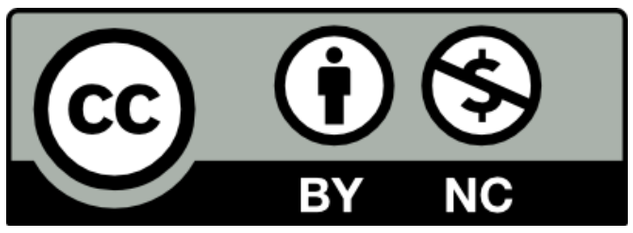
Hack-Back

Steven M. Bellovin
https://www.cs.columbia.edu/~smb



Why Hack Back?

- Tracking
- Inability of governments to protect people and institutions?
- Self defense?
- Undesirability of governmental action?
- All of the above?

Tracking Hackers

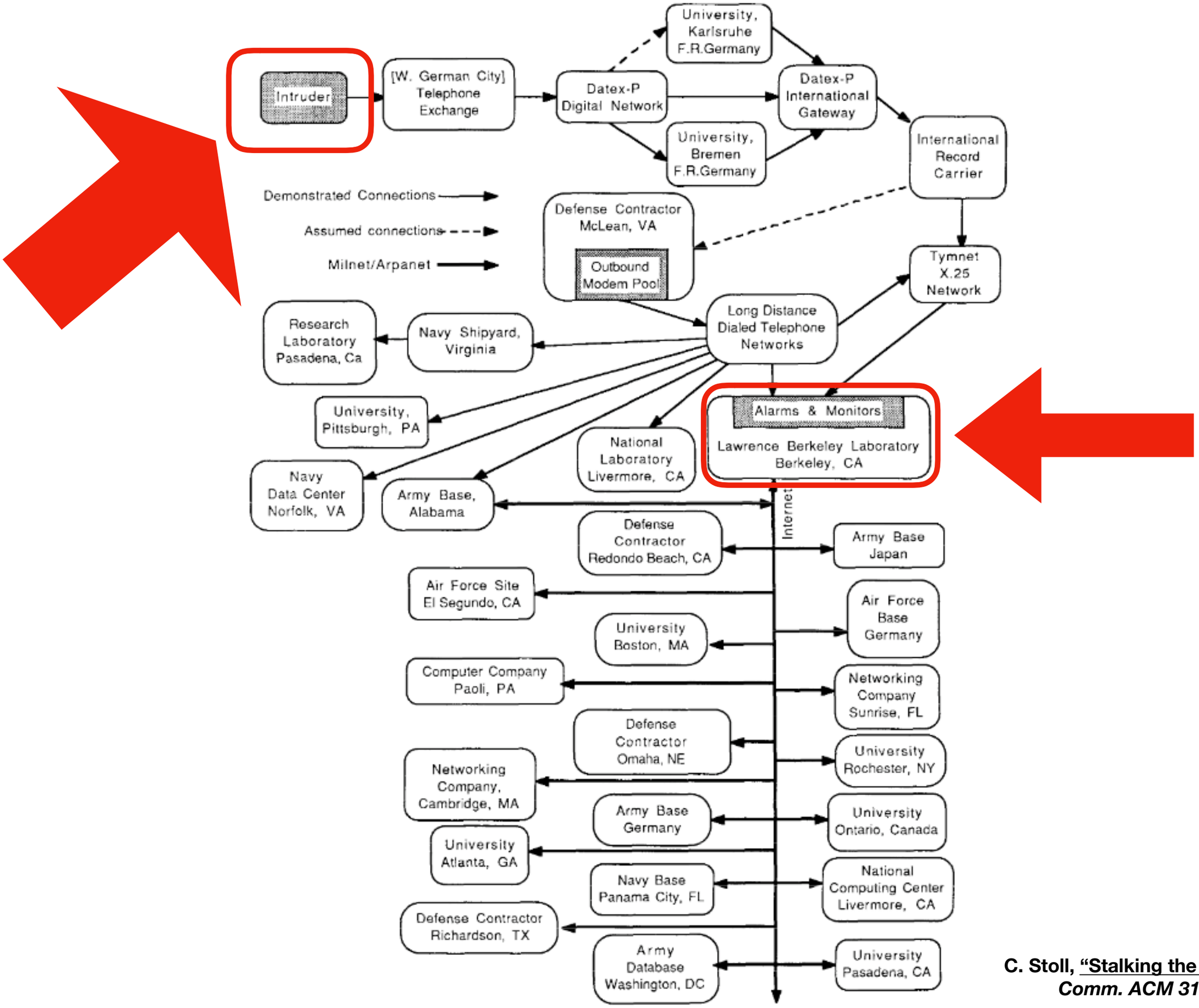
- Attackers have *always* used stepping stones
- But all you see is the immediate source of the attack
- The path can be complex!

