CS329E: Elements of Security

It's a Dangerous (Cyber) World

Dr. Bill Young
Department of Computer Sciences
University of Texas at Austin

Last updated: January 26, 2015 at 14:30

What I'd Like to Discuss

- The scope of the problem
- Why cyber security is hard
- Are we at (Cyber) war?
- What responses are legal and feasible

From the Headlines

Silent War, Vanity Fair, July 2013

On the hidden battlefields of history's first known cyber-war, the casualties are piling up. In the U.S., many banks have been hit, and the telecommunications industry seriously damaged, likely in retaliation for several major attacks on Iran.

Washington and Tehran are ramping up their cyber-arsenals, built on a black-market digital arms bazaar, enmeshing such high-tech giants as Microsoft, Google, and Apple.

From the Headlines

Iran’s supreme leader tells students to prepare for cyber war, rt.com, 2/13/14

Ayatollah Ali Khamenei has delivered a sabre-rattling speech to Iran’s ’Revolutionary foster children’ (in other words, university students) to prepare for cyber war. The supreme leader has urged his country’s students whom he called “cyber war agents” — to prepare for battle.

Israel, Tehran’s main adversary in regional politics, has voiced similar statements recently; Major General Aviv Kochavi said that cyber warfare will change the nature of conflict. “Cyber, in my modest opinion, will soon be revealed to be the biggest revolution in warfare, more than gunpowder and the utilization of air power in the last century.”

From the Headlines

House Intel Chair Mike Rogers Calls Chinese Cyber Attacks 'Unprecedented', ABC News, 2/24/13

House Intelligence Committee Chair Mike Rogers, R-Mich., said it was "beyond a shadow of a doubt" that the Chinese government and military is behind growing cyber attacks against the United States, saying "we are losing" the war to prevent the attacks.

"It is unprecedented," Rogers added. "This has never happened in the history of the world, where one nation steals the intellectual property to re-purpose it—to illegally compete against the country ... and I'll tell you, It is as bad as I've ever seen it and exponentially getting worse. Why? There's no consequence for it."

From the Headlines

Pentagon accuses China of trying to hack US defence networks, The Guardian, 5/7/13

China is using espionage to acquire technology to fuel its military modernisation, the Pentagon has said, for the first time accusing the Chinese of trying to break into US defense computer networks and prompting a firm denial from Beijing.

From the Headlines

Cyber security in 2013: How vulnerable to attack is US now?, Christian Science Monitor, 1/9/13

The phalanx of cyberthreats aimed squarely at Americans' livelihood became startlingly clear in 2012 and appears poised to proliferate in 2013 and beyond.

That prediction came true:
2013 was the most historic year ever for cyber attacks. The industry saw several mega attacks that included sophisticated DDoS attack methods. (IT Business Edge, 12/16/13)

Do you think that 2014 was even worse? What's your evidence of that?

From the Headlines

U.S. Not Ready for Cyberwar Hostile Attackers Could Launch, The Daily Beast, 2/21/13

The Chinese reportedly have been hacking into U.S. infrastructure, and Leon Panetta says future attacks could plunge the U.S. into chaos.

If we are plunged into chaos and suffer more physical destruction than 50 monster hurricanes and economic damage that dwarfs the Great Depression ... Then we will wonder why we failed to guard against what outgoing Defense Secretary Leon Panetta has termed a "cyber-Pearl Harbor."

The U.S. at Risk?

Experts believe that U.S. is perhaps particularly vulnerable to cyberattack compared to many other countries.

- The U.S. is probably more dependent on technology than any other society on earth.
- Sophisticated attack tools are readily available to anyone on the Internet.
- The openness of U.S. society means critical information and vulnerabilities are accessible.

The U.S. at Risk?

More reasons we're vulnerable:

- Much of the U.S. critical infrastructure is accessible on-line.
- Other nation states have much more control over their national communication infrastructure.
- The defense establishment is drowning in data.
- Technology advances rapidly but remains riddled with vulnerabilities.

How Bad Is It?

Cyberwarfare greater threat to US than terrorism, say security experts, Al Jazeera America, 1/7/14

Cyberwarfare is the greatest threat facing the United States — outstripping even terrorism — according to defense, military, and national security leaders in a Defense News poll, a sign that hawkish warning about an imminent 'cyber Pearl Harbor' have been absorbed in defense circles.

