Cyber Laws

CS-3113: PRINCIPLES OF CYBER SECURITY

BENJAMIN R. ANDERSON

Cyber Laws

There are a number of laws that cover operating in cyberspace

There are many question when it comes to jurisdiction

- The U.S. government has jurisdiction in the United States
- Does it have jurisdiction if someone is in another country, but conducts malicious activities against a system in the United States?
- What about if that is reversed and the attacker is in the United States, but their target is in another country?
- There are some laws that cover these situations, but extradition and inconsistencies in legal requirements make this difficult
- Plus, there is the issue of attribution – how do you prove it was someone in Canada or France or Brazil that attacked a server in Texas?

Best practice: Always consult legal counsel when you are conducting cyber operations

- This includes legal operations, especially if they take place in other jurisdictions
- For example, the EU has different privacy requirements for data than the US – so EU customer data may have to be protected in a different way
- You can accidentally break the law – so you want to be careful

U.S. Cyber Laws

When discussing federal laws that govern or are related to cybersecurity and warfare, there are two documents we need to examine:

- The Constitution
- The U.S. Code

The Constitution does not specifically mention computers, but it is the basis for all laws in the U.S.

The Constitution

- Article I (Legislative Branch)
- Article II (Presidency)
- Article III (Judiciary)
- Amendment 4 (Search and Seizure)
- Amendment 14 (Due Process)

U.S. Code

- Title 10 (Armed Forces)
- Title 18 (Crimes)
- Title 50 (War and National Defense)

U.S. Cyber Laws

If you have not read the Constitution of the United States, I highly recommend it

- The National Constitution Center has the text online
- https://constitutioncenter.org/interactive-constitution/full-text
- Did you know that Article I, Section 8 allows Congress to authorize someone to be a privateer or corsair?
  - It also prevents individual states from doing so

U.S. Cyber Laws

Key Articles of the Constitution, and their (short) definitions from Wikipedia:

- ***Article One***: Establishes the legislative branch of the federal government, the United States Congress
- ***Article Two***: Establishes the executive branch of the federal government, which carries out and enforces federal laws
- ***Article Three***: Establishes the judicial branch of the federal government
- ***Article Four***: Outlines the relationship between the various states, as well as the relationship between each state and the United States federal government
- ***Article Five***: Outlines the process for amending the Constitution
- ***Article Six:*** Establishes the Constitution, and all federal laws and treaties of the United States made according to it, to be the supreme law of the land, and that "the judges in every state shall be bound thereby, any thing in the laws or constitutions of any state notwithstanding."
- ***Article Seven***: Describes the process for establishing the proposed new frame of government

The Signing of the United States Constitution occurred on September 17, 1787 when 39 delegates to the Constitutional Convention endorsed the constitution created during the convention

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

U.S. Cyber Laws

Fourth Amendment

- The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized
- Are computer files considered “papers”?

Fourteenth Amendment

- The Fourteenth Amendment addresses many aspects of citizenship and the rights of citizens
- Section 1. All persons born or naturalized in the United States, and subject to the jurisdiction thereof, are citizens of the United States and of the state wherein they reside. No state shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any state deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws

U.S. Cyber Laws

From Wikipedia:

- "The Code of Laws of the United States of America (variously abbreviated to Code of Laws of the United States, United States Code, U.S. Code, U.S.C., or USC) is the official compilation and codification of the general and permanent federal statutes of the United States. It contains 53 titles"
  - Title 10: Armed Forces (including the Uniform Code of Military Justice)
  - Title 18: Crimes and Criminal Procedure
  - Title 32: National Guard
  - Title 50: War and National Defense
    - Chapter 36: Foreign Intelligence Surveillance
      - SUBCHAPTER I - ELECTRONIC SURVEILLANCE (§§ 1801 to 1813)
      - SUBCHAPTER II - PHYSICAL SEARCHES (§§ 1821 to 1829)
      - SUBCHAPTER III - PEN REGISTERS AND TRAP AND TRACE DEVICES FOR FOREIGN INTELLIGENCE PURPOSES (§§ 1841 to 1846)
      - SUBCHAPTER IV - ACCESS TO CERTAIN BUSINESS RECORDS FOR FOREIGN INTELLIGENCE PURPOSES (§§ 1861 to 1864)
      - SUBCHAPTER V - [INTELLIGENCE] OVERSIGHT (§§ 1871 to 1874)
      - SUBCHAPTER VI - ADDITIONAL PROCEDURES REGARDING CERTAIN PERSONS OUTSIDE THE UNITED STATES (§§ 1881 to 1881g)
      - SUBCHAPTER VII - PROTECTION OF PERSONS ASSISTING THE GOVERNMENT (§§ 1885 to 1885c)

