


Cyber conflict
Introduction

CSCI E 45b: The Cyber World – part B

1 Copyright © Scott Bradner & Ben Gaucherin 2016


Introduction: learning goals



- Understand the evolution of cyber in becoming a key element of national defense
- Understanding the actors and key concepts relating to cyber conflict
- Understanding (yet again) the complexity of mapping real-world ideas to cyberspace

2 Copyright © Scott Bradner & Ben Gaucherin 2016

Early signs of trouble

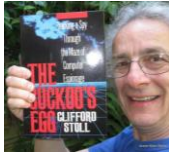


Vladimir Vetrov

- Alleged to be one of the first documented case of cyber attack with kinetic impact
- Halloween 1982 – A newly built trans-Siberian pipeline explodes allegedly because Russian industrial spies were “fed the wrong information” by the CIA that had been warned by agent Farewell

3 Copyright © Scott Bradner & Ben Gaucherin 2016

Early signs of trouble, contd.



- One of the first documented case of cyber espionage
- August 1986 – A Russian spy penetrates Lawrence Berkeley National Laboratory

4

Copyright © Scott Bradner & Ben Gaucherin 2016

Topics, all required



- Conflict – R
Basic concepts of real-world conflict
- Actors – R
Who is involved, in playing what role
- Cyber conflict – R
What it is, and its evolution over the recent past
- Kinetic impact – R
Crossover between cyber and the real world

5

Copyright © Scott Bradner & Ben Gaucherin 2016

Topics, all required, contd.



- Key terms and concepts – R
Important terminology relating to conflict and warfare
- Attribution – R
Finding out who did it is tricky business
- Conflict resolution – R
How does a conflict end
- Zero days – R
Bugs with useful side effects

6

Copyright © Scott Bradner & Ben Gaucherin 2016

Image credits

All drawings and photos by Ben Gaucherin unless noted

Slide# credit

5 <http://www.cfr.org/peacekeeping/global-regime-armed-conflict/p24180>

5 <http://www.eraofwisdom.org/guy-fawkes-mask-is-a-global-symbol-of-our-age-of-activism/>

5 <http://www.flagpatchshop.com/estonia.html>

5

https://en.wikipedia.org/wiki/Urengoy%E2%80%99SPrimary%E2%80%93Uzhgorod_pipeline

6 <http://www.svtuition.org/2013/02/how-cyber-criminals-steal-money.html>

6 <http://uvmzombies.blogspot.com/2013/02/computer-zombies.html>

6 <http://cisac.fsi.stanford.edu/news/herb-lin-wants-put-stanford-forefront-cyber-policy-and-security>

6 <http://www.hitekpals.com/what-is-a-zero-day-exploit/>

7


Copyright © Scott Bradner & Ben Gaucherin 2016

Cyber conflict
Conflict

CSCI E 45b: The Cyber World – part B

1 Copyright © Scott Bradner & Ben Gaucherin 2016


Incident



- **in-ci-dent** (www.merriam-webster.com)
noun \ˈin(t)-sə-dənt, -dənt\ : an unexpected and usually unpleasant thing that happens : an event or disagreement that is likely to cause serious problems in relations between countries
- **Implies:**
Two or more parties
Small scale

2 Copyright © Scott Bradner & Ben Gaucherin 2016

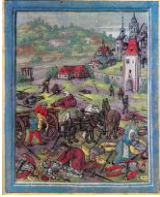
Conflict



- *“Conflict refers to some form of friction, disagreement, or discord arising within a group when the beliefs or actions of one of more members of the group are either resisted by or unacceptable to one or more members of another group.”* – Wikipedia
- Different types of conflicts:
e.g., armed, economic, religious,

3 Copyright © Scott Bradner & Ben Gaucherin 2016

War



- War - A contention by force; or the art of **paralyzing the forces of an enemy**
lectlaw.com
- Public war can be civil or national
Civil – both parties are member of the same nation
National – war between nation states
- The constitution typically defines how to declare a state of war and which branch of government can do so

4

Copyright © Scott Bradner & Ben Gaucherin 2016

Aim and impact of war

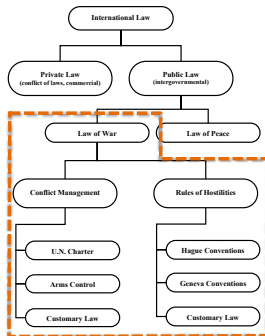


- The achievement of strategic objectives
e.g., control of contested lands
e.g., access to precious resources
e.g., affect a nation's position in a broader context
- Impact historically measured as:
Magnitude of kinetic impact to people, objects, environment
Impact to national infrastructure and economy