45 percent of the 352 industry leaders polled said cyberwarfare is the gravest danger to the U.S., underlining the government's shift in priority—and resources—toward the burgeoning digital arena of warfare.

The U.S. Government Takes this Seriously

"The Pentagon has concluded that computer sabotage coming from another country can constitute an act of war, a finding that for the first time opens the door for the U.S. to respond using traditional military force." (Wall Street Journal, 5/31/11)

"The Pentagon plans to triple its cybersecurity staff by 2016, U.S. Secretary of Defense Chuck Hagel announced recently. A few days later, FBI Supervisory Special Agent Charles Gilgen said at a conference on cybercrime that his agency's cyber division plans to hire 1,000 agents and 1,000 analysts in the coming year. Just those two agencies are looking for 6,000 people with cybersecurity skills in the next two years." (Bloomberg Business, 4/15/14)

Current Concern

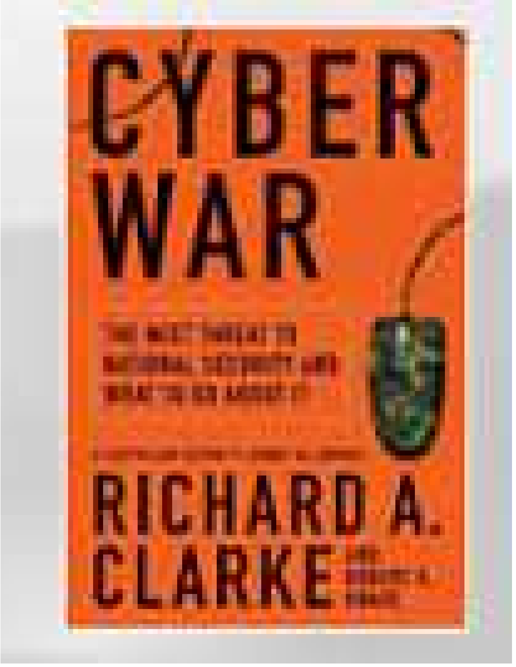
The Obama administration has placed an emphasis on protection of critical infrastructure from cyber attack.

On 2/12/13, the administration released an executive order *Improving Critical Infrastructure Cybersecurity* and Presidential Policy Directive 21: *Critical Infrastructure Security and Resilience*

> *The Nation's critical infrastructure provides the essential services that underpin American society. Proactive and coordinated efforts are necessary to strengthen and maintain secure, functioning, and resilient critical infrastructure including assets, networks, and systems that are vital to public confidence and the Nation's safety, prosperity, and well-being.*

But Are We Already at (Cyber) War?

Cyber warfare involves "actions by a nation-state to penetrate another nation's computers or networks for the purpose of causing damage or disruption." –Clarke and Knape.



This definition raises as many questions as it addresses:

- Can't a non-state entity engage in warfare?
- Which computers or networks matter?
- Which actions should qualify as acts of war?
- Is "warfare" even a useful term in this context?
- Why not just make our computers and networks impervious to such attacks?

Why Are We At Risk?

Arguably, the only way that another nation-state can "penetrate [our] computers or networks for the purpose of causing damage or disruption" is

1. if they have insider access; or
2. there are exploitable vulnerabilities that allow them to gain remote access.

So, why not just "harden" our computers and networks to remove the vulnerabilities?

Why Security is Hard: Target Rich Environment

From the DoD 2010 *Quadrennial Defense Review*:

"On any given day there are as many as 7 million DoD computers and telecommunication tools in use in 88 countries using war-fighting and support applications. The number of potential vulnerabilities, therefore, is staggering."

That means that there are *lots* of insiders, in addition to the possible vulnerabilities in the software and hardware.

Is Cyber Security Particularly Hard?

But why is cybersecurity any harder than any other technological problem? Or is it?

Partial answer: Most technological problems are concerned with ensuring that something good happens. Security is all about ensuring that *bad things never happen*.

In cybersecurity, you have to defeat an *actively malicious adversary*. Security Guru Ross Anderson characterizes this as *"Programming Satan's Computer."*

Cyber Defense is Asymmetric

The defender has to find and eliminate *all* exploitable vulnerabilities; the attacker only needs to find *one*!