The Cuckoo's Egg

- In 1986, Cliff Stoll, an astronomy grad student, was working for the Berkeley Computer Center and noticed a $.75 accounting discrepancy

- Eventual outcome: West German hackers were trying to steal tech and defense information to sell to the Stasi to get money to buy cocaine

- After tracing the attack, Stoll got a technical paper ("Stalking the Wily Hacker"), a book ("The Cuckoo's Egg"), and an episode of Nova ("The KGB, the Computer, and Me")
  - And a video interview: https://www.c-span.org/video/?10122-1/the-cuckoos-egg



C. Stoll, "Stalking the Wily Hacker",
Comm. ACM 31:5, 1988

Tracing is Hard

"We did not know who to contact in the law-enforcement community. At first, assuming that the intruder was local, our district attorney obtained the necessary warrants. Later, as we learned that the intruder was out of state, we experienced frustration in getting federal law-enforcement support. Finally, after tracing the intruder abroad, we encountered a whole new set of ill-defined interfaces between organizations."

—Cliff Stoll (1988)

Tracing is Hard

"I didn't realize it would take weeks to get a trace. I wasn't sure exactly what CERT does in these circumstances. Do they call The Feds? Roust a prosecutor? Activate an international phone tap network?"

—Bill Cheswick (1992)

Warrants

“Hey, we need a telephone line traced.” “Got a search warrant?” “No, do we need one?” “We won’t trace without a warrant.” (Cliff Stoll)

- Warrants require judges and lawyers
- Warrants are limited to particular jurisdictions
- And then there’s international hacking:

  “The message from Germany read: “The German State Prosecutor needs to contact high-level U.S. criminal justice persons so as to execute proper search warrants. The Bundespost cannot move until officially notified by a high-level U.S. criminal office.”

Traceback by Hack-Back?

- Observation: some Internet site is attacking you using vulnerability X from site Y
- Hypothesis: site Y also has vulnerability X
- Experiment: you attack site Y using X, to trace the attack from there
- Iterate as needed

It's Been Done

- 1994: Hackers compromised every unclassified system at Griffiss Air Force Base (NY) and were attacking many other military systems from there

- The Air Force Information Warfare Center had a hack-back tool

- They wanted to go after the attackers—by hacking back along the chain

- But…

Legality

- 18 U.S.C. §1030(a)(5)(C) “Whoever… intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss” is guilty, etc.

- 18 U.S.C. §1030(b): “Whoever conspires to commit or attempts to commit an offense under subsection (a)”, etc.

- But: 18 U.S.C. §1030(f): “This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States"

In Other Words

- Hack-back is *generally* illegal
- Law enforcement *may* be able to do it, if their activity is "lawfully authorized"
- The Air Force Information Warfare Center cannot
- But: they could *if* they were supervised by the Office of Special Investigations and/or DoJ

Self-Defense

- What about self-defense?
- Bill Cheswick and me (1994):

"Some people have suggested that in the event of a successful attack in progress, we might be justified in penetrating the attacker's computers under the doctrine of self-defense. That is, it may be permissible to stage our own counterattack in order to stop an immediate and present danger to our own property. The legal status of such an action is quite murky, although analogous precedents do exist."

- Law enforcement isn't that good at tracking down cybercriminals

"Well regulated Hacking, being necessary to the security of a free State"…?