5

Copyright © Scott Bradner & Ben Gaucherin 2016

Laws of war

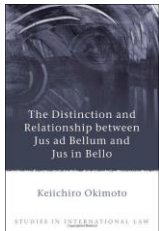


Source: Law of War Deskbook

6

Copyright © Scott Bradner & Ben Gaucherin 2016

Laws of war



- **jus ad bellum** – “justice to war”
How countries proceed to a state of war
- **jus in bello** – “justice in war”
How countries conduct war
- Grounded in the traditional context of war, and diplomacy
- Traditional language is not always useful to assess and establish clear parameters for cyber conflict

7

Copyright © Scott Bradner & Ben Gaucherin 2016

U.S. code and armed conflict



- **DoD Directive 5100.77** establishes requirement for US armed forces compliance to International Law of War
- **USC Title 10** establishes the role of the armed forces
- **USC Title 50** establishes foundational elements of national defense

8

Copyright © Scott Bradner & Ben Gaucherin 2016

Borders and national sovereignty



- Nations exist in the physical world and are defined by their borders
Borders are artificial constructs unrelated to other underlying structures (e.g. culture/people)
- Internet topology does not match national borders
Some exceptions (e.g. China)
From inside the net you cannot see national borders
i.e., there is no technology to account for national borders in operations of the Internet

9

Copyright © Scott Bradner & Ben Gaucherin 2016

Borders and national sovereignty, contd.

FAIL

- La ligne Maginot (the Maginot line)
- Wall built in the 1930's to prevent or at least slow down a German invasion



10

Copyright © Scott Bradner & Ben Gaucherin 2016

Borders and national sovereignty, contd.



- Increasingly, nations have national assets or constituents assets hosted outside their national border

e.g., Estonian "data embassies"



11

Copyright © Scott Bradner & Ben Gaucherin 2016

Sherman – The war on infrastructure



- General in the Union army during the American Civil War
- Focused war efforts on destroying infrastructure
 - "Scorched earth" policy
 - Sherman's bowties
- Few civilian casualties
- Allows for rebuilding
 - Drives economy after war time



12

Copyright © Scott Bradner & Ben Gaucherin 2016

Image credits

Slide#	credit
2	http://www.zerohedge.com/news/2015-11-25/russia-says-turkeys-attack-jet-was-planned-provocation-ankara-moves-tanks-near-syria
3	http://www.cfr.org/peacekeeping/global-regime-armed-conflict/p24180
4, 5	https://en.wikipedia.org/wiki/War
7	http://www.lpbr.net/2013/10/the-distinction-and-relationship.html
8	https://en.wikipedia.org/wiki/Uncle_Sam
9	http://www.outline-world-map.com/political-transparent-white-world-map-b8a
10	http://www.alphr.com/cloud-computing/1000629/microsofts-data-sovereignty-battle-a-disaster-or-triumph-in-the-making
10	http://innac.com/personal_copy_Estonian_Government_Cloud_Kotka_Liiv_2015.PDF
11	https://en.wikipedia.org/wiki/Magnot_Line
12	https://en.wikipedia.org/wiki/William_Tecumseh_Sherman
12	https://www.thinglink.com/scene/702201687082795008

13


Copyright © Scott Bradner & Ben Gaucherin 2016

Cyber conflict
Actors

CSCI E 45b: The Cyber World – part B


1 Copyright © Scott Bradner & Ben Gaucherin 2016

Government – US as an example




- Government agencies are both target and protagonist
- Different agencies hold different parts of the overall picture

Defense, active defense, offense, SIGINT, information protection, inside the US, outside the US, etc.



2 Copyright © Scott Bradner & Ben Gaucherin 2016

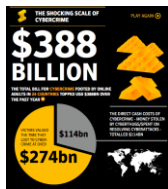
Businesses



- A potential target
For economic impact
Commercial infrastructure operators
- A partner of convenience for the government
Subject to different limitations as government in their ability to counterstrike
Government contractors able to hire personnel that could not be hired by government agencies

3 Copyright © Scott Bradner & Ben Gaucherin 2016

Organized crime



- Uses the Internet as a new platform to do the same old business, and new business
- Cyber weapons are useful for crime related activities as well
- Interested in the economic potential of supporting government cyber needs
 - e.g. the Zero Day market
- Can act as a tool of governments
 - Plausible deniability

4

Copyright © Scott Bradner & Ben Gaucherin 2016

Individual actors, Hackers, Hactivists



- Individuals with special skills, knowledge, and/or access
- Motivated by money, cause, bragging rights, etc.
- Can act independently from government
 - Can be very impactful
 - Plausible deniability, but also headaches...
- Hacktivists - A particular case of individual actor, with cause as a motivation
 - Someone's freedom fighter is someone else's terrorist

