Cyber Decision Making

CS-3113: PRINCIPLES OF CYBER SECURITY

BENJAMIN R. ANDERSON

The Cyber Domain

This is going to examine “cyber” from the perspective of national security and military operations

This is not going to discuss decisions made for a return on investment (ROI) for a company

Instead this will look at the implications of our dependency on cyber systems for our nation and society

The importance of this warfighting domain was illustrated with the formation of the U.S. Cyber Command in 2010

According to the Cyber Command Mission and Vision webpage:

- The Commander, USCYBERCOM, Gen. Paul M. Nakasone, has the mission to:
  - Direct, Synchronize, and Coordinate Cyberspace Planning and Operations - to Defend and Advance National Interests - in Collaboration with Domestic and International Partners
- https://www.cybercom.mil/About/Mission-and-Vision/

The Cyber Domain

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

Is it really necessary to create an entirely new decision-making model for the cyber domain?

What differentiates cyberspace from [the more conventional domains of military and intelligence] are four primary attributes:

- *The cyber domain is man-made*
- *Military capabilities across the other domains are managed through the cyber domain*
- *Military and civilian aspects of the cyber domain are often intertwined and difficult to differentiate.*
- *Attribution within cyberspace is often difficult to assign.*

These attributes combine to create a novel domain of interaction necessitating a nuanced and rigorous decision-making model predicated on existing models for conventional state behavior.

Cyberspace is often traced to two creators, Vinton Cerf and Bob Kahn… Although these two pioneers in networking and TCP/IP … Established the protocols of the modern information renaissance, the roots of cyberspace are more accurately placed with Donald Davies, a researcher with Britain's National Physical laboratory, and Paul Baran, a Polish émigré and researcher at RAND.

The process of development from the early computing machines to something now recognizable as the modern Internet was a combined military and civilian effort fraught with bureaucracy, passion, and unexpected benefits along the way.

What defines the Internet is not its intrinsic physical characteristics in the way that land is defined by its terrestrial nature, sea by vast amounts of water, and air by its fluid properties. Instead, the Internet is defined by the linking of computers and the creation of a virtual space that would evolve into a popular science fiction term coined in the 1980s as "Cyberspace".

Vinton Cerf

Vinton “Vint” Cerf is considered one of the “fathers of the Internet”

He and Bob Kahn invented TCP/IP (among other achievements)

Vint Cerf was a manager for the United States' Defense Advanced Research Projects Agency (DARPA) funding various groups to develop TCP/IP technology

When the Internet began to transition to a commercial opportunity during the late 1980s, Cerf moved to a civilian role at MCI

- He helped create the first commercial email system (MCI Mail) connected to the Internet

He has many notable awards including:

- National Medal of Technology
- The Turing Award
- The Presidential Medal of Freedom
- And others

From: https://en.wikipedia.org/wiki/Vint_Cerf

Bob Kahn

Bob Khan is the co-inventor (with Vint Cerf) of the Transmission Control Protocol (TCP) and the Internet Protocol (IP) creating the TCP/IP protocol stack

- While there were other protocols developed for the Internet, they lost out to TCP/IP
- Today, TCP/IP is the fundamental communication protocol (family of protocols) at the heart of the Internet

While at the Directory of DARPA's Information Processing Techniques Office (IPTO) Bob Khan started the U.S. government's Strategic Computing Initiative – the largest computer R&D program funded by the U.S. government

He founded a non-profit called the Corporation for National Research Initiatives (CNRI) in 1986

His awards include:

- The National Medal of Technology
- Inducted into the National Inventors Hall of Fame
- Queen Elizabeth Price for Engineering

https://en.wikipedia.org/wiki/Bob_Kahn

The TCP Protocol

This is a review of the TCP/IP protocol suite

You are not responsible for the specific details of the protocol - but you will be responsible for the general concepts

The TCP Header image is from:

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

TCP Header

Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Source port																Destination port															
4	32	Sequence number																															
8	64	Acknowledgment number (if ACK set)																															
12	96	Data offset				Reserved 0 0 0			NS	CWR	ECE	URG	ACK	PSH	RST	SYN	FIN	Window Size															
16	128	Checksum																Urgent pointer (if URG set)															
20	160	Options (if *data offset* > 5. Padded at the end with "0" bytes if necessary.)																															
...	...	...																															

Source port (16 bits)

Identifies the sending port

Destination port (16 bits)

Identifies the receiving port

Sequence number (32 bits)

Has a dual role:

- If the SYN flag is set (1), then this is the initial sequence number. The sequence number of the actual first data byte and the acknowledged number in the corresponding ACK are then this sequence number plus 1.
- If the SYN flag is clear (0), then this is the accumulated sequence number of the first data byte of this segment for the current session.