Not only do you have to find “bugs” that make the system behave differently than expected, you have to identify any features of the system that are susceptible to misuse and abuse, *even if your programs behave exactly as you expect them to.*

Cyber Security is Tough

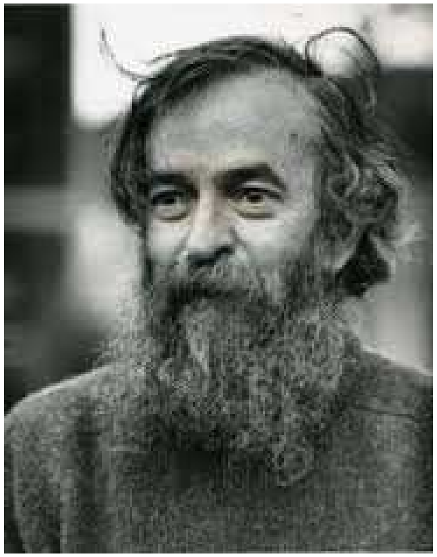
Perfect security is unachievable in any useful system. We trade-off security with other important goals: functionality, usability, efficiency, time-to-market, and simplicity.

MORDAC, THE PREVENTER OF INFORMATION SERVICES.
SECURITY IS MORE IMPORTANT THAN USABILITY.
scottadams@aol.com
www.dilbert.com
IN A PERFECT WORLD, NO ONE WOULD BE ABLE TO USE ANYTHING.
©2007 Scott Adams, Inc./Dist. by UFS, Inc.
To complete the log-in procedure, stare directly at the sun.

© Scott Adams, Inc./Dist. by UFS, Inc.

Is It Getting Better?

"The three golden rules to ensure computer security are: do not own a computer; do not power it on; and do not use it." –Robert H. Morris (mid 1980's), former chief scientist of the National Computer Security Center



"Unfortunately the only way to really protect [your computer] right now is to turn it off, disconnect it from the Internet, encase it in cement and bury it 100 feet below the ground." –Prof. Fred Chang (2009), former director of research at NSA

Some Sobering Facts

- It is *undecidable* whether a given piece of software contains malicious functionality.
- Once PCs are infected they tend to stay infected. The median length of infection is 300 days.

- "More than 5.5 billion attempted attacks were identified in 2011, an increase of 81 percent over 2010, with an unprecedented 403 million unique malware variants that year, a 41 percent leap." (Symantec Internet Security Threat Report, 2012)

The Cost of Data Breaches

The Privacy Right's Clearinghouse's *Chronology of Data Breaches* (January, 2012) estimates that more than half a billion sensitive records have been breached since 2005. This is actually a very "conservative estimate."

The Ponemon Institute estimates that the approximate current cost per record compromised is around $318.

"A billion here, a billion there, and pretty soon you're talking real money" (attributed to Sen. Everett Dirksen)

Security is About Managing Risk

In *Building Secure Software*, Viega and McGraw assert that software and system security is “all about managing risk.” This can be done through:

Risk acceptance: some risks are simply tolerated by the organization.

Risk avoidance: not performing an activity that would incur risk.

Risk mitigation: taking actions to reduce the losses due to a risk.

Risk transfer: shift the risk to someone else.

There is generally much more money in a bank than in a convenience store; but which is more likely to be robbed? Why?

But is it War?

- How real is the threat?
- Is the warfare metaphor a help or a hinderance?
- Are cyberattacks best viewed as crimes, "armed attacks," both, or something else entirely?
- Is this issue about semantics or substance?
- Does it really matter?

Why Does it Matter?

Many experts believe that cyber attacks are a serious risk to U.S. national interests today.

America's failure to protect cyberspace is one of the most urgent national security problems facing the new administration that will take office in January 2009. ... It is a battle we are losing. Losing this struggle will wreak serious damage on the economic health and national security of the United States. –CSIS report on *Securing Cyberspace for the 44th Presidency*, Dec. 2008

But others argue the threat is overrated and is largely hype by the security establishment.

Is it really warfare or is it just crime, that should be dealt with by the criminal justice establishment?

Warfare: Cyber and Otherwise

In modern parlance, a shooting war is called *kinetic warfare*, where "kinetics" is concerned with the relationship between the motion of bodies and its causes.

Recall Clarke's definition of cyber warfare: "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption."

Can activity in cyberspace have kinetic consequences such as property damage and loss of lives? *Does it have to have such consequences to qualify as an act of war?*

The Pentagon View

Cyber Combat: Act of War, Wall Street Journal, 5/31/11

"The Pentagon has concluded that computer sabatoge coming from another country can constitute an act of war, a finding that for the first time opens the door for the U.S. to respond using traditional military force. ...