U.S. Cyber Laws

The Computer Fraud and Abuse Act (CFAA) was the first major attempt at creating a law that directly addressed computer crime

- Enacted in 1986
- Based on *18 U.S.C. § 1030*

According to Wikipedia:

- *The Computer Fraud and Abuse Act of 1986 (CFAA) is a United States cybersecurity bill that was enacted in 1986 as an amendment to existing computer fraud law (18 U.S.C. § 1030), which had been included in the Comprehensive Crime Control Act of 1984. The law prohibits accessing a computer without authorization, or in excess of authorization. Prior to computer-specific criminal laws, computer crimes were prosecuted as mail and wire fraud, but the applying law was often insufficient.*
- https://en.wikipedia.org/wiki/Computer_Fraud_and_Abuse_Act

U.S. Cyber Laws

The CFAA was carefully written to avoid infringing on states' rights

- The Constitution limits the jurisdiction of the federal government to certain areas
- To avoid this issue, the law carefully states what computers are covered by the CFAA

From Wikipedia:

- *The only computers, in theory, covered by the CFAA are defined as "protected computers". They are defined under section 18 U.S.C. § 1030(e)(2) to mean a computer:*
  - *exclusively for the use of a financial institution or the United States Government, or any computer, when the conduct constituting the offense affects the computer's use by or for the financial institution or the government; or*
  - *which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States ...*
  - *In practice, any ordinary computer has come under the jurisdiction of the law, including cellphones, due to the interstate nature of most Internet communication.*

If you ping a server that is in Oklahoma – that is interstate communication

If you access a web site or service hosted outside of Texas (if you are in Texas) – that is interstate communication

What if your DNS request goes to a DNS server in Texas, but it pings an authoritative server outside of Texas? Is that interstate communication?

- I have no idea – but that's why I gave the advice of talking to legal counsel

U.S. Cyber Laws

Read: 18 U.S. Code § 1030 - Fraud and related activity in connection with computers

- Just Subsection (a) 1-7
- https://www.law.cornell.edu/uscode/text/18/1030
- ***Remember***: Unless you are a lawyer, don't assume you understand the legal meaning of these items

U.S. Cyber Laws

Other Laws:

- Electronic Communications Privacy Act (ECPA), 18 U.S.C 2510-22
- The Wiretap Act, 18 U.S.C. 2511
- Unlawful Access to Stored Communications, 18 U.S.C. 2701
- Identity Theft, 18 U.S.C. 1028
- Access Device Fraud, 18 U.S.C. 1029
- Wire Fraud, 18 U.S.C. 1343, Communication lines 1362
- CAN-SPAM Act of 2003, 18 U.S.C. 1037; Controlling the Assault of Non-Solicited Pornography And Marketing Act of 2003
- Economic Espionage Act, 18 U.S.C. 1831-32

U.S. Cyber Laws

Other Regulations Important to Cybersecurity:

- Health Insurance Portability and Accountability Act (HIPAA): Privacy regulations in Healthcare industry
- Graham-Leach-Bliley (GLB): Financial institutions have to have process in place to protect private info
- Sarbanes-Oxley (SOX or SarbOx): Auditability, protection and accuracy of financial data
- Payment Card Industry (PCI) Data Security Standards (PCI DSS): Protections for those who use credit cards
- Federal Information Security Management Act (FISMA): Addresses security risks to critical data
  - If you work with the federal government, you will become very familiar with FISMA
- Cybersecurity Information Sharing Act (CISA): provides protections to organizations that share information
- Homeland Security Presidential Directive No. 7 (HSPD-7): Enhance the protection of the nation's critical Infrastructures
  - This is one that many people are not familiar with, but is still one to know

The highlighted regulations are encountered throughout the cybersecurity industry

Texas Cyber Laws

Here is an example of some things that are computer crimes under Texas law:

- Knowingly accessing a computer, computer network or computer system without the consent of the owner;
- Knowingly soliciting a minor under the age of 17 over the internet, text message, or other electronic system, to meet in person for the purpose of engaging in sexual behavior with the defendant;
- Knowingly accessing a computer system, network, program, software or machine that is part of a voting system that uses direct recording electronic voting machines and tampers with the votes or the ability of someone to vote.
- Creating a web page or leaving messages on a social networking site using the persona of another without the person's consent and with the intent to harm, defraud, intimidate or threaten someone; or
- Referencing the name, domain address, phone number or any other identifying information of a person without that person's consent, intending to cause the recipient to think the message is truly coming from that person, with the intent to harm or defraud someone.