Acknowledgment number (32 bits)

If the ACK flag is set then the value of this field is the next sequence number that the sender is expecting. This acknowledges receipt of all prior bytes (if any). The first ACK sent by each end acknowledges the other end's initial sequence number itself, but no data.

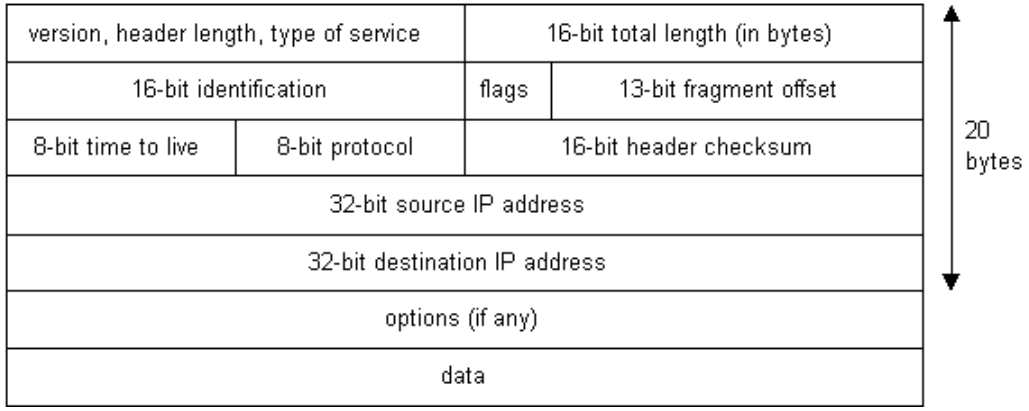
Data offset (4 bits)

Specifies the size of the TCP header in 32-bit words. The minimum size header is 5 words and the maximum is 15 words thus giving the minimum size of 20 bytes and maximum of 60 bytes, allowing for up to 40 bytes of options in the header. This field gets its name from the fact that it is also the offset from the start of the TCP segment to the actual data.

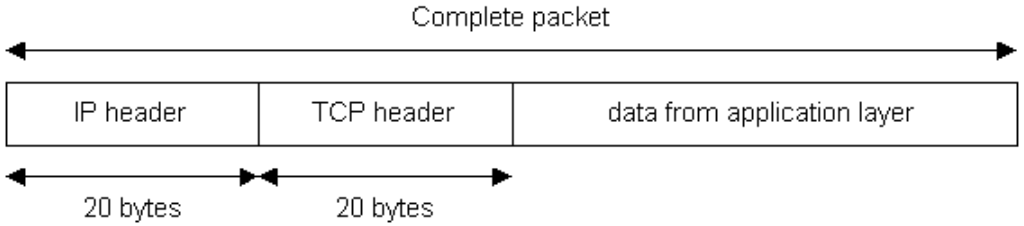
Reserved (3 bits)

For future use and should be set to zero

The IP Protocol



We hear the term "packet" used a lot when talking about information being passed along the Internet. A packet consists of the following parts:



Images from: http://www.theshulers.com/whitepapers/internet_whitepaper/

The TCP/IP Suite of Protocols

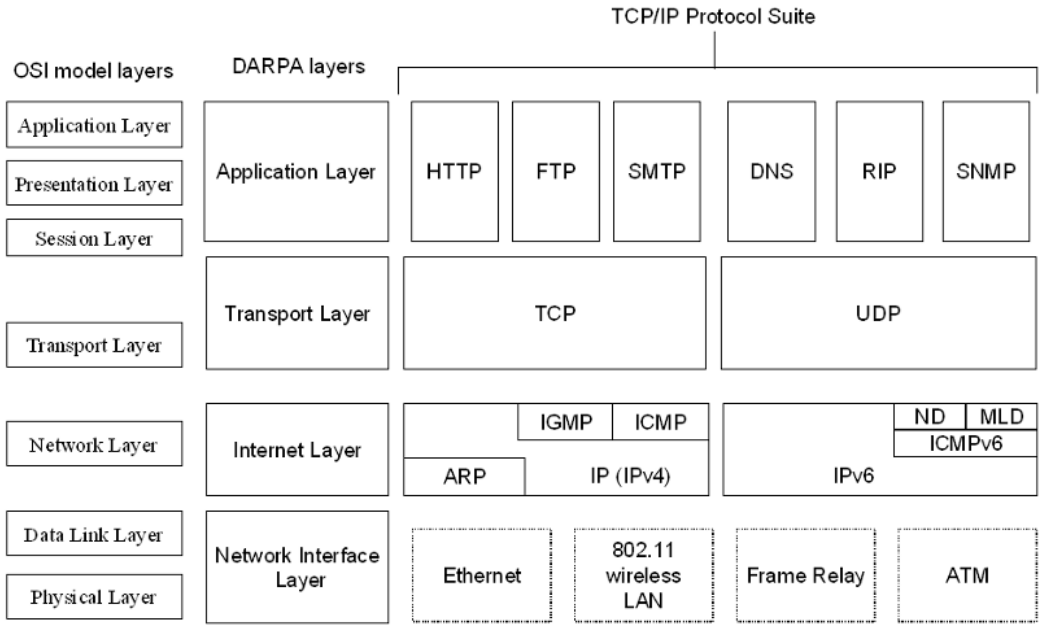
TCP and IP are just two of the protocols in the complete Protocol Suite.