Massachusetts Law

"In Commonwealth v. Donahue, 148 Mass. 529, 531, 20 N.E. 171 (1889), the court held that 'a man may defend or regain his momentarily interrupted possession by the use of reasonable force, short of wounding or the employment of a dangerous weapon.'" (Commonwealth v. Haddock, 46 Mass. App. Ct. 246 (1998))

But What About New Jersey?

b. Limitations on justifiable use of force in defense of [property].

(1) Request to desist. The use of force is justifiable under this section only if the actor first requests the person against whom such force is used to desist from his interference with the property, unless the actor reasonably believes that:

(a) Such request would be useless;

NJ Rev Stat § 2C:3-6 (2013)

But Intangible Property?

- Laws on use of “force” to protect property are complex
- They *may* permit you to act to stop an intrusion
- Is hacking back really the best way to *stop* an ongoing attack?
- And what about to track one back?
- Besides: there’s an explicit Federal law that doesn’t have a self-defense exception.

Law in General

- We are, generally speaking, not a vigilante society
- We prefer that people rely on law enforcement
- As noted, the police are not that good at dealing with cybercrime, especially in realtime
- In the physical world, we rely on defenses (e.g., door locks) and deterrence (e.g., police)—but in the cyber world, we have only the former, and our defenses aren't that good (but neither are most locks)

Maybe Cyberspace is Different

- On the other hand—why should physical space rules apply to cyberspace?

- Where is “the Internet”?

Barlow's "Declaration of the Independence of Cyberspace"

"Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather."

...

"Cyberspace does not lie within your borders."

...

"Your legal concepts of property, expression, identity, movement, and context do not apply to us. They are all based on matter, and there is no matter here."

(https://www.eff.org/cyberspace-independence)

Do “Borders” Matter?

- A Congressional power under Article I of the US constitution: “To define and punish Piracies and Felonies committed on the high Seas, and Offences against the Law of Nations”

- “Universal jurisdiction”: “Universal criminal jurisdiction is the principle of international law that permits any nation to prosecute certain serious international crimes, regardless of where they are committed, by whom or against whom, or any other unique tie to the prosecuting nation” (https://www.americanbar.org/groups/crsj/publications/human_rights_magazine_home/human_rights_vol31_2004/winter2004/irr_hr_winter04_universal/)

- Should this principle apply to the Internet?

Maybe this Principle Should Apply

- There are no clear national boundaries
  - What is the equivalent of the twelve mile limit?
- The problem manifests itself without regard to attacker or victim location
- It's hard to catch the offenders
- But: universal jurisdiction applies to *governments*, not to individuals
- Is that right, today, for the Internet?

But There Are Governments

- Why should the existence of a new technology make governments disappear?

- Why should you want government to disappear? “Rabbi Chanina, the Deputy High Priest, said: Pray for the welfare of the government, For were it not for the fear of it, One person would eat the other alive.” (Pirkei Avot, ~200 CE)

Do We Want Pure Vigilantism?

- What are the *norms* we want in cyberspace?

- Hacking is illegal *because* there are norms—and laws

“A Man for All Seasons”

William Roper: So, now you give the Devil the benefit of law!

Sir Thomas More: Yes! What would you do? Cut a great road through the law to get after the Devil?

William Roper: Yes, I’d cut down every law in England to do that!

Sir Thomas More: Oh? And when the last law was down, and the Devil turned ‘round on you, where would you hide, Roper, the laws all being flat? This country is planted thick with laws, from coast to coast, Man’s laws, not God’s! And if you cut them down, and you’re just the man to do it, do you really think you could stand upright in the winds that would blow then? Yes, I’d give the Devil benefit of law, for my own safety’s sake!

But What of Norms for *Governments?*

- Governments hack
  - Espionage
  - “Preparing the battlefield”
  - Cyberwar—but we’ve never had one
- International law disallows war, but tacitly permits espionage—and is silent on preparing the battlefield

Can Governments Hack Back?

- Against another government, absolutely
  - The private sector does not have its own surface-to-air missiles to protect against other countries
- What if it's a private actor?
  - Is that law enforcement exercising long-arm jurisdiction? Universal jurisdiction?
- What if it's a private actor that's tolerated by some government?
- What if it's a private actor working on behalf of a government?