Cyber-bullying could break several of these laws

Texas Cyber Laws

The actual text of the Texas Computer Crimes law can be found here:

- https://statutes.capitol.texas.gov/docs/PE/htm/PE.33.htm

This law covers a lot of ground

- It includes “critical infrastructure facility” as a definition for this law
  - Sec. 33.01. DEFINITIONS. (10-a)
- It also discusses ransomware
  - Sec. 33.023. ELECTRONIC DATA TAMPERING.

From the law:

- *Sec. 33.02. BREACH OF COMPUTER SECURITY. (a) A person commits an offense if the person knowingly accesses a computer, computer network, or computer system without the effective consent of the owner.*

Cyberwarfare and Law

***From**: Cyberwarfare: Information Operations in a Connected World* by Chapple and Seidl:

- "The Geneva Conventions and the additional protocols that have been added to them since their original creation in 1949 have shaped how modern warfare is fought – describing what is acceptable and what is not …
- "Cyberwarfare tests the boundaries of existing international laws for many reasons. By its nature, it typically requires the use of civilian infrastructure to conduct attacks. The systems from which attacks are conducted are often civilian systems – or the attacks pass through civilian systems as part of their path to government and military targets
- "Cyberwarfare also creates the potential for unrestricted attacks by nontraditional combatants. It places what may be a possibly far more powerful weapon in their hands in the form of malware… It provides a powerful asymmetric weapon in the hands of insurrectionists and guerrillas

Cyberwarfare and Attribution

Remember our previous discussion regarding attribution:

- Guerrillas, insurrectionists, and terrorists can take advantage of this difficulty

If an attacker is using a bot, the organization that owns the system that is the source of the attack, is not the one launching the attack

- There are attribution methods, such as tool analysis
- A capable organization (or nation state) can imitate the tools and tactics to mislead any analysis
  - A Canadian, Norwegian, or even American hacking group could use an OS that is configured to use a Russian keyboard, and a Russian time zone
  - They could conduct their operations between 8:00 am and 5:00pm Moscow time
  - An initial analysis would then take this as Russian activity
- Organizations can also take credit for attacks they didn't commit

Types of Warfare

There are two high-level divisions to the type of warfare

- Traditional or kinetic warfare
- Cyberwarfare

Traditional Warfare:

- Fought using physical weapons
  - Bullets, tanks, ships, planes, helicopters
- Involves moving people and physical assets into the war zone
  - Drones may not require moving people, but they still need to physically go to a location
- Since there is a specific area that is being attacked or occupied, civilians are aware they are in or near a combat area
  - They may not be able to leave the area, but they are generally aware of the conflict

Cyberwarfare:

- Does not have the same characteristics as kinetic warfare
- It is fought in cyberspace, and can impact the other side of the globe in seconds, and civilian infrastructure may be impacted with no warning

The United Nations

The United Nations Charter covers every country that is a member of the United Nations

- This is almost all of them

Article 1 of the U.N. Charter gives the purpose of the United Nations

From Wikipedia:

- *To maintain international peace and security, to take effective collective measures for the prevention and removal of threats to the peace, and for the suppression of acts of aggression or other breaches of the peace, and to bring about by peaceful means, and in conformity with the principles of justice and international law, adjustment or settlement of international disputes or situations which might lead to a breach of the peace;*
- *To develop friendly relations among nations based on respect for the principle of equal rights and self-determination of peoples, and to take other appropriate measures to strengthen universal peace;*
- *To achieve international co-operation in solving international problems of an economic, social, cultural, or humanitarian character, and in promoting and encouraging respect for human rights and for fundamental freedoms for all without distinction as to race, sex, language, or religion; and*
- *To be a centre for harmonizing the actions of nations in the attainment of these common ends.*
- https://en.wikipedia.org/wiki/Charter_of_the_United_Nations