The concept of layering in networks protocols is often first explained using the 7-layer OSI model.

The DARPA layers were the precursor to the TCP/IP Protocol Suite.

The diagram is a comparison of the three models, and is from:

- https://technet.microsoft.com/en-us/library/bb726993.aspx



Topology and Data Flow in TCP/IP

The protocols have to work together to make communication possible

While it "appears" to users that they are directly connected to the system they are communicating with, this is not the case

- In reality there are a number of systems between the two
- They all have to work together to ensure that packets are routed from source to destination correctly.

Notice in the diagrams to the right, that the application layers world view only contains the other application layer

The other layers abstract out the other information

The Transport layer view is simply between the two hosts - the actual routing through the Internet is the concern of the lower layers.

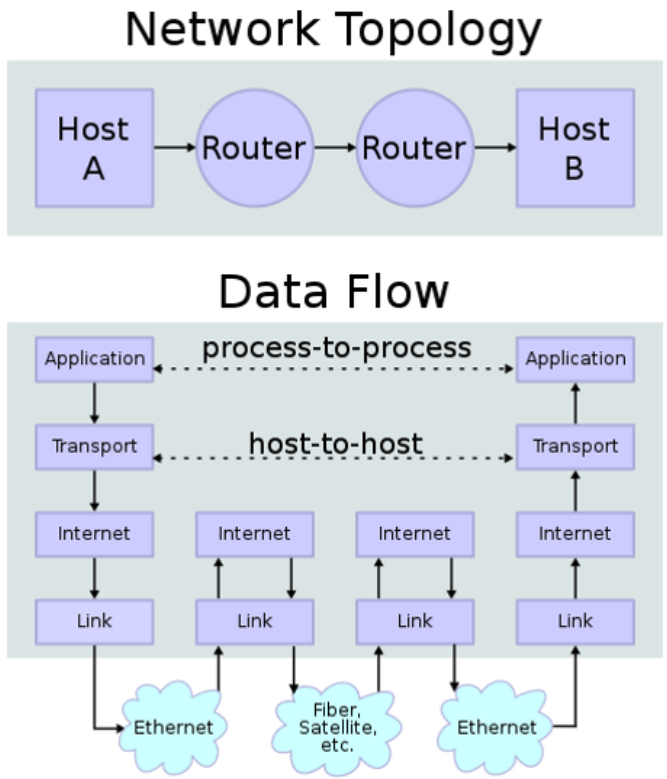


Image from: https://en.wikipedia.org/wiki/Internet_protocol_suite

Encapsulation in TCP/IP

Encapsulation is an important concept in how how the TCP/IP and OSI model work

At any layer, the layer only is concerned with what it needs to do to either pass the developing packet to the next layer below it or pass it to the next layer above

- This basically means that it will add a header (and possibly a trailer) which will then be stripped off at the destination
- These headers and trailers are used to describe what to do with the packet at the other end
- For example, the system can determine: is this a TCP or a UDP packet?
  - It can then send it to the appropriate code to handle it