One idea gaining momentum at the Pentagon in the notion of 'equivalence.' If a cyber attack produces the death, damage, destruction, or high level disruption that a traditional military attack could cause, it would be a candidate for a 'use of force' consideration."

Notable Cyber Campaigns

First Persian Gulf War (1991): Iraq's command and control infrastructure is targeted. Radar and missile control network is fragmented and sections of radar coverage are taken offline without central control being aware of the outage.

Estonia (2007): Cyberattacks disabled the websites of government ministries, political parties, newspapers, banks, and companies. Russia was suspected of launching the attack in retaliation for the removal of the Bronze Soldier Soviet war memorial in central Tallinn.

Georgia (2008): Russia attacked the nation of Georgia in a dispute over the province of South Ossetia. In addition to the military attack, a concerted cyber DoS attack shut down much of Georgia's ability to communicate with the external world.

What Might an Attack Look Like: Stuxnet

Stuxnet is a Windows computer worm discovered in July 2010 that targets Siemens SCADA (Supervisory Control and Data Acquisition) systems.

In interviews over the past three months in the United States and Europe, experts who have picked apart the computer worm describe it as far more complex and ingenious than anything they had imagined when it began circulating around the world, unexplained, in mid-2009. –New York Times, 1/16/11

Stuxnet Characteristics

> *Stuxnet is the new face of 21st-century warfare: invisible, anonymous, and devastating. ... Stuxnet was the first literal cyber-weapon. America's own critical infrastructure is a sitting target for attacks like this.*
> *(Vanity Fair, April 2011)*

- Stuxnet was the first (known) malware that subverts specific industrial systems.
- Believed to have involved years of effort by skilled hackers to develop and deploy.
- Narrowly targeted, quite possibly at Iran's nuclear centrifuges.
- Widely believed to have been developed by Israel and the U.S.

Stuxnet Worm

Kaspersky Lab Provides Its Insights on Stuxnet Worm, Kaspersky.com, 9/24/10

"I think that this is the turning point, this is the time when we got to a really new world, because in the past there were just cyber-criminals, now I am afraid it is the time of cyber-terrorism, cyber-weapons and cyber-wars."

Children of Stuxnet

The successors of Stuxnet may be even more sophisticated:

DuQu: (Sept. 2011) looks for information that could be useful in attacking industrial control systems.

Flame: (May 2012) designed for cyber-espionage, targeted government organizations and educational institutions in Iran and elsewhere.

Gauss: (Aug. 2012) complex cyber-espionage toolkit designed to steal sensitive data.

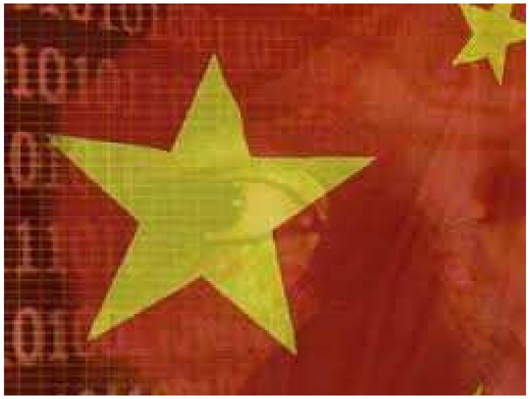
Unlike conventional munitions, could be repurposed and redirected at the sender.

Cyber Attacks on the U.S.

The U.S. has already been "attacked" in the sense of cyber espionage.

Moonlight Maze: coordinated attacks on U.S. computer systems in 1999, traced to a computer in Moscow. Hackers obtained large stores of data possibly including classified naval codes and information on missile guidance systems.

Titan Rain: series of coordinated attacks on U.S. computer systems since 2003. Probably Chinese in origin and probably gathering intelligence; *an estimated 10-20 terabytes of data may have been downloaded.*



There are undoubtedly others that we don't yet know about.

Does This Go Beyond Espionage?

Some security experts warn that a successful possible widespread attack on U.S. computing infrastructure *could largely shut down the U.S. economy for up to 6 months.*

It is estimated that the destruction from a single wave of cyber attacks on U.S. critical infrastructures could exceed $700 billion USD—the equivalent of 50 major hurricanes hitting U.S. soil at once. (Source: US Cyber Consequences Unit, July 2007)

CyberAttacks: An Existential Threat?