5

Copyright © Scott Bradner & Ben Gaucherin 2016

Image credits

All drawings and photos by Ben Gaucherin unless noted

- | Slide# | credit |
|--------|---|
| 2 | Emblems for Directorate of National Intelligence, Department of Transportation, Federal Reserve Systems, Department of Energy, Food and Drug Administration |
| 3 | Logos for Target, Sony, Google, Raytheon |
| 4 | https://samscybersec.wordpress.com/2014/05/11/the-cyber-black-market-a-hackers-haven/ |
| 4 | https://en.wikipedia.org/wiki/Whitey_Bulger |
| 5 | http://www.bbc.co.uk/news/education-15061377 |
| 5 | http://www.eraofwisdom.org/guy-fawkes-mask-is-a-global-symbol-of-our-age-of-activism/ |

6



Copyright © Scott Bradner & Ben Gaucherin 2016

Cyber conflict
 Cyber conflict

CSCI E 45b: The Cyber World – part B

1 Copyright © Scott Bradner & Ben Gaucherin 2016

Some interesting questions

- Is cyber war a “thing” or is it an over-hyped concept aimed at scaring people, and getting more money to spend?
- Is cyberspace a new conflict domain (like air/space, sea, ground) or is it a new facet of war in existing domains?
 The current answer US Cyber Command (USCYBERCOM)

2 Copyright © Scott Bradner & Ben Gaucherin 2016

Conflicting premises (or fear mongering?)



- RAND report in 1993 “the cyber war is coming”
- Air Force in 2005 Declares cyber as “fifth domain”
- Secretary of Defense Leon Panetta – 2012 “cyber-Pearl Harbor”
- Erik Gartzke – 2013 “The Myth Of Cyberwar”
- Thomas Rid – 2013 “Cyber War Will Not Take Place”

3 Copyright © Scott Bradner & Ben Gaucherin 2016

Cyber conflicts – some highlights



- **Indonesia/China - May 1998**
Chinese hackers attack Indonesian government website in response to anti-Chinese riots in Indonesia
- **US/China - May 1999**
Chinese Hackers target US sites in response to accidental bombing by NATO forces of Chinese embassy in Belgrade
- **US/China – 2001**
Chinese fighter jet collides with US aircraft over South China Sea, as a result an estimated 80,000 hackers engage in act of self-defense




4 Copyright © Scott Bradner & Ben Gaucherin 2016

Cyber conflicts – some highlights, contd.



- **Estonia – 2007**
Became independent in 1991
Finland offered antiquated phone switch infrastructure
Estonia's young government politely refused and made move towards building a national digital infrastructure
In March 2007, Estonia had its first national online elections
Estonian government moves the statue of the soldier of Tallinn, pro-soviet supporters take offense
Attacks in 3 waves
April, May 8th and 9th, mid-May
Response - cut off the Internet access to outside the country

5 Copyright © Scott Bradner & Ben Gaucherin 2016

Cyber conflicts – some highlights, contd.

- **Israel/Palestine – December 2008**
During Operation Cast Lead, mass defacement of Israeli and Palestinian websites
- **Iran – June 2009**
Twitter used to DDoS Iranian government websites
- **South Korea/DPRK – July 2009**
DDoS of US and South Korean government and commercial sites allegedly by the DPRK
- **US/China – April 2009**
WSJ reports Joint Strike Fighter project compromised and terabytes of data exfiltrated

6 Copyright © Scott Bradner & Ben Gaucherin 2016

Cyber conflicts – some highlights, contd.

- United States – 2013**
 Syrian Electronic Army hacks AP Twitter account, reports attack on White House, triggered automated trading systems, and sends Dow Jones down 150 points
- Snowden revelations show mass compromise of global infrastructure by the NSA
- Ukraine – 2014**
 Hackers attack the mobile phone service of members of the Ukraine parliament

7 Copyright © Scott Bradner & Ben Gaucherin 2016

Cyber conflicts – some highlights, contd.

- Sony Hack – 2015**
 Large scale compromise of Sony
 Sony cut-off from the Internet
 Over 3.000 machines compromised and needing to be rebuilt
 Massive amounts of data exfiltrated and exposed
 U.S. attributes the attacks to North Korea
 Considered to be hostile actions taken on U.S. ground and directed or executed by foreign government
 U.S. drives to sanctions
 North Korea Internet goes dark (no confirmed attribution)

8 Copyright © Scott Bradner & Ben Gaucherin 2016

U.S. 2016 presidential elections

- Cyber-destabilization or good old "cloak and dagger" intelligence work?
 "Fancy Bear", "Cozy Bear", APT28, etc.
 Spear phishing and email compromise
 Social network "trolling" campaign
 Wikileaks
- Remember, this is about achieving strategic goals...

9 Copyright © Scott Bradner & Ben Gaucherin 2016

Where is this going?