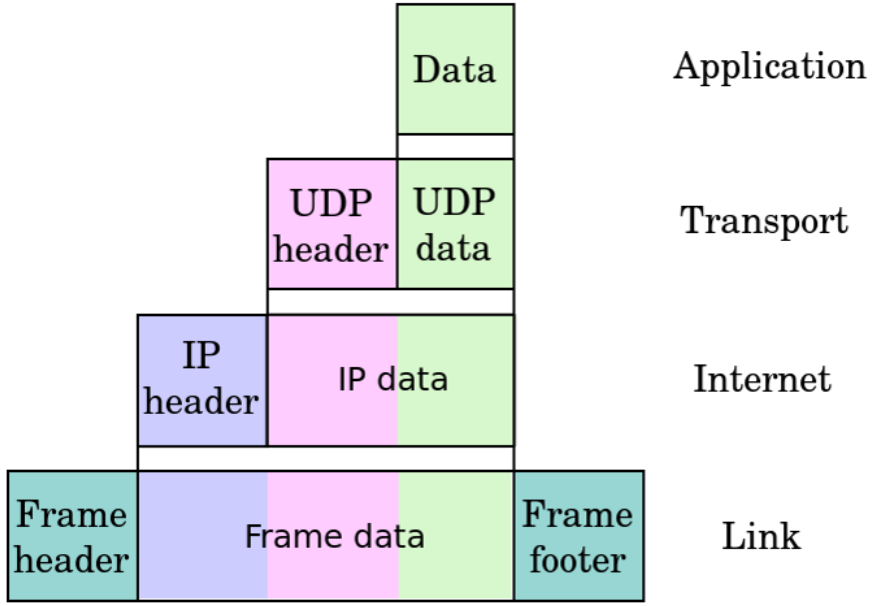


Image from: https://en.wikipedia.org/wiki/Internet_protocol_suite

Well-known Port Numbers

At a destination host, the way that the system knows what process or application should handle the data is through the use of "port numbers“

- There are 64K port numbers (0 - 65,535)

The source host has to know what port number to insert in the packet so that the destination host knows what to do it

There are a number of common applications that utilize some well-known ports.

The table lists some of the common ports for various services

Internet Service	Port Number
FTP	20/21
SSH	22
Telnet	23
Domain Name Service (DNS)	53
HTTP	80
HTTPS	443
Minecraft	25565

Important Point to Remember

The TCP/IP Protocol Suite was a tremendous step in the evolution of networking since it provided an efficient mechanism to conduct packet switching in an often unreliable networking environment

- It is still in use almost 50 years later
- Additional protocols have been added (such as HTTP and HTTPS)
- IP itself has had new versions (such as IPv6)
- However, the basic design remains the same

When TCP/IP was created, security was not a primary consideration

- The original design of TCP/IP did not emphasize security
- The goal was efficient and reliable transmission of packets/messages
- After all, in 1985 a transmission speed of 50Kbps was considered ***fast!***
- The original purpose TCP/IP was created for was to allow researchers to communicate and transmit information/messages between themselves

What Is Cyberspace

There are many definitions, opinions, and statements about what cyberspace is

We will use the definition by Dan Kuehl, provided by Aaron Brantly in his book: *The Decision to Attack: Military and Intelligence Cyber Decision-Making*

- *Cyberspace is important and dramatically affects our lives in many ways, but what is cyber? Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz acknowledge more than nineteen different definitions of cyberspace, giving a moving target, difficult to pin down. This book has settled on Dan Kuehl's definition as the most encompassing of various agencies and author positions. Kuehl defines cyberspace as follows:*
  A global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies.

Note: This is an important book for this topic, and will be quoted repeatedly in this lesson

Critical Infrastructures

Critical infrastructure is another important term

- Like cyberspace, there are many different lists and definitions

The Cybersecurity and Infrastructure Security Agency (CISA) which is a department of DHS provides a list of the critical infrastructure sectors – from that webpage:

- *There are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof. Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience advances a national policy to strengthen and maintain secure, functioning, and resilient critical infrastructure. This directive supersedes Homeland Security Presidential Directive 7.*
- https://www.cisa.gov/critical-infrastructure-sectors

PPD-21 identifies 16 critical infrastructure sectors:

- Chemical Sector
- Commercial Facilities Sector
- Communications Sector
- Critical Manufacturing Sector
- Dams Sector
- Defense Industrial Base Sector
- Emergency Services Sector
- Energy Sector
- Financial Services Sector
- Food and Agriculture Sector
- Government Facilities Sector
- Healthcare and Public Health Sector
- Information Technology Sector
- Nuclear Reactors, Materials, and Waste Sector
- Transportation Systems Sector
- Water and Wastewater Systems Sector

Cyber-Controlled Instruments Pertinent to National Security

This list, from Aaron Brantly's book, are some examples of systems that can be impact by operations in cyberspace:

- Satellites
- Radio transmissions
- Drones
- GPS
- Heads-up displays for pilots
- Most modern avionics
- Communications technologies
- Logistical coordination systems
- Intellipedia
- Smart projectiles
- Electric grids
- Power plants
- Banks
- Stock Exchanges

All of these use cyber in their operations - either directly or for monitoring or control

Note: This list above does not distinguish between public and private cyber domains