Cyberattacks an 'Existential Threat' to U.S., FBI Says, Computerworld, 3/24/10

A top FBI official warned today that many cyber-adversaries of the U.S. have the ability to access virtually any computer system, posing a risk that's so great it could "challenge our country's very existence."

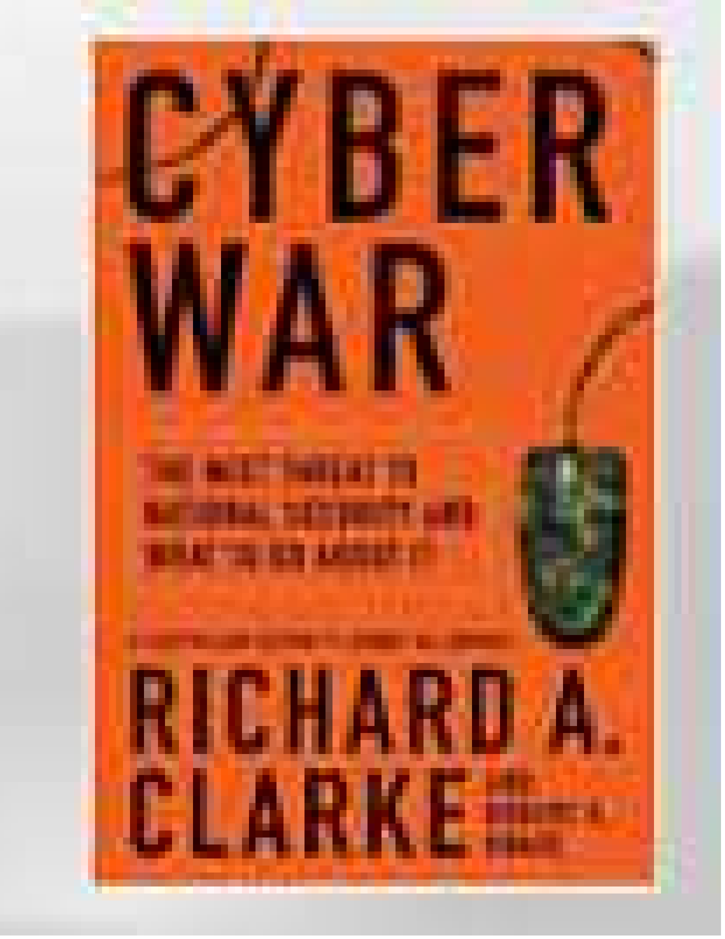
According to Steven Chabinsky, deputy assistant director of the FBI's cyber division: "The cyber threat can be an existential threat—meaning it can challenge our country's very existence, or significantly alter our nation's potential."

Not Everyone Agrees

Howard Schmidt, the new cybersecurity czar for the Obama administration, has a short answer for the drumbeat of rhetoric claiming the United States is caught up in a cyberwar that it is losing. “There is no cyberwar. I think that is a terrible metaphor and I think that is a terrible concept,” Schmidt said. “There are no winners in that environment.” (Wired, 3/4/10)

Does Mr. Schmidt think there is no problem? Or just that we’re calling it by the wrong name?

Not Everyone Agrees



The cyberwar rhetoric is dangerous. Its practitioners are artists of exaggeration, who seem to think spinning tall tales is the only way to make bureaucracies move in the right direction. ... Not only does it promote unnecessary fear, it feeds the forces of parochial nationalism and militarism undermining a communications system that has arguably done more to connect the world's citizens than the last 50 years of diplomacy. (Ryan Singel review of Clarke and Knape in Wired, 4/22/10)

Is a Cyber Attack an Act of War?

There are some serious questions that deserve national and international dialogue.

- How serious would a cyber attack have to be considered an “act of war”?
- What if it were an act by *non-state* actors?
- Would it require *certainty* about who initiated it?
- What degree of control would the offending nation have to exert over such actors?
- Must the response be electronic or could it be a “kinetic”?

An Act of War?

According to the McAfee *2009 Virtual Criminology Report*:

“When determining whether a cyber attack is an act of cyber war, experts evaluate four key attack attributes:

- **Source:** Was the attack carried out or supported by a nation-state?
- **Consequence:** Did the attack cause harm?
- **Motivation:** Was the attack politically motivated?
- **Sophistication:** Did the attack require customized methods and/or complex planning?”

What do you think of these criteria? Are they precise enough to be useful?

Cyber Attacks as Armed Attacks

Various international conventions allow a self-defense or "anticipatory self-defense" response to an *armed attack*. But they don't define "armed attack."