- **Cyber to exploit**
Intelligence, information exfiltration
US China agreement – national espionage ok, economic not ok
- **Cyber to destabilize**
Sherman's war through cyber
Instill doubt in institutions, markets, etc.
- **Cyber to kill**
Cyber to kinetic

10 Copyright © Scott Bradner & Ben Gaucherin 2016

The economics of war




- **Preparing, deploying troops and arming them is an expensive proposition**
Moving the "iron mountain" is slow and expensive
- **By comparison, cyber is extremely cheap, and less "messy"**
- **So we should expect cyber to play a bigger role moving forward**
On its own or in support of other attacks

11 Copyright © Scott Bradner & Ben Gaucherin 2016

Image credits

All drawings and photos by Ben Gaucherin unless noted

Slide#	credit
2	http://www.foxnews.com/tech/2013/04/10/budgetary-cost-cutting-realigns-military-technology-for-cyberwar.html
2	http://www.stonesoft-security.co.uk/solutions/cyber-strategy/
3	http://www.nato.int/cps/en/SID-0C0E4E5F-41945B7B/natolive/news_100906.htm
3	http://www.achevx.com/news/how-hacker-bogeyman-coming-get-you
4	http://www.cnn.com/SPECIALS/1999/china.50/asian.superpower/us.vchina/
4	https://en.wikipedia.org/wiki/File:EP-3_Hainan_Island_2001.jpg
5	http://www.flagpatchshop.com/estonia.html
5	http://sites-of-memory.de/main/tallinnsovietoldier.html
6	http://www.wired.com/2009/06/activists-launch-hack-attacks-on-tehran-regime/

12 Copyright © Scott Bradner & Ben Gaucherin 2016

Image credits

All drawings and photos by Ben Gaucherin unless noted

Slide#	credit
6	http://www.cyberdefensemagazine.com/snowden-reveals-that-china-stole-plans-for-a-new-f-35-aircraft-fighter/
7	http://www.huffingtonpost.com/2013/04/23/syrian-electronic-army-ap-twitter-hack_n_3140849.html
7	https://www.techdirt.com/articles/20150320/08335930383/cisco-shipping-hardware-to-bogus-addresses-to-throw-off-nsa-intercept-and-implant-efforts.shtml
8	http://www.businessinsider.com/sony-hack-should-be-considered-act-of-war-2014-12
8	http://www.elle.com/culture/celebrities/news/a31127/jennifer-lawrence-gender-pay-gap-american-hustle/
8	http://www.businessinsider.com/stops-saying-north-korea-didnt-hack-sony-2014-12
9	https://onsizzle.com/t/memes?since=1477161000%2C3101941

13 Copyright © Scott Bradner & Ben Gaucherin 2016

Image credits

All drawings and photos by Ben Gaucherin unless noted

Slide#	credit
9	http://www.worldinwaceu/cozy-bear/
10	https://en.wikipedia.org/wiki/Swiss_Army_knife
11	https://www.defense.gov/Photos/Essay-View/CollectionID/9904/
11	https://dmna.ny.gov/pressroom/?id=1311090605

14 Copyright © Scott Bradner & Ben Gaucherin 2016

Cyber conflict
Kinetic impact

CSCI E 45b: The Cyber World – part B

1 Copyright © Scott Bradner & Ben Gaucherin 2016

Comparing kinetic and cyber

Source Herb Lin – National Research Council



Kinetic	Cyber
Space of conflict largely separate from civilians	Space of conflict is where civilians live and work
Offense – defense technologies often in rough balance	Given time, offense always beats defense
Attribution to adversary presumed	Attribution hard, slow, uncertain
Capabilities of non-state actors relatively small	Capabilities of non-state actors relatively large
Significance of distance large	Significance of distance minimal
National boundaries important	National boundaries irrelevant
Clear lines between attack and spying as security threats	Attack and spying hard to distinguish
Effects reasonably predictable	Effects hard to predict or control

Consequence: much of what we know about kinetic conflict cannot be applied directly to cyber conflict

2 Copyright © Scott Bradner & Ben Gaucherin 2016

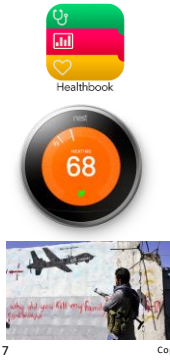
Cross over from cyber to kinetic

- Late 80's - Making hard drives "walk across the floor"
- You could also ask to read an un-reachable sector of a disk
- 1982 Urengoy–Surgut–Chelyabinsk pipeline



3 Copyright © Scott Bradner & Ben Gaucherin 2016

Killing people with cyber weapons



- Individuals with technology in/on them that can be subverted
e.g., wirelessly accessible heart defibrillator, wirelessly accessible insulin pumps, Apple iWatch and HealthBook
- Compromising control systems of life essential or life threatening structures
e.g., water filtering systems, power systems during extreme weather, nuclear plant control systems
- Cyber as decision maker
Algorithms directing drones