The United Nations

Other Articles of the U.N. Charter:

- ***Article 41***: The Security Council may decide what measures not involving the use of armed force are to be employed to give effect to its decisions, and it may call upon the Members of the United Nations to apply such measures. These may include complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication, and the severance of diplomatic relations
  - Do computer systems fall under “other means of communication”?
  - Since this does not include armed force, could a government ask Google to “blockade” their services to another country?
- ***Article 42***: Should the Security Council consider that measures provided for in Article 41 would be inadequate or have proved to be inadequate, it may take such action by air, sea, or land forces as may be necessary to maintain or restore international peace and security. Such action may include demonstrations, blockade, and other operations by air, sea, or land forces of Members of the United Nations
  - Does the U.N. have authority to use cyber efforts to achieve these goals?

The United Nations

Other Articles of the U.N. Charter:

- ***Article 45***: In order to enable the United Nations to take urgent military measures, Members shall hold immediately available national air-force contingents for combined international enforcement action. The strength and degree of readiness of these contingents and plans for their combined action shall be determined within the limits laid down in the special agreement or agreements referred to in Article 43, by the Security Council with the assistance of the Military Staff Committee
  - Does this include cyber weapons?
- ***Article 51***: Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defense shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.

Other Factors To Consider

Nations may be involved in coalitions, treaties, conventions, or other agreements that may define when they become involved in a conflict to help defend another nation

- Depending on the wording, this might include cyber attacks
- Would NATO have to act if a member nation was hit with a cyber attack?

Long-standing Concepts In Warfare

There are two concepts that define what makes a war “just”

- Jus ad bellum (Latin for: Right to War)
- Jus in bello (Latin for: Law of War)

From the International Committee of the Red Cross:

- Jus ad bellum refers to the conditions under which States may resort to war or to the use of armed force in general.
- Jus in bello regulates the conduct of parties engaged in an armed conflict. IHL [International Humanitarian Law] is synonymous with jus in bello; it seeks to minimize suffering in armed conflicts, notably by protecting and assisting all victims of armed conflict to the greatest extent possible.
- https://www.icrc.org/en/document/what-are-jus-ad-bellum-and-jus-bello-0

While it generally refers to armed forces, it could also apply to cyber forces

- This brings in the question of when a cyber attack could be responded to with a kinetic attack (or vice-versa)

The Geneva Convention

Read: Geneva Conventions, Wikipedia:

- https://en.wikipedia.org/wiki/Geneva_Conventions
- This is for your general understanding

From the article:

- The Geneva Conventions extensively define the basic rights of wartime prisoners (civilians and military personnel), established protections for the wounded and sick, and provided protections for the civilians in and around a war-zone; moreover, the Geneva Convention also defines the rights and protections afforded to non-combatants. The treaties of 1949 were ratified, in their entirety or with reservations, by 196 countries. The Geneva Conventions concern only prisoners and non-combatants in war; they do not address the use of weapons of war, which are instead addressed by the Hague Conventions of 1899 and 1907, which concern conventional weapons, and the Geneva Protocol, which concerns biological and chemical warfare.

As noted previously, a cyber attack against critical infrastructure would affect civilians

The Geneva Protocol

From: Geneva Protocol, Wikipedia

- https://en.wikipedia.org/wiki/Geneva_Protocol
- *The Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or other Gases, and of Bacteriological Methods of Warfare, usually called the Geneva Protocol, is a treaty prohibiting the use of chemical and biological weapons in international armed conflicts.*
- *It prohibits the use of "asphyxiating, poisonous or other gases, and of all analogous liquids, materials or devices" and "bacteriological methods of warfare". This is now understood to be a general prohibition on chemical weapons and biological weapons, but has nothing to say about production, storage or transfer.*

What if a cyber attack against critical infrastructure released chemicals, overflowed storage tanks, or disrupted water purification systems

- Would that be considered a chemical or biological attack?