So, when is a cyber attack "equivalent" to an armed attack?

At least three different analytic frameworks have been proposed:

Instrument-based: the damage is such that it previously could only have been caused by a kinetic attack.

Effects-based: what are the overall effects of the attack on the victim state.

Strict liability: attacks against critical infrastructure qualify because of the potential serious consequences.

Which of these analytic frameworks do you find most reasonable?

Selecting Targets

In traditional warfare, the targets tend to be *military*, or industrial sites with military value. Maybe it's too obvious, but why is that?

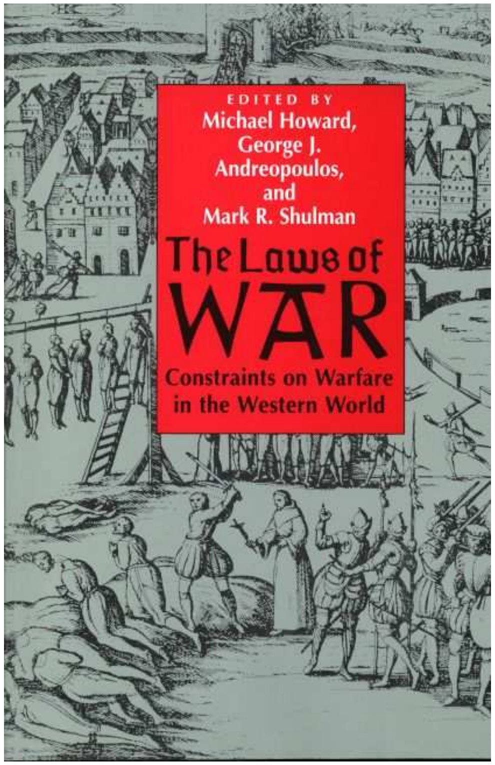
Selecting Targets

In traditional warfare, the targets tend to be *military*, or industrial sites with military value. Maybe it's too obvious, but why is that?

1. Military and industrial targets allow the enemy to counterattack, so have high value.
2. Military assets are likely to be on the defensive perimeter.
3. Certain principles (are supposed to) regulate the conduct of states during warfare.

Selecting Targets

States are supposed to adhere to certain criteria in selecting targets:



- **Distinction:** requires distinguishing combatants from non-combatants and directing actions against military objectives
- **Necessity:** limits force to that “necessary to accomplish a valid military objective”
- **Humanity:** prohibits weapons designed “to cause unnecessary suffering”
- **Proportionality:** protects civilians and property against excessive uses of force

Do these apply to cyberattacks? To responses to cyberattacks?

Targets

There are good reasons to believe that the choice of targets might be different in cyber vs. kinetic warfare.

- Non-state actors may not feel bound by the conventional laws of war.
- The actors may be in an asymmetric power relationship.
- Non-state actors may be looking for “soft” high-value targets.
- Cyber attacks offer the ability to “skip the battlefield.”

> *Systems that people rely upon, from banks to air defense radars, are accessible from cyberspace and can be quickly taken over or knocked out without first defeating a country’s traditional defenses.* –*Clarke and Knape, 31*

Targets

In a cyberattack, targets could be: *military, civil or private sector.*

If a major cyber conflict between nation-states were to erupt, it is very likely that the private sector would get caught in the crossfire. Most experts agree that critical infrastructure systems—such as the electrical grid, banking and finance, and oil and gas sectors—are vulnerable in many countries. Some nation-states are actively doing reconnaissance to identify specific vulnerabilities. –McAfee report, 3

Targets

If adversaries intended to attack nations in cyber space, they would select targets which would cause the largest impacts and losses to their opponents with the least effort. It is therefore a very reasonable assumption that adversaries would attack critical infrastructure systems via the Internet. –McAfee report, 16

