrupt or Destroy the enemy’s information and its functions; protecting ourselves against those actions and exploiting our own military information functions
- https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Chronicles/borden.pdf

From The Free Dictionary

- ***C2 Warfare***: is an application of information operations in military operations. Also called C2W. C2W is both offensive and defensive:
  - a. C2-attack. Prevent effective C2 of adversary forces by denying information to, influencing, degrading, or destroying the adversary C2 system.
  - b. C2-protect. Maintain effective command and control of own forces by turning to friendly advantage or negating adversary efforts to deny information to, influence, degrade, or destroy the friendly C2 system.
- https://www.thefreedictionary.com/command+and+control+warfare

The First Information War

The Gulf War is often considered to be the first information war

- The U.S. forces had far more information assets than the Iraqi forces
- GPS, AWACs, and J-Stars were all used to provide an advantage to the U.S.
- In addition, Iraqi information infrastructure was specifically targeted to hinder the Iraqi forces

Two of the most powerful information weapons flew over the Gulf, AWACs (Airborne Warning and Control System) and J-Stars (Joint Surveillance and Target Attack Radar System). AWACS is a Boeing 707 capable of scanning 360 degrees in all directions to detect enemy aircraft or missiles or jam radar. J-Stars used for the first time in Gulf provided commanders on the ground a visual of enemy movements, under all weather conditions. This aircraft detects fighting vehicles, helicopters, low-speed aircraft, missile launchers, rotating antennas, ships/barges, tanks, trucks/convoys

- (PBS, Frontline)

From: Report to Congress on the Conduct of the Persian Gulf War, April 1992 by the Department of Defense

- *Attacks on mircowave relay towers, telephone exchanges, switching rooms, fiber optic nodes and bridges carrying coaxial communications cables affected Iraqi communications.*
- *Saddam Hussein's ability to transmit detailed, timely orders to his senior field commanders deteriorated rapidly. The physical destruction of the Iraqi C3 (Command and Control) capability destroyed key nodes of the air defense and C3 systems*

C3: Command, Control and Communications

The above quote also provides a good list of potential targets for cyber techniques

The Four Pillars: Military Security

Quotes from *The Decision to Attack* (ch. 2) related to this pillar*:*

- *The connectedness of modern militaries has been cited as a revolution in military affairs. Beneath this connectedness is the networked infrastructure itself. Military and civilian systems alike rely heavily on electricity. The modern electric grid, according to a 2011 MIT study, is best thought of as a system of systems increasingly vulnerable to attack.* ***The electric grid also powers sewage and water treatment facilities, supports hospitals, and provides electricity to air traffic controllers and many more aspects of critical infrastructure.*** *More importantly, each of the devices listed in the previous sentence is attached to SCADA systems and PLCs to manage their efficiency and to prevent accidents. Although many of these systems have redundancies, they are of critical importance to the military and civilian communities, and disruptions in these systems can significantly degrade or even possibly damage national security.*
- ***Again, the emphasis (bold text) is my edit***

- *Beyond military reliance on services such as electricity, the military relies on cyber to conduct virtually all aspects of modern combat. As former deputy secretary of defense William Lynn wrote in Foreign Affairs, 'Information Technology enables almost everything the military does: Logistical support and global command and control of forces, real-time provision of intelligence, and remote operations.'* ***The need for maintaining the critical infrastructures upon which military and civilian infrastructures depend is such a problem that the DoD established a new sub-unified command, United States Cyber Command (USCYBERCOM), to manage the defense of networks.***
- ***Again, the emphasis (bold text) is my edit***

Reference: Aaron Brantly, *The Decision to Attack: Military and Intelligence Cyber Decision-Making, 2018*

The Four Pillars: Military Security

Quote from *The Decision to Attack* (ch. 2)*:*

- *Penetration of DoD networks potentially compromise operational readiness of the military by introducing risks and threats to critical mission assets such as logistics, planning, C2W, and integrated communications. Incident such as Titan Rain, an attack that focused on the Defense Information Systems Agency, the Redstone Arsenal, the Army Space and strategic Defense Command, and several computer systems critical to military logistics, have the potential to severely degrade the effectiveness of military security.*