Cyberwarfare in a Kinetic Environment

From: *Cyberwarfare: Information Operations in a Connected World* by Chapple and Seidl:

- *Kinetic warfare can also cross over into cyberwar when the combatants respond to or preempt cyberattacks using traditional means of warfare. A defender may be able to stop an attack in the following circumstances:*
  - *If the location that the attacks are coming from can be determined*
  - *If the network carrying the attacks can be targeted*
  - *If the individuals who are conducting the attack can be captured or killed*
- ***Note that the highlighted item brings back the issue of attribution***

Rules For Cyberwarfare

From: *It's Time to Write the Rules of Cyberwar*, by Karl Rauscher, 27 Nov 2013

- http://spectrum.ieee.org/telecom/security/its-time-to-write-the-rules-of-cyberwar
- *To find the way forward, the EastWest Institute has created the Cyber 40, with delegates from 40 digitally advanced countries. … Since we presented our first proposal for "rules of the road" for cyber conflicts in a Russia-U.S. bilateral report at the 2011 Munich Security Conference, the ideas have gained traction. Other groups are also working on the legal issues surrounding cyberattacks—most notably a NATO-related collaboration based in Tallinn, Estonia, which published its findings this March as the Tallinn Manual*

Tallinn Manual

From Wikipedia:

- https://en.wikipedia.org/wiki/Tallinn_Manual
- *The Tallinn Manual (originally entitled, Tallinn Manual on the International Law Applicable to Cyber Warfare) is an academic, non-binding study on how international law (in particular the jus ad bellum and international humanitarian law) applies to cyber conflicts and cyber warfare. Between 2009 and 2012, the Tallinn Manual was written at the invitation of the Tallinn-based NATO Cooperative Cyber Defence Centre of Excellence by an international group of approximately twenty experts. In April 2013, the manual was published by Cambridge University Press.*

Tallinn 2.0 made several key updates, including changing from “Cyber conflict” to “Cyber operations”

From Wikipedia:

- *States are challenged daily, however, by malevolent cyber operations that do not rise to the aforementioned level. The Tallinn 2.0 project examines the international legal framework that applies to such cyber operations.*

The Tallinn Manual is published, and is available for purchase

- https://www.amazon.com/Tallinn-Manual-International-Applicable-Operations/dp/1316630374/ref=sr_1_1

Tallinn Manual

From: *Cyberwarfare: Information Operations in a Connected World* by Chapple and Seidl

- *One of the first things that must be settled during warfare is the question of where nations have authority, where they can extend that authority, and when they are expected to be in control of actions that they, or others, take on their behalf.*

These questions are addressed by the Tallinn Manual:

- ***Rule 1 – Sovereignty***: A state may exercise control over cyber infrastructure and activities within its sovereign territory
- ***Rule 2 – Jurisdiction***: A State may exercise its jurisdiction:
  - Over persons engaged in cyber activities on its territory
  - Over cyber infrastructure located on its territory
  - Extraterritorially, in accordance with international law
- ***Rule 3*** – Cyber infrastructure located on aircraft, ships, or other platforms in international airspace, on the high seas, or in out space is subject to the jurisdiction of the flag State
- ***Rule 4*** – Any interference by a State with cyber infrastructure aboard a platform, wherever located, that enjoys sovereign immunity constitutes a violation of sovereignty

Tallinn Manual

Other Rules:

- Rule 13 – Self-defense against armed attack:
  - A State that is the target of a cyber operation that rises to the level of an armed attack may exercise its inherent right of self-defense. Whether a cyber operation constitutes an armed attack depends on its scale and effects
- Rule 27 – Levèe en masse (mass national conscription into the military)
  - In an international armed conflict, inhabitants of unoccupied territory who engage in cyber operations as part of a levèe en masse enjoy combatant immunity and prisoner of war status.
  - This could cover ISPs or tech company employees that provide services to support military operations
- Rule 28 – Mercenaries:
  - Mercenaries involved in cyber operations do not enjoy combatant immunity or prisoner of war status.
- Rule 29 – Civilians:
  - Civilians are not prohibited from directly participating in cyber operations amounting to hostilities, but forfeit their protection from attacks for such time as they so participate.
- Rule 44 – Cyber booby traps:
  - It is forbidden to employ cyber booby traps associated with certain objects specified in the law of armed conflict.

Acts of War

With the laws and other information that was covered in this chapter, consider:

- What actions could be considered an “Act of War”?
- Would STUXNET be an act of war?
- What about an attack on a power grid?
- Would the Colonial Pipeline attack be an act of war?
  - It was a criminal operation, but could it have started a cyber war? Or even a kinetic war?
- What about state-sanctioned cyber espionage?
  - If it impacts the operations of critical infrastructure, would it be an act of war?