Protecting Critical Infrastructure

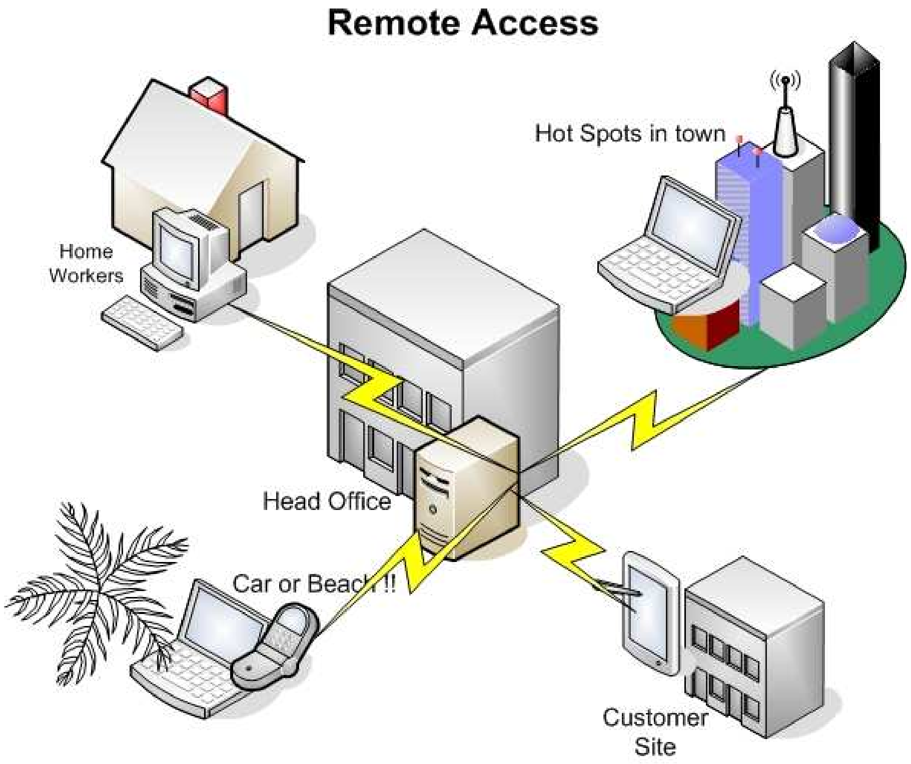
The government takes protection of infrastructure very seriously. Presidential Decision Directive (PDD-63) of 1998 states:

- Civilian systems are "essential to the minimum operations of the economy and government"
- Examples: telecommunications, energy, banking, transportation and emergency services

Surely such systems are not vulnerable to cyberattack. *Nobody would be dumb enough to make such critical functionality accessible remotely.* Would they?

How Vulnerable is Our Infrastructure?

Surely our critical infrastructure is not vulnerable to cyberattack. Nobody would be dumb enough to make such critical functionality accessible remotely. *Would they?*



"I have yet to meet anyone who thinks SCADA systems should be connected to the Internet. But the reality is that SCADA systems need regular updates from a central control, and it is cheaper to do this through an existing Internet connection than to manually move data or build a separate network." –Greg Day, Principal Security Analyst at McAfee

Non-State Actors

Should a nation-state act against another nation-state in response to actions by a non-state actor?

Did the Afghan government (Taliban) attack the World Trade Center and Pentagon on September 11, 2001?

Did Russia actively organize, encourage and facilitate private hackers participating in the cyber attacks on Georgia and Estonia?

Herb Lin, Senior Scientist of the National Academy of Sciences, said that cyberattacks against the U.S. *go up* during exam periods in China. *What do you think that's about?*

Active vs. Passive Defenses

Defenses against cyber attack can be:

Passive: taking steps to prevent an attack or to mitigate the damage should an attack occur (access control, secure system design, security administration).

Active: electronic measures designed to strike attacking computer systems and shut down an attack midstream (destructive viruses, packet flooding)

Most effective approach is probably a *layered* defense or *"defense in depth"* incorporating both approaches.

But victim states often worry that active defenses may violate the laws of war.

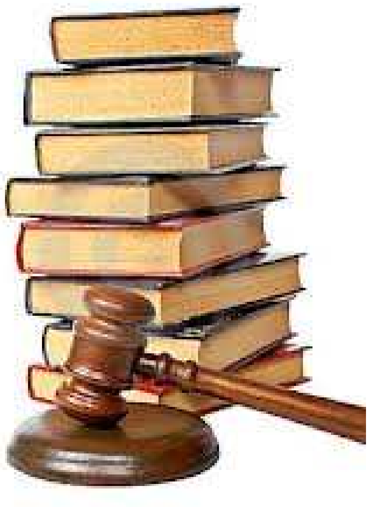
The Attribution Problem

Often it is extremely difficult to determine the source of a cyber attack.