7 Copyright © Scott Bradner & Ben Gaucherin 2016

Image credits

All drawings and photos by Ben Gaucherin unless noted

Slide# credit

3

<http://www.techtimes.com/articles/51295/20150508/merombertik-a-deadly-virus-that-will-self-destruct-and-destroy-your-computer-once-you-detect-it.htm>

3

https://en.wikipedia.org/wiki/Urengoy%E2%80%993Pomary%E2%80%93Uzhgorod_pipeline

4

<http://www.wired.com/2008/04/industrial-cont/>

5

<http://www.isssource.com/stuxnet-report-ii-a-worm%E2%80%99s-life/>

5

<https://commons.wikimedia.org/wiki/File:S7300.JPG>

6

<https://commons.wikimedia.org/wiki/File:S7300.JPG>

7

<http://www.appsrumors.com/news-rumors/ios-8-healthbook-app-visualized-new-mockups/>

7

<https://store.nest.com/product/thermostat/>

7

<http://www.theguardian.com/commentisfree/2016/feb/2>


8

Cyber conflict
Key terms and concepts

CSCI E 45b: The Cyber World – part B

1 Copyright © Scott Bradner & Ben Gaucherin 2016


Activities



- **Cybercrime**
Use of cyber instruments for criminal purposes
- **Hacktivism**
Use of cyber instruments for political or ideological purposes
- **Cyber exploitation and cyber espionage**
Penetration of an adversary for the purpose of exfiltration (but not defiling) of data

2 Copyright © Scott Bradner & Ben Gaucherin 2016

Activities, contd.



- **Cyber attack**
Deliberate disruption of a computer system, and or of its supported functions outside of cyberspace
Can be an adjunct to other forms of attack
Syria 2007 - Israeli cyber attacked Syrian air defense before bombing nuclear infrastructure
Or only form of attack
Generalized - Estonia 2007
Customized - Stuxnet 2010
- **In the US:**
Title 10 vs. Title 50 operations

3 Copyright © Scott Bradner & Ben Gaucherin 2016

(Passive) defense



- DoD definition – “*measures taken to reduce the probability of and to minimize the effects of damage caused by hostile action without the intention of taking the initiative*”
Examples: firewalls, Anti Virus, IDS, audits, etc.
- Parameters:
 - Within one’s jurisdiction
 - Reaction to hostile event
 - Hostile is recognizable

4

Copyright © Scott Bradner & Ben Gaucherin 2016

Active defense



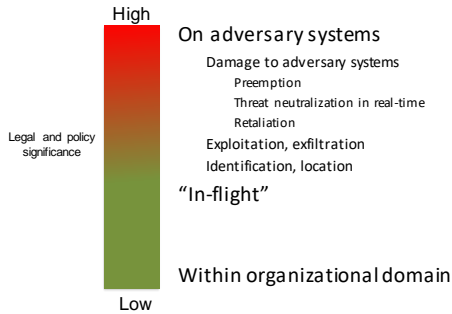
- Confused concept
- DoD’s definition
“Active cyber defense is DoD’s synchronized, real-time capability to discover, detect, analyze, and mitigate threats and vulnerabilities.”
- Not offensive, but darn near it
- Anything that is not passive defense
 - Pro-active
 - Outside one’s jurisdiction
 - Harmful

5

Copyright © Scott Bradner & Ben Gaucherin 2016

Hierarchy of Active Defense

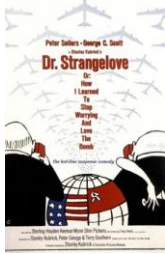
From Herb Lin



6

Copyright © Scott Bradner & Ben Gaucherin 2016

Deterrence



- Deterrence allows one actor to discourage actions from another actor
 - Both sides need to know
- Keys elements of deterrence:
 - Who is being deterred
 - From doing what
 - Using what threat

7

Copyright © Scott Bradner & Ben Gaucherin 2016

Deterrence, contd.



- In the Nuclear days deterrence was Mutually Assured Destruction (MAD)
- No real equivalent in cyber, or is there?...
 - Assuming attribution is accurate enough
 - Response does not need to be cyber
 - Cyber can be a response
 - Most countries "don't know what they don't know" about their own cyber vulnerabilities
 - An advanced cyber response does not require a lot of resources/people

"If you really want to protect your network you have to know your network, including all the devices and technology in it. In many cases we know networks better than the people who designed and ran them."
 Rob Joyce, NSA Head Hacker