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

Understanding the Decisions of State

More from Aaron Brantly:

- *Because the cyber domain is unique from other more conventional domains and is of critical importance to the functioning of the national security of modern states, there is a need for a logical conceptualization of state-rational decision processes to influence the policy actions of other states using cyber weapon systems. The power of states in cyberspace and consequences of actions in a networked system of systems environment are not straightforward.*

  There is a larger degree of consensus on the ability to leverage cyberspace tactics, techniques, and procedures (TTPs) for soft power gain. The U.S. State Department frequently makes reference to cyber and implicitly soft power and has used its influence to provide tools or maintain services for the communication and organization of popular uprisings. Various organizations have identified corresponding online trends associated with large-scale social and political movements that indicate a role for cyberspace in influencing public discourse. Hard power, unlike soft power, necessitates approval by the executive of a state. Whereas applications of soft power are institutionalized and part of an ongoing policy process, decisions to use hard power are not continuous policy processes, but rather moments of extreme contention requiring decision choke points indicating a substantive benefit associated with a specific deliberate action.

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

Hard and Soft Power

From Aaron Brantly:

- *Hard power and soft power exist on a spectrum. Joseph Nye defines hard power on one end of the spectrum as the ability to command, threaten, or sanction. More simply, he defines the difference between hard and soft power as the difference between "push" and "pull". The decision to use the stick rather than the carrot is typically an executive one requiring a rational decision that weighs the utility of action versus inaction or actions that do not make use of the constitutive aspects of hard power.*

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

Defining Offensive Cyber Operations

Building the argument for a decision-making model predicated on the use of hard power has inadvertently created a logical shortcut around an area of major concern for many cyber theorists. Often scholars discussing the use of cyberspace in the context of national security offense and defense get stuck when it comes time to defining what constitutes an offensive cyber operation. U.S. Cyber Command, a sub-unified command under U.S. Strategic Command, issued a combined lexicon document that facilitates consistent terminology and definitions across the Department of Defense. Although the specific terms are not consistent internationally, it is beneficial to use this combined lexicon as a basis for defining terms in the cyber domain.

- Aaron Brantly

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

Cyberwar

Watch: Cyberwar – a TEDxStandord talk by Amy Zegart

- https://www.youtube.com/watch?v=JSWPoeBLFyQ
- Amy Zegart is a professor at Stanford University and has been a member of the National Security Council (under President Clinton) and specializes in the national security, technology, and intelligence areas

From this talk, there were 5 key ways cyberwar is different from conventional war:

- Most powerful=most vulnerable
- The government can't go it alone
- Attack surface is huge
- Victims often don't know they are victims
- Warning and Decision

Definitions

Cyberspace: A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

Cyberspace Operations: CO: All activities conducted in and through cyberspace in support of the military, intelligence, and business operations of the Department.

Cyber Warfare: CW: Creation of effects in and through cyberspace in support of a combatant commander's military objectives, to ensure friendly forces freedom of action in cyberspace while denying adversaries these same freedoms. Composed of cyber attack (CA), cyber defense (CD), and cyber exploitation (CE).

Cyber Attack: CA: Cyber warfare actions intended to deny or manipulate information and/or infrastructure in cyberspace. Cyber attack is considered a form of fires.

Cyber Defense: CD: Cyber warfare actions to protect, monitor, detect, analyze, and respond to any uses of cyberspace that deny friendly combat capability and unauthorized activity within the DOD global information grid (GIG).

Cyber Exploitation: CE: Cyber warfare enabling operations and intelligence collection activities to search for, collect data from, identify, and locate targets in cyberspace for threat recognition, targeting, planning, and conduct of future operations.

Cyber Warfare Capability: CWC: A capability (e.g., device, computer program, or technique), including any combination of software, firmware, and hardware designed to create an effect in cyberspace, but that has not been weaponized. Not all cyber capabilities are weapons or potential weapons.

Cyber Weapon Systems: CWS: A combination of one or more weaponized offensive cyber capabilities with all related equipment, materials, services personnel, and means of delivery and deployment (if applicable) required for self-sufficiency.