Titan Rain:

- *Titan Rain was the designation given by the federal government of the United States to a series of coordinated attacks on American computer systems since 2003; they were known to have been ongoing for at least three years. The attacks were labeled as Chinese in origin, although their precise nature, e.g., state-sponsored espionage, corporate espionage, or random hacker attacks, and their real identities – masked by proxy, zombie computer, spyware/virus infected – remain unknown. The activity known as "Titan Rain" is believed to be associated with an Advanced Persistent Threat.*
- https://en.wikipedia.org/wiki/Titan_Rain
- While this may have been the first APT campaign, there have been many since then, as we noted in previous lessons

Reference: Aaron Brantly, *The Decision to Attack: Military and Intelligence Cyber Decision-Making, 2018*

The Four Pillars: Environmental Security

Quote from *The Decision to Attack* (ch. 2)*:*

- *The final pillar supporting national security in the evolving digitized world is environmental security. Although it might seem difficult to conceptualized the environmental pillar's relationship to the cyber domain and national security, the connection is clear. The cyber domain does not control the weather, but weather can affect the cyber domain, and networked technologies are the vanguard of information on potential environmental issues from hurricanes to earthquakes. Moreover, networked technologies control many of the systems that manage chemicals, nuclear fission processes, locks, and dams, and catastrophic damage would result should their systems falter.*
- *Beyond the control of the systems that monitor wastewater, nuclear power plants, and the navigation of oil tankers, cyber is also immensely dependent on environmental security in the form of fossil fuels, renewable energy, and more, creating a symbiotic relationship. Because cyber is a man-made domain, it is heavily reliant on electricity for its connections and control mechanisms. Solar storms, large weather events, and natural disasters can all impact the flow of electricity and by extension can dramatically impact the cyber domain.*

This is a less-obvious pillar, but still important

- Consider: a cyber attack could be launched in conjunction with weather (terrestrial or solar) that impairs the target’s ability to respond
  - Solar storms can force satellites offline, or impact radio communications

Reference: Aaron Brantly, *The Decision to Attack: Military and Intelligence Cyber Decision-Making, 2018*

Asymmetric Domain

This is an EXTREMELY important concept to understand

- The reason why cyber is an asymmetric domain and what the impact of this will be discussed at several points this semester
- Also understand what a "zero-day", or 0-day, attack is

Quote from *The Decision to Attack* (ch. 2)*:*

- *Asymmetry in cyberspace has risen to the level of national policy and was included in the Department of Homeland Security's 2009 National Infrastructure Plan. The International CIIP Handbook cites the U.S. fear of being caught off guard by asymmetric threats. Network defenders often find themselves at the mercy of asymmetric attacks instigated by an individual or a small group leveraging decentralized capabilities. A system or network maintained to 100 percent perfection only requires one previously unknown vulnerability called a zero-day exploit to fall victim to a potential attack. Asymmetry in financial terms can be the millions of dollars spent maintaining a network and patching known vulnerabilities versus the lone bad actor who has identified a zero-day exploit in his garage.*

Reference: Aaron Brantly, *The Decision to Attack: Military and Intelligence Cyber Decision-Making, 2018*

Asymmetric Domain

Quotes from *The Decision to Attack* (ch. 2)*:*

- *…positive and negative types of asymmetry. Positive asymmetries are strategic/tactical advantages one country has over another. Negative asymmetries are advantages that a country's opponent has over it.*
- *Positive asymmetry in cyber refers to cyber technologies that provide an advantage over potential opponents; more specifically, such asymmetry refers to the potential vulnerabilities present with an opponent's systems. The manipulation of zero-day vulnerabilities found within the PLCs that controlled the Iranian uranium enrichment centrifuges would be consistent with an asymmetric exploit. Instead of the centrifuges being hit with a bomb, they were hit with code at a weak point.*
- *Negative asymmetry constitutes a weakness in systems that an opponent is likely to target. The Titan Rain exploitation of confidential information on U.S. defense networks would be consistent with this type of vulnerability.*
- *At its most basic, a positive asymmetry is an offensive advantage, whereas a negative asymmetry is a defensive [dis]advantage.*