Letters of Marque and Reprisal

Letter of marque

A license to fit out an armed vessel and use it in the capture of enemy merchant shipping and to commit acts which would otherwise have constituted piracy.

Under the US constitution, only Congress can issue letters of marque

But some countries seem to be blessing activities by their own “patriotic” hackers

Historical Problems

"This method of commerce destruction was adopted by all nations from the earliest times until the 19th century, but it frequently proved impossible to restrain the activities of privateers within the legitimate bounds laid down in their commissions or letters of marque. Hence, in earlier times, it was often difficult to distinguish between privateers, pirates, corsairs, or buccaneers, many of whom sailed without genuine commissions."

Encyclopedia Britannica, *https://www.britannica.com/topic/letter-of-marque*

International Law

"In international law, privateering is prohibited by the 1856 Paris Declaration Respecting Maritime Law. Though the U.S. is not a signatory, it has in effect abided by the Declaration and has not commissioned a privateer since the War of 1812. However, while the 1856 Paris Declaration prohibits privateering, it neither defines what constitutes a privateer nor explicitly prohibits the issuance of letters of marque. Letters of marque have historically been issued to private vessels for activities other than privateer-like commerce raiding, examples include anti-piracy and self-defense. Consequently, although letters of marque have fallen into disuse, they are not explicitly prohibited by international law."

National Security Law Brief, http://nationalsecuritylawbrief.com/2018/03/23/not-without-a-letter-of-marque-constitutional-requirement-regarding-the-use-of-armed-private-military-contractors-at-sea

International Norms on Hack-Back

"Non-state actors should not engage in offensive cyber operations and state actors should prevent and respond to such activities if they occur."

Global Commission on the Stability of Cyberspace, https://cyberstability.org/wp-content/uploads/2018/11/Additional-Note-to-the-Norm-Against-Offensive-Cyber-Operations-by-Non-state-Actors-Norm-Package-Singapore.pdf

But: this isn't international *law*

Why?

- Attribution is very hard
  - Only a very few parties actually have the capability
  - What if you get it wrong and attack an innocent party?
  - Attacking *arbitrary* systems without causing damage is hard—and given the use of stepping stones, many of the targets will be innocent
- Society is based on the premise that governments have a monopoly on lawful use of “force”

Attribution

- Early: IP address only—but the problem of stepping stones was obvious even then
- Other intelligence sources—HUMINT, SIGINT, etc. Hard if you're not a government agency…
- Modus operandi: look for common tools, techniques, libraries
- Infrastructure: look for common servers for reporting, command and control, etc.
- Internal clues: language, dates, etc
- Politics: who stands to gain?
- Commercial: Follow the money

Errors in Attribution

- False flag operations
- Following only positive clues
- Overestimating the sophistication necessary; underestimating others' capabilities
  - SOLAR SUNRISE: They told the President it was Iraq, but it was California teenagers and an Israeli hacker
- Mistaking the technical source for the party behind it

Attribution and Hack-Back

- If your attribution is doubtful, you can't hack back
  - "Lack of attribution, in turn, leads to paralysis in active defense responses to the attack. If the DoD is not sure precisely who is attacking it, legal implications concerning responses cannot be easily calculated." (Healy, *A Fierce Domain*)
- If your attribution is incorrect, you're counter-attacking against the wrong party
- Even successful, correct attributions take time, which means that the hack-back is revenge, rather than stopping the attack

Where Are We?

- Current US law and developing international norms say that private actor hack-back is improper
  - At best, it might be accepted to halt an attack in progress
- There is increased interest in legalizing it, due to frustration with increasingly bold hackers—but law enforcement is getting better
- Governments seem to do it to each other sometimes, but never overtly
  - After North Korea hacked Sony, Pres. Obama said the US would respond “in a place and time and manner that we choose” (Dec. 19)
  - Dec. 21-22: North Korea was suddenly offline
  - BBC: “Officials would not comment on any US involvement in the current outages.”

Questions?

(these slides at https://www.cs.columbia.edu/~smb/talks/tufts-hackback.pdf)