First Bytes Talk:

It's a Dangerous (Cyber) World

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

Last updated: July 8, 2016 at 07:36

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.

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. We're not prepared. If the nightmare scenario becomes suddenly real ... If hackers shut down much of the electrical grid and the rest of the critical infrastructure goes with it ...

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."

From the Headlines

Cyberwar Ignites a New Arms Race: Dozens of countries amass cyberweapons, reconfigure militaries to meet threat, Wall Street Journal, Oct. 11, 2015

Countries toiled for years and spent billions of dollars to build elaborate facilities that would allow them to join the exclusive club of nations that possessed nuclear weapons. Getting into the cyberweapon club is easier, cheaper and available to almost anyone with cash and a computer.

A series of successful computer attacks carried out by the U.S. and others has kicked off a frantic and destabilizing digital arms race, with dozens of countries amassing stockpiles of malicious code.

The U.S. at Risk?

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

- The U.S. is highly dependent on technology.
- Sophisticated attack tools are easy to come by.
- A lot of critical information is available on-line.
- Critical infrastructure may be accessible remotely.
- Other nations exercise more control over information and resources.

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.

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

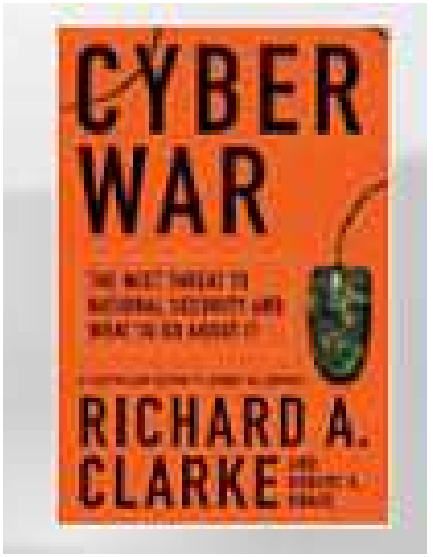
"The Pentagon has concluded that computer sabatoge coming from another country can constitute an act of war, a finding that for the first time opens the door for the U.S. to respond using traditional military force." (Wall Street Journal, 5/31/11)

"The Pentagon will expand its cyber security force from 900 personnel to a massive 4,900 troops and civilians over the next few years following numerous concerns over the dangerously vulnerable state of their defenses, according to US officials." (rt.com, 1/18/13)

By 2019, the cybersecurity job shortage will be 1.5 million, according to the CEO of Symantec Michael Brown.

And Are We Already There?

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.



Clarke's definition of Cyber warfare 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?

Is Cyber Security Particularly Hard?

Why would cybersecurity by any harder than other technological problems?

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

To ensure that, you have to know what all the bad things are!