All of these definitions are from *The Decision to Attack: Military and Intelligence Cyber Decision-Making* by Aaron Brantly

Cyber attack, defense, and exploitation are key terms that you should be familiar with

Influencing National Policy

This is getting into key areas of using cyberspace in national security areas

There are many ways this can be done

- For example, in 2010, Stuxnet was a direct attack on Iran's nuclear program
  - https://en.wikipedia.org/wiki/Stuxnet
- In 2015, there was an attack on the Ukrainian power grid
  - https://en.wikipedia.org/wiki/Ukraine_power_grid_hack
- Indirectly, social media can be used to influence people and policies to achieve objectives
  - Consider terms like "fake news" or "misinformation"
  - Even slight changes to algorithms, purchased ads, or policies can have a huge effect on information that people are provided with
    - https://en.wikipedia.org/wiki/Social_media_use_in_politics

Influencing National Policy

More from Aaron Brantly:

- *The use of means other than nonhostile diplomacy to influence the policy decisions of other states requires a decision to be made. This decision is dependent on a multitude of considerations. However, the decision itself is broadly constrained by three generic qualifiers:*
  (1)What is the utility of action?
  (2)What is the uncertainty that such an action will not work?
  (3)What risk is associated with this type of action?
  These constraints weigh heavily on the decision to forgo nonhostile methods of political action in favor of actions likely to be construed as hostile.

Consider: How does this relate to Cyber actions?

Consider: How does it relate to influencing politics?

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

Influencing National Policy

More from Aaron Brantly:

- *The policy process can be broken down into three broad categorizations:*
  (1) nonhostile overt bargaining,
  (2) hostile overt bargaining, and
  (3) hostile covert action.

  Most of the international relations literature focuses on the first two. It is, however, the third type of action, which has gone largely unnoticed in modern theorizing, that has the largest independent political value and is most applicable to the cyber domain.

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

Influencing National Policy

More from Aaron Brantly:

- *Sacrifice is required in overt nonhostile bargaining to reach a mutual decision.*
  One or both sides must lose to achieve a political goal in overt hostile bargaining.
  Yet covert political action offers a third path, one that influences the intended target to achieve a political result, altering policy positions without knowledge and explicit consent. As in chess, it is best to have the opponent think they are making their best move, when in reality they are positioning themselves in checkmate. The broad tenets of the decision to use any of the three types of action are the same. A state engaging in any political action will attempt to define its utility for each type of action, and from there it will choose the best path to take.

Decision-makers are in essence weighing the options of these three broad paths to influence the political environment. The ability to decide which path to take is based on a fully rational understanding of the value of each of the paths. Each of these options contains risk and uncertainty over whether it will achieve the desired change and create the political utility desired. It is by deconstructing this complex nested decision process that states are able to understand whether it is better to maintain normal international relations through diplomatic action or engage in alternative means to shift the policy preferences of others. The emphasis in the [textbook] is on the two paths diverging from the diplomatic. These two paths are closely intertwined and often overlap either intentionally or accidentally. Specifically, decision-makers are presented with a new set of tools, which can influence the decision to use one or both of these paths. These tools fall within the new and man-made cyber domain but have very real and tangible aspects felt in the physical world.

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

Offensive Cyber Operations

More from Aaron Brantly:

- *[The textbook] particularly contends with the utility of one type of covert action – cyber attacks (CAs) in the form of offensive cyber operations (OCOs). Beyond merely the consideration of the covert versus overt nature of options available to states, the cyber domain offers up a unique set of challenges…for the development of utility in a decision-making process…*

  From a traditional conflict decision-making perspective… A state that is better endowed with resources than its potential adversary has a higher probability of being successful in a conflict. The farther a state attempts to extend its power and resource capabilities out from its center of gravity, the more its relative power begins to decline.

  For the cyber domain it is inappropriate to use…scores of monotonic declines in power over distance. In addition to these two inappropriate attributes, cyber adds complexity of anonymity and attribution.

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

Computer Network Operations

Cyberwar is a very real threat, and can cause widespread problems

- Consider what would happen if Google Maps was taken offline – could you find your way without looking it up online?
- The issues at Facebook when they had a DNS problem, could be done maliciously (instead of by accident) preventing a company from conducting business operations
- "Cyber" is everywhere – from our phones, to our vehicles, to our smart homes

The U.S. Government and the National Security Agency take this very seriously and is continuously hiring for computer science professionals (and other specialties) who are skilled in computer network operations and other fields

- https://www.nsa.gov/careers/career_fields/

The Cyber Operations specialty at the NSA can include:

- ***Computer Network Attack (CNA):*** Includes actions taken via computer networks to disrupt, deny, degrade, or destroy the information within computers and computer networks and/or the computers/networks themselves.
- ***Computer Network Defense (CND)***: Includes actions taken via computer networks to protect, monitor, analyze, detect, and respond to network attacks, intrusions, disruptions, or other unauthorized actions that would compromise or cripple defense information systems and networks
- ***Computer Network Exploitation (CNE)***: Includes enabling actions and intelligence collection via computer networks that exploit data gathered from target or enemy information systems or networks

DoD Cyber Strategy
Joint Publication (JP) 3-12 Cyberspace Operations

DODIN: The Department of Defense information network (DODIN)

JP 3-12 defines the following Cyberspace Operations Core Activities:

Cyberspace Missions: All actions in cyberspace that are not cyberspace-enabled activities are taken as part of one of three cyberspace missions: offensive cyberspace operations (OCO), defensive cyberspace operations (DCO), or DODIN operations. These three mission types comprehensively cover the activities of the cyberspace forces. The successful execution of CO requires integration and synchronization of these missions.