8

Copyright © Scott Bradner & Ben Gaucherin 2016

Image credits

- All drawings and photos by Ben Gaucherin unless noted
- | Slide# | credit |
|--------|---|
| 2 | http://www.svtuition.org/2013/02/how-cyber-criminals-steal-money.html |
| 3 | http://www.slate.com/articles/technology/future_tense/2011/08/what_is_cyberwachtml |
| 4 | http://marineparents.com/marinecorps/publications.asp |
| 5 | http://www.politico.com/story/2013/10/department-of-defenses-revolving-door-in-full-swing-098813 |
| 7 | https://en.wikipedia.org/wiki/Dr_Strangelove |
| 8 | http://www.gostrategic.org/blog/the-genius-of-the-madness-of-mutually-assured-destruction/ |

9


Copyright © Scott Bradner & Ben Gaucherin 2016

Cyber conflict
Attribution

CSCI E 45b: The Cyber World – part B

1 Copyright © Scott Bradner & Ben Gaucherin 2016


Attribution
From Herb Lin



- If A is trying to attack C
- A can hijack B and use B to attack C
 - C can filter out B
 - But C won't easily be able to identify A
- And to make this more complicated A hijack (or rents) more than one machine (e.g. botnet) that can be distributed around the globe: B₁, B₂, B₃, B...

2 Copyright © Scott Bradner & Ben Gaucherin 2016

Attribution, contd.
From Herb Lin




- The three general meanings of attribution
 1. Machine or machines
 2. Human operator
 3. Party ultimately responsible for the actions of the human operator
- **P** itself can be viewed in different ways:
 - Where the human operator is when launching the attack
 - The nation under whose authority the human operator falls
 - The entity under whose auspices the human operator acted

3 Copyright © Scott Bradner & Ben Gaucherin 2016

Different levels of attribution

From Herb Lin



- Stopping the pain – **M**
- Legal prosecution – **H (or P)**
- Deter future acts – **H or P**

4 Copyright © Scott Bradner & Ben Gaucherin 2016

Different levels of attribution


From Herb Lin

Very hard or impossible if..	But perpetrators sometimes..
Perpetrator's techniques are unprecedented	... use techniques/software seen before
Perpetrator's actions have left no clues	... make tradecraft mistakes that leave behind clues, e.g., use of dating profile in code or reuse an IP address
Perpetrator has maintained perfect operational security (no one else knows)	... discuss their plans on insecure communications media or receive help (such as intelligence information) from sources who are not careful
Perpetrator's motivations or demands are unknown	... do take action in response to political circumstances (nations)
Time scales required are short	... can be attacked "at times and places and in manners of our choosing"

All-source attribution vs Technical attribution

5 Copyright © Scott Bradner & Ben Gaucherin 2016

Beyond technical attribution



- The NSA says they can do attribution with a high degree of certainty – what does that mean?
Perfect visibility into all networks or deceitful, delusional...
- Discovering who did it is hard, but legal proof is much harder
- Assigning political responsibility is a political act, not a technological problem

6 Copyright © Scott Bradner & Ben Gaucherin 2016

Image credits

All drawings and photos by Ben Gaucherin unless noted

Slide#	credit
2	http://uvmzombies.blogspot.com/2013/02/computer-zombies.html
3, 4	http://www.wisegeek.com/what-is-a-zombie-computechtm
6	http://breakingdefense.com/tag/cyber-command/page/3/

7


Copyright © Scott Bradner & Ben Gaucherin 2016

Cyber conflict
Conflict resolution

CSCI E 45b: The Cyber World – part B

1 Copyright © Scott Bradner & Ben Gaucherin 2016

The five stages of conflict
from Herb Lin




Herb Lin

- Conflicts go through generic sets of stages:
 1. Preparation
 2. Initiation of hostilities
 3. Escalation
 4. De-escalation
 5. Termination

2 Copyright © Scott Bradner & Ben Gaucherin 2016

Escalation makes de-escalation difficult
from Herb Lin



Three types of escalations:

- Deliberate escalation**
Carried out for specific purpose: getting the upper hand, showing intent, motivation, etc.
- Accidental escalation**
Unilateral or mutual misunderstanding
- Catalytic escalation**
A third party provokes two parties to engage in conflict

- In cyber, how do you figure out which (if any) escalation is happening?

3 Copyright © Scott Bradner & Ben Gaucherin 2016

Elements of termination

from Herb Lin



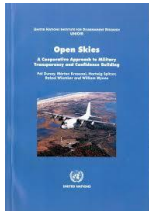
- Presumes there is an interest in terminating conflict
- Need a trustworthy mechanism for parties involved to negotiate terms
 - How do you do this if communication channels have been compromised
- Clear understanding of the terms for termination
 - How to know where cyber weapons have been deployed?
 - One term can be capitulation

4

Copyright © Scott Bradner & Ben Gaucherin 2016

Elements of termination, contd.

from Herb Lin



- Assurance that parties will adhere to the terms
 - Difficulty in determining "acceptable levels of hacking"
 - Patriotic hackers still continuing
- Capabilities for each parties to verify compliance
 - How to verify cyber cease-fire?
 - Overt/cooperative intelligence not likely to be believed
 - Covert intelligence to verify can be misread as provocation
 - Attribution still a problem