Note that Brantly discusses both positive and negative types of asymmetry

A good example of asymmetry is when Colonial Pipeline – a multi-billion dollar company – was taken down by a small (albeit well-organized) criminal group

Reference: Aaron Brantly, *The Decision to Attack: Military and Intelligence Cyber Decision-Making, 2018*

Asymmetric Domain

Quotes from *The Decision to Attack* (ch. 2)*:*

- *A November 2010 Chatham house report summarized best the problem of asymmetry in cyber: 'Cyber warfare could be the archetypal illustration of 'asymmetric warfare' -- a struggle in which one opponent might be weak in conventional terms but is clever and agile, while the other is strong but complacent and inflexible.*
- *… asymmetry affects how decisions are made within the cyber domain. A decision-maker would have a hard time deriving a benefit from attacking a country with few to no cyber assets via cyber means. If a target's dependence on cyberspace is limited, the effect of the attack would be minimal; therefore, any resultant utility to be gained would also be minimal.*
- *Conversely, it is logical for a state with few cyber assets to engage in hostile cyber action against a highly cyber dependent state, because it need not worry about an in-kind retaliation, and it can have a much larger effect on the state with high levels of cyber dependence.*

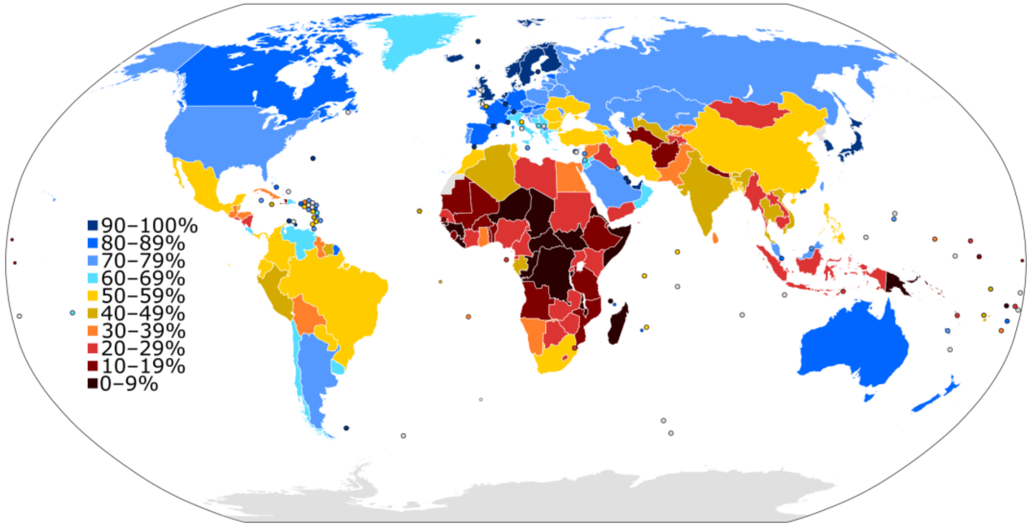


Image from Wikipedia: https://en.wikipedia.org/wiki/List_of_countries_by_number_of_Internet_users

Reference: Aaron Brantly, *The Decision to Attack: Military and Intelligence Cyber Decision-Making, 2018*

Covert Action

Reasons to conduct covert actions:

- *Offensive Cyber Operations (OCOs) by state actors are a new typology of covert action.*
- *Covert actions are as old as political man. The subversive manipulation of others is nothing new… People and nations have always sought the use of shadowy means to influence situations and events.*
- *Covert action is, and has always been, a tool aimed at achieving positive utility for political leaders.*
- Quotes from *The Decision to Attack* (ch. 3)

Of course, the most important reason to conduct covert actions:

- You just don't want to get caught because there are consequences for doing the actions
- Of course, an attack being detected is different than having the attack attributed to you
- This is why threat intelligence and identifying attackers (i.e. – what APT is responsible) is critical

Reference: Aaron Brantly, *The Decision to Attack: Military and Intelligence Cyber Decision-Making, 2018*

Covert Action

The Decision to Attack has an interesting perspective on the various "levels" that exist inside covert actions

As you can see, it includes more than just cyber operations – and scales all the way to use of WMD

One covert activity from the Cold War, was the use of a Trojan Horse to cause a major explosion in a Soviet gas pipeline in 1982

- https://en.wikipedia.org/wiki/At_the_Abyss

Stuxnet was also used to attack the Iranian nuclear program, and resulted in hundreds of centrifuges not operating correctly and being destroyed

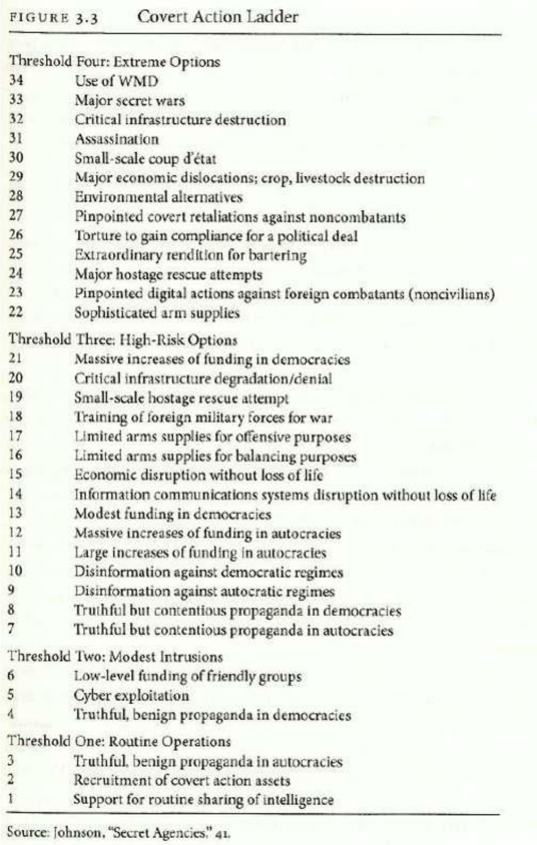


FIGURE 3.3 Covert Action Ladder

Threshold Four: Extreme Options	
34	Use of WMD
33	Major secret wars
32	Critical infrastructure destruction
31	Assassination
30	Small-scale coup d'état
29	Major economic dislocations; crop, livestock destruction
28	Environmental alternatives
27	Pinpointed covert retaliations against noncombatants
26	Torture to gain compliance for a political deal
25	Extraordinary rendition for bartering
24	Major hostage rescue attempts
23	Pinpointed digital actions against foreign combatants (noncivilians)
22	Sophisticated arm supplies
Threshold Three: High-Risk Options	
21	Massive increases of funding in democracies
20	Critical infrastructure degradation/denial
19	Small-scale hostage rescue attempt
18	Training of foreign military forces for war
17	Limited arms supplies for offensive purposes
16	Limited arms supplies for balancing purposes
15	Economic disruption without loss of life
14	Information communications systems disruption without loss of life
13	Modest funding in democracies
12	Massive increases of funding in autocracies
11	Large increases of funding in autocracies
10	Disinformation against democratic regimes
9	Disinformation against autocratic regimes
8	Truthful but contentious propaganda in democracies
7	Truthful but contentious propaganda in autocracies
Threshold Two: Modest Intrusions	
6	Low-level funding of friendly groups
5	Cyber exploitation
4	Truthful, benign propaganda in democracies
Threshold One: Routine Operations	
3	Truthful, benign propaganda in autocracies
2	Recruitment of covert action assets
1	Support for routine sharing of intelligence

Source: Johnson, "Secret Agencies," 41.

Image from: Aaron Brantly, *The Decision to Attack: Military and Intelligence Cyber Decision-Making, 2018*