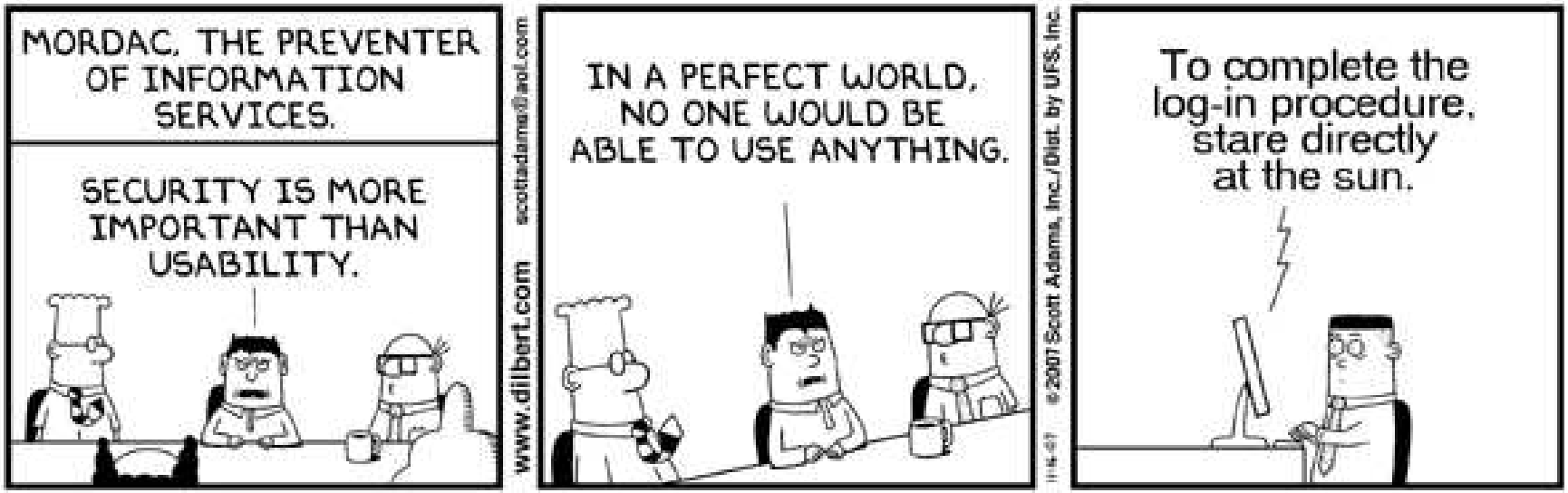
Cyber Defense is Asymmetric

In cybersecurity, you have to defeat an *actively malicious adversary*.

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

Cyber Security is Tough

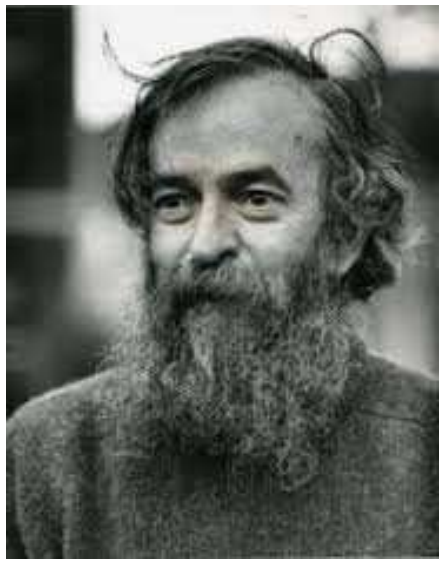
Perfect security is unachievable in any useful system. We trade-off security with other important goals: functionality, usability, efficiency, time-to-market, and simplicity.



© 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

- There is no completely reliable way to tell 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.

- "The number of detected information security incidents has risen 66% year over year since 2009. In the 2014 survey, the total number of security incidents detected by respondents grew to 42.8 million around the world, up 48% from 2013—an average of 117,339 per day." (CGMA Magazine, 10/8/2014)

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)

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?

Warfare: Cyber and Otherwise

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.

Notable Cyber Campaigns

- First Persian Gulf War (1991): Iraq's radar and missile control network taken offline.
- Estonia (2007): websites of government ministries, political parties, newspapers, banks, and companies disabled.
- Georgia (2008): DoS attack shuts down much of Georgia's ability to communicate with the external world.

What Might a Cyber-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.

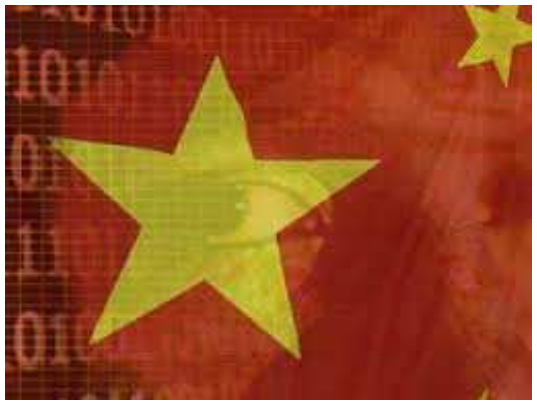
Unlike conventional munitions, could be repurposed and redirected at the sender.

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 (1999), traced to Moscow; compromised huge amount of data, possibly including classified naval codes and missile guidance systems specs.

Titan Rain: coordinated attacks on U.S. systems since 2003 probably Chinese and compromising *an estimated 10-20 terabytes of data.*



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

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."

Does It 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."

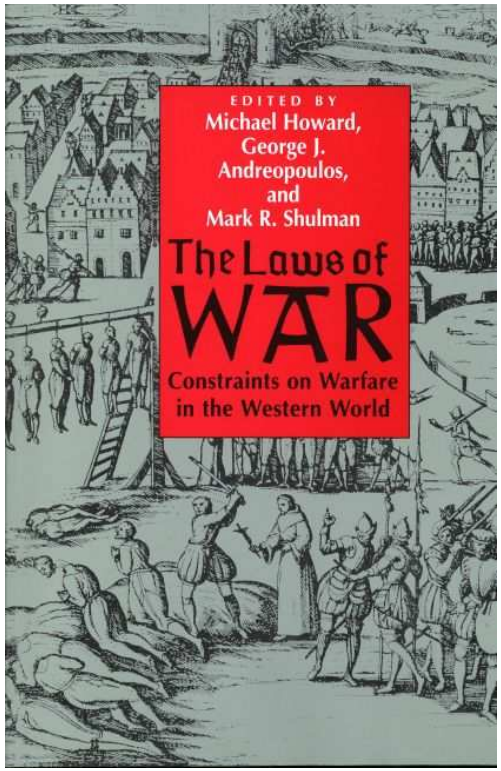
Is a Cyber Attack an Act of War?