5

Copyright © Scott Bradner & Ben Gaucherin 2016

Image credits

All drawings and photos by Ben Gaucherin unless noted

Slide# credit

2 <http://cisac.fsi.stanford.edu/news/herb-lin-wants-put-stanford-forefront-cyber-policy-and-security>

3 <http://www.cominwork.com/weekly/2015-09-21/productivity/conflict-escalation-in-communication>

4 <http://www.wolfsonian.org/explore/collections/souvenir-du-wagon-du-mar%C3%A9chal-foch-dans-lequel-fut-sign%C3%A9-larmistice-du-11-nove-0>

5 <http://www.unidic.org/files/publications/pdfs/open-skies-a-cooperative-approach-to-military-transparency-and-confidence-building-319.pdf>

6


Copyright © Scott Bradner & Ben Gaucherin 2016

Cyber conflict
Cyber weapons and zero days

CSCI E 45b: The Cyber World – part B


1 Copyright © Scott Bradner & Ben Gaucherin 2016

Cyber weapons




Ralph Langner

- **Cyber Weapon**
Ralph Langner - A software artifact designed to cause physical harm (to objects, people, or the environment)
Wiktionary - Computer hardware or software used as a weapon in cyberwarfare.
- **Code is inherently neither good nor bad**
Bits are “dual use”
- **The danger is contextual**
Code in the hands of a pen-tester vs. a malicious actor



2 Copyright © Scott Bradner & Ben Gaucherin 2016

Cyber weapons, contd.



- **Require three components:**
Access
Vulnerability
Payload/exploit
- **Low barrier to entry compared to traditional weapons**
- **Cyber weapons are like “drug deals”**
Underground market
Cannot be successfully regulated

3 Copyright © Scott Bradner & Ben Gaucherin 2016

Cyber weapons, contd.

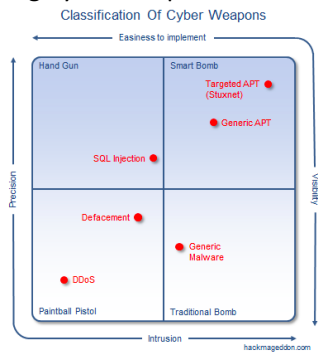


- Some cyber weapons are for attack, others for espionage
Title 10 v. Title 50
- Traditional weapons controls approaches completely unable to deal with cyber weapons
 - Utilizes tools that are available to everyone
 - They are non-physical
 - How do you keep track of things that do not have physical manifestations?

4

Copyright © Scott Bradner & Ben Gaucher in 2016

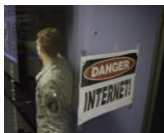
Mapping cyber weapons



5

Copyright © Scott Bradner & Ben Gaucher in 2016

Developing targeted cyber weapons



- Identify target
- Perform reconnaissance on the target
- Find/buy vulnerabilities and exploits based on reconnaissance (e.g., Zero Days)
 - Methods on how to use vulnerabilities are better than the vulnerabilities themselves
- Develop/customize exploits, delivery, and activation mechanisms

6

Copyright © Scott Bradner & Ben Gaucher in 2016

The known unknowns



- Report from NSS Labs 12/2013
"...on *any given day* over the past three years, privileged groups have had access to at least 58 vulnerabilities targeting Microsoft, Apple, Oracle, or Adobe."
...these vulnerabilities remain private for an average of 151 days.
Specialized companies are offering zero day vulnerabilities for subscription fees

25 zero days per year for USD \$2.5 million

10

Copyright © Scott Bradner & Ben Gaucherin 2016

The market for zero days

- Who sells?
Individuals, exploit brokers
- Who buys?
Organized crime, governments, government contractors, etc.

ADOBE READER	\$5,000-\$30,000
MAC OSX	\$20,000-\$50,000
ANDROID	\$30,000-\$60,000
FLASH OR JAVA BROWSER PLUG-INS	\$40,000-\$100,000
MICROSOFT WORD	\$50,000-\$100,000
WINDOWS	\$60,000-\$120,000
FIREFOX OR SAFARI	\$60,000-\$150,000
CHROME OR INTERNET EXPLORER	\$80,000-\$200,000
IOS	\$100,000-\$250,000

Source: fobes.com 3/29/2013

11

Copyright © Scott Bradner & Ben Gaucherin 2016

Pricing zero days



- Size of target population
OS X zero days less expensive than Windows ones
- Complexity of security system to overcome
iOS more complex and therefore more pricey than Android
- Local market dynamic
Prices in China are lower because of the number of hackers identifying zero days
- More expensive if requirement of "exclusive use"