"States find themselves in a 'response crisis' during a cyber attack, forced to decide between effective but arguably illegal, active defenses, and the less effective, but legal, passive defenses and criminal laws." –Carr, *Inside Cyber Warfare*, 47

The Law of War

How do the laws of war apply to cyber attacks?



Laws of war arose in a conventional context in which:

- it is easy to assess the damage following an attack, and
- it is typically easy to identify the attacker.

"Current international law is not adequate for addressing cyber war. Analogies to environmental law, law of the sea and kinetic war all break down at some point. Answering the question of when to use force in response to a cyber attack needs its own framework." –Eneken Tikk, legal advisor for the Cooperative Cyber Defence Centre of Excellence in Estonia

The Prevailing View

According to Lt. Cmd Matt Sklerov (quoted in Carr, 47):

"The prevailing view of states and legal scholars is that states must treat cyber attacks as a criminal matter

1. out of uncertainty over whether a cyberattack can even qualify as an armed attack, and
2. because the law of war requires states to attribute an armed attack to a foreign government or its agents before responding with force."

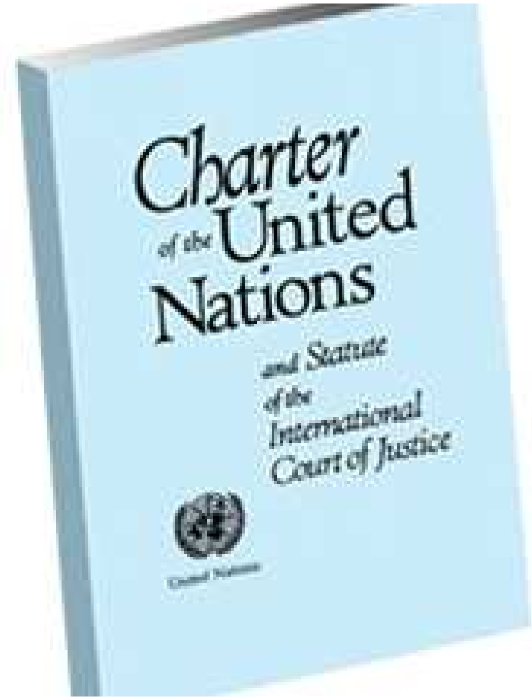
The Crime-Based Approach

If you treat cyber attacks as a criminal matter, with deterrence from criminal laws and penalties, *how do you force states to comply with international criminal laws?*

- "Several major states, such as China and Russia, allow their attackers to operate with impunity when their attacks target rival states." (Carr, 47)
- "International legal acts regulating relations arising in the process of combating cyber crimes and cyber terrorism must not contain norms violating such immutable principles of international law as non-interference in the internal affairs of other states, and the sovereignty of the latter." (Moscow Military Thought, 3/31/97)

U.N. Charter

The U.N. Charter preserves the right of states to engage in "individual or collective self-defense" in response to an "armed attack." (Article 51).


Charter of the United Nations
and Statute of the International Court of Justice
United Nations

However, that begs the question of when a cyber attack should be considered an "armed attack."

The Law of War

States have a long-standing duty to prevent non-state actors from using their territory to commit cross-border attacks, including the requirement for states to act against groups generally known to carry out illegal attacks.

Sklerov suggests that duty “should be interpreted to require states to enact and enforce criminal laws to deter cross-border cyber attacks.”

A state which fails to do so could be labeled a *sanctuary state* and sanctioned by the international community.

The Laws of War

In the cases relating to war crimes in the former Yugoslavia, it was allowed:

> *to impute host-state responsibility for the actions of groups of non-state actors when a state exercised "overall control" of the group, even though the state may not have directed the particular act in question. (Prosecutor vs. Tadic)*

International Agreements

Most directly relevant is the European Convention on Cybercrime, which recognizes the need of states to criminalize cyber attacks and the duty of states to prevent non-state actors on their territory from launching them.

- requires states to establish domestic criminal offenses for most types of cyber attacks
- recognizes the importance of prosecuting attackers
- requires extending jurisdiction to cover a state's territory and actions of citizens regardless of their location.

The Convention has been signed by 26 countries including the U.S.

Conclusions

- Cyber attacks are a serious threat to the U.S. and other states.
- Cyber warfare may not be a helpful metaphor.
- The nature of the Internet makes cyber attacks powerful, difficult to counter, and difficult to attribute.
- No technical solutions are on the horizon.

- Treaties and legal frameworks have not kept pace with the threat.
- Promising theories and approaches are developing to help the international community cope.