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 "kinetic"?

Selecting Targets

Nation states are supposed to adhere to certain criteria in selecting targets of attack:



- **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*

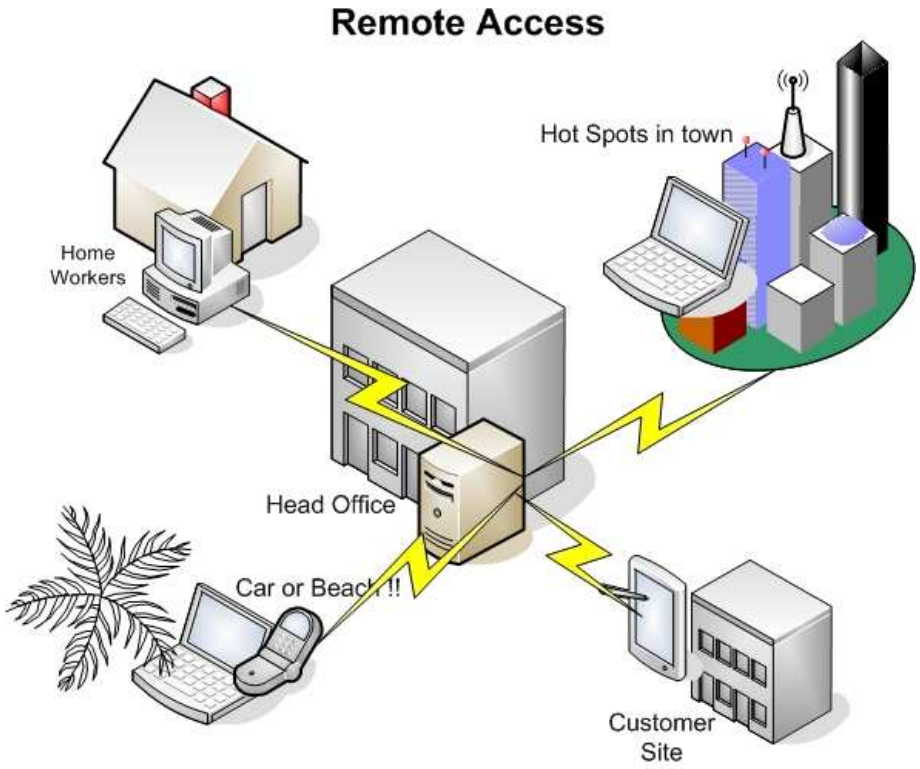
Targets

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. –McAfee (2009) Virtual Criminology Report

How Vulnerable is Our Infrastructure?

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

The Attribution Problem

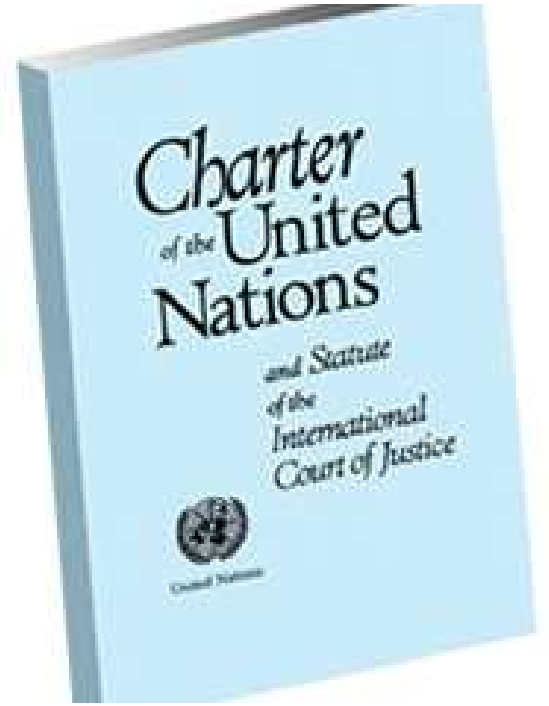
Often it is extremely difficult to determine the source of a cyber attack.

If you're not sure who attacked you, can you attack back?

"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

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).



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

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.

How Do You Enforce It?

But how do you force nation 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)

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.