12

Copyright © Scott Bradner & Ben Gaucherin 2016

Models of disclosure

From Ryan Ellis



Ryan Ellis

- **Limited** disclosure
Disclose to technology producer, usually for a price. The technology producer in turn can develop a patch to address the issue
Pro - Can get money
Con - Limited or no bragging rights
Con - Time lag between discovery and patch can be high

13

Copyright © Scott Bradner & Ben Gaucherin 2016

Models of disclosure

From Ryan Ellis



- **Full** disclosure
Public disclosure, often times at big security conferences. As a result the technology producer is forced into creating a patch very quickly.
Pro - Time lag between discovery and patch is low
Con - Won't get paid
Con - Considered reckless
Con - Exposure to legal liability

14

Copyright © Scott Bradner & Ben Gaucherin 2016

Models of disclosure

From Ryan Ellis



- **Coordinated** disclosure
Notify technology provider and government oversight.
Government oversight publicly discloses vulnerability after X days
e.g., security researcher pre-announces, to vendor and CERT, when they are going to make the information public
- Or, **don't disclose** and sell the vulnerability to a third party

15

Copyright © Scott Bradner & Ben Gaucherin 2016

Patching



- Patching allows software manufacturers to fix problems with their software – some of them critical problems such as Zero Days
Therefore, Zero Days are “one time use” weapons
- The Speed vs. Quality dilemma
Apply the patch quickly and take the risk that it may introduce new vulnerabilities or take the time to validate

16

Copyright © Scott Bradner & Ben Gaucherin 2016

Patching, contd.

- Patching can be a powerful cyber weapon/vulnerability delivery mechanism
Do you trust Adobe, Microsoft, McAfee, Symantec, etc.?



17

Copyright © Scott Bradner & Ben Gaucherin 2016

Image credits

All drawings and photos by Ben Gaucherin unless noted

Slide#	credit
2	http://www.langner.com/en/about/
2	https://blog.zogdigital.com/tag/google-webmaster-guidelines/
3	http://www.defenseone.com/technology/2015/05/army-shopping-cyber-weapons/113185/
4	http://clui.org/ludb/site/titan-missile-museum
5	http://spuniknews.com/military/2015/10/7/1029738101/pentagon-cyber-weapons-capable-killing.html
6	https://www.linkedin.com/pulse/apt-advanced-persistent-threats-nutshell-sameera-de-alwis-phd
7	http://www.hackmageddon.com/2012/04/22/what-is-a-cyber-weapon/
8	http://www.pcworld.com/article/217016/hackers_toolkit_returns_symantec_says.html
9	http://www.hitekpals.com/what-is-a-zero-day-exploit/

18

Copyright © Scott Bradner & Ben Gaucherin 2016

Image credits, contd.

All drawings and photos by Ben Gaucherin unless noted

Slide#	credit
10	https://twitter.com/nsslabs
12	http://community.norton.com/en/blogs/horton-protection-blog/hackingteam-data-dump-leads-adobe-zero-day-discovery
13	http://belfercenterksg.harvard.edu/experts/2698/ryan_ellis.html
14	https://www.defcon.org/html/defcon-18/dc-18-news.html
15	http://www.sis.pitt.edu/lersais/resources/external.php
16	http://redlance.com/wp/support-is-ending-for-windows-xp-what-does-this-mean-for-you/
17	http://thehackmews.com/2015/08/windows-update-malware.html

Cyber conflict
Conclusion

CSCI E 45b: The Cyber World – part B

1 Copyright © Scott Bradner & Ben Gaucherin 2016


Final thoughts



- Still early days, and fast evolving
- Cyber potential for kinetic impact, economic and government disruption proven possible

2 Copyright © Scott Bradner & Ben Gaucherin 2016

Final thoughts, contd.



- Defense establishment still trying to map cyber to nationalistic and physical models

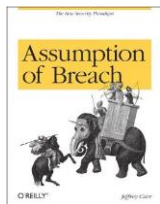
Understanding of the basic mechanics of cyber space seem to be lacking – it's new, it'll take a while

Some multi-national collaboration starting for intelligence and cyber crime fighting

Not always to good ends – Five Eyes

3 Copyright © Scott Bradner & Ben Gaucherin 2016

Final thoughts, contd.



- Moving to a new mindset:
Assumption of breach

4

Copyright © Scott Bradner & Ben Gaucherin 2016

Image credits

All drawings and photos by Ben Gaucherin unless noted

Slide# credit

2 <https://www.linkedin.com/pulse/case-cyber-war-kosovo-conflict-nikola-milo%C5%A1evi%C4%87>

3 https://en.wikipedia.org/wiki/The_Pentagon

4 <http://www.amazon.co.uk/Assumption-Breach-The-Security-Paradigm/dp/1449340628>

5

Copyright © Scott Bradner & Ben Gaucherin 2016