DODIN Operations: The DODIN operations mission includes operational actions taken to secure, configure, operate, extend, maintain, and sustain DOD cyberspace and to create and preserve the confidentiality, availability, and integrity of the DODIN.

DCO: DCO missions are executed to defend the DODIN, or other cyberspace DOD cyberspace forces have been ordered to defend, from active threats in cyberspace.

OCO: OCO are CO missions intended to project power in and through foreign cyberspace through actions taken in

Another key definition:

Department of Defense (DOD) Cyberspace: The Department of Defense information network (DODIN) is the set of information capabilities and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel, whether interconnected or stand-alone, including owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and national security systems.

Reference: Joint Publication 3-12 Cyberspace Operations, 8 June 2018

DoD Cyber Strategy
Field Manual (FM) 3-38

FM 3-38 list the following Functions of Cyberspace Operations as it relates to physical operations

- 3-1. Army forces coordinate and integrate CO through CEMA [***Cyber Electromagnetic Activities***]. They do this to gain and maintain freedom of action in cyberspace and as required to achieve periods of cyberspace superiority.

  3-2. Cyberspace superiority is the degree of dominance in cyberspace by one force that permits the secure, reliable conduct of operations by that force, and its related land, air, maritime, and space forces at a given time and place without prohibitive interference by an adversary (JP 1-02). Such interference is possible because large portions of cyberspace are not under the control of friendly forces. Cyberspace superiority establishes conditions describing friendly force freedom of action while denying this same freedom of action to enemy and adversary actors. Ultimately, Army forces conduct CO to create and achieve effects in support of the commander's objectives and desired end state.

  3-3. CO are categorized into three functions including offensive cyberspace operations (OCO), defensive cyberspace operations (DCO), and Department of Defense information network operations. These functions are described in joint doctrine as missions in cyberspace that require specific actions in cyberspace (see joint doctrine for CO). Figure 3-1 on page 3-2 depicts the three interdependent functions of CO.

Reference: FM 3-38 Cyber Electromagnetic Activities, February 2014, Headquarters, Department of the Army

DoD Cyber Strategy (2015) - Deterrence

Deterrence is partially a function of perception. It works by convincing a potential adversary that it will suffer unacceptable costs if it conducts an attack on the United States, and by decreasing the likelihood that a potential adversary's attack will succeed.

The United States must be able to declare or display effective response capabilities to deter an adversary from initiating an attack; develop effective defensive capabilities to deny a potential attack from succeeding; and strengthen the overall resilience of U.S. systems to withstand a potential attack if it penetrates the United States' defenses

In addition, the United States requires strong intelligence, forensics, and indications and warning capabilities to reduce anonymity in cyberspace and increase confidence in attribution.

The United States has been clear that it will respond to a cyberattack on U.S. interests through its defense capabilities

The United States has articulated this declaratory policy in the 2011 United States International Strategy for Cyberspace, in the Department of Defense Cyberspace Policy Report to Congress of 2011, and through public statements by the President and the Secretary of Defense

The United States will continue to respond to cyberattacks against U.S. interests at a time, in a manner, and in a place of our choosing, using appropriate instruments of U.S. power and in accordance with applicable law.

- Emphasis (bold text) is my edit

Reference: The DoD Cyber Strategy, Pages 11-12, The Department of Defense

DoD Cyber Strategy (2015) - Attribution

Attribution is a fundamental part of an effective cyber deterrence strategy as anonymity enables malicious cyber activity by state and non-state groups. On matters of intelligence, attribution, and warning, DoD and the intelligence community have invested significantly in all source collection, analysis, and dissemination capabilities, all of which reduce the anonymity of state and non-state actor activity in cyberspace. Intelligence and attribution capabilities help to unmask an actor's cyber persona, identify the attack's point of origin, and determine tactics, techniques, and procedures. Attribution enables the Defense Department or other agencies to conduct response and denial operations against an incoming cyberattack.

Public and private attribution can play a significant role in dissuading cyber actors from conducting attacks in the first place. The Defense Department will continue to collaborate closely with the private sector and other agencies of the U.S. government to strengthen attribution. This work will be especially important for deterrence as activist groups, criminal organizations, and other actors acquire advanced cyber capabilities over time.

Reference: The DoD Cyber Strategy, Pages 11-12, The Department of Defense

Cyber Strategy

There have been numerous Cyber Strategies developed since 2015

- There is the DoD Cyber Strategy from 2018
- There is also a National Cyber Strategy from 2018
- In fact, there are updated cyber strategies, Executive Orders, and other documents published almost every year
  - There is even a guide to help find those resources
  - https://dodcio.defense.gov/Portals/0/Documents/Library/CSResourceReferenceGuide.pdf

The National Cyber Strategy also stresses the importance of attribution, with a section devoted to:

- ***Attribute and Deter Unacceptable Behavior in Cyberspace***
- After all, if you can't figure out who conducted a cyberattack, it is very hard to respond in a meaningful way

Cyber Espionage

There are many references to ***Cyber Espionage***, but few attempts to define what it is

The National Cyber Strategy of 2018 even uses the term “cyber-enabled economic espionage”

- It sounds very specific, but it leaves a lot of room for interpretation
- Ex. If a foreign agent uses Google Maps to find a facility and go dumpster diving, is that cyber-enabled economic espionage?

Cyber Espionage – Definitions

Here are some definitions provided by Dimitar Kostadinov from the Infosec Institute:

- *The science of covertly capturing e-mail traffic, text messages, other electronic communications, and corporate data for the purpose of gathering national-security or commercial intelligence (Hersh, 2010).*
- *The practice of spying or obtaining secrets from rivals or enemies for military, political, or business advantage. Advances in IT and the proliferation of tiny, embedded storage devices have added considerably to espionage dangers (Janczewski& Colarik, 2008, p. 25)*
- *Cyber espionage, also known as "cyber exploitation, can be understood as "the use of actions and operations—perhaps over an extended period of time—to obtain information that would otherwise be kept confidential and is resident on or transiting through an adversary's computer systems or networks (Lin, 2010, p.63).*
- *The Tallinn Manual on the International Law Applicable to Cyber Warfare, non-binding opinion of an independent group of experts on the legal aspects of cyber threats provides a narrow definition of cyber espionage:*

  Any act undertaken clandestinely or under false pretenses that uses cyber capabilities to gather (or attempt to gather) information with the intention of communicating it to the opposing party to the conflict" (Tallinn Manual on the International Law Applicable to Cyber Warfare, 2012, p. 159)
- *"Clandestinely" means that the perpetrator attempts to hide his identity, while the "under false pretenses" phrase signifies that his intention is to present himself as a person entitled to certain rights and authorization to access the targeted information.*

Reference: The Infosec Institute, https://resources.infosecinstitute.com/topic/cyber-exploitation/

Computer Network Exploitation

NIST defines computer network exploitation (CNE) as:

- *Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary information systems or networks.*

This definition also has a note:

- *Note: Within the Department of Defense (DoD), term was approved for deletion from JP 1-02 (DoD Dictionary). Original source of term was JP 1-02 (DoD Dictionary). The military no longer uses this term to describe these operations, but it is still used outside of military operations.*

DoD might use different terms now but, essentially, CNE is the U.S. government term for cyberespionage (it includes “intelligence collection”)

There are many groups that make up the U.S. government CNE team

- The most obvious is Cyber Command, but there are other – more specialized – groups as well
- The Shadow Brokers revealed multiple zero days that were attributed to the “Equation Group” a team within the NSA’s Tailored Access Operations (TAO) group

Videos on Cyber Attacks

The Solarwinds attack:

- CNBC, *The U.S. government is under the 'hack of a decade' after massive cyberattack grows*
- https://www.youtube.com/watch?v=B4P09aicB-4

Solarwinds was critical enough that SANS held an Emergency Webcast to inform the industry about the attack

- SANS Emergency Webcast: What you need to know about the SolarWinds Supply-Chain Attack
- https://www.youtube.com/watch?v=qP3LQNsjKWw
- This one is almost an hour long – but has a lot of good details and recommendations

Videos on Cyber Attacks

General Information:

- ABC News In-depth, *How hackers threaten everything from your bank account to national security (2016)*
- *https://www.youtube.com/watch?v=bUXtuMf2o10*
- ***Note***: ABC is the ***Australian*** Broadcasting Corporation – not the ***American*** Broadcasting Corporation

A Discussion on ransomware

- CNBC, *Why The U.S. Can't Stop Cyber Attacks*
- https://www.youtube.com/watch?v=hSQf3hUx9J0