Cybersecurity and Emerging Global Threats

Steven M. Bellovin

https://www.cs.columbia.edu/~smb

CC BY NC

Nuclear Weapons Are *Hard*

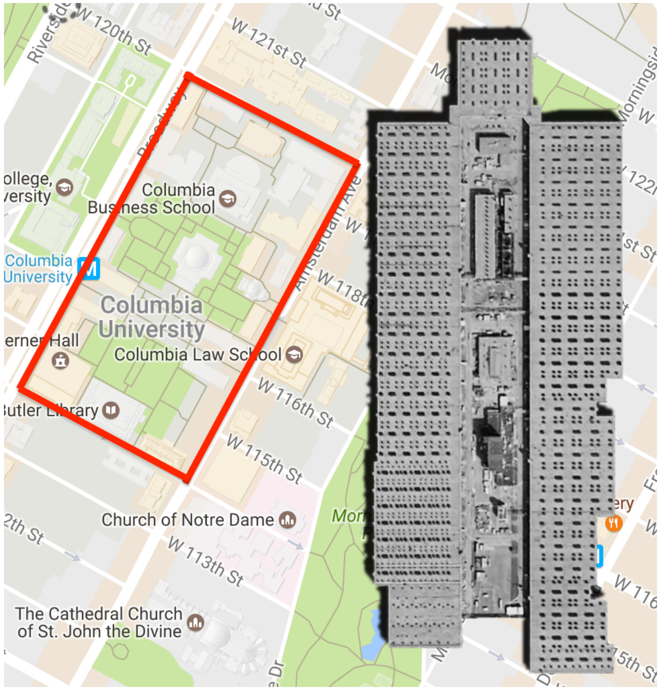
- The science is very well known, and most of it has been known since 1945.
  - The biggest "secret" in 1945: that a bomb could be built at all.
- Most of the engineering issues are also well understood.
- Why are there so few nuclear states? Actually building atomic weapons is *expensive.*

Enriching Uranium

- The uranium enrichment effort was about 63% of the cost of the Manhattan Project (http://blog.nuclearsecrecy.com/2013/05/17/the-price-of-the-manhattan-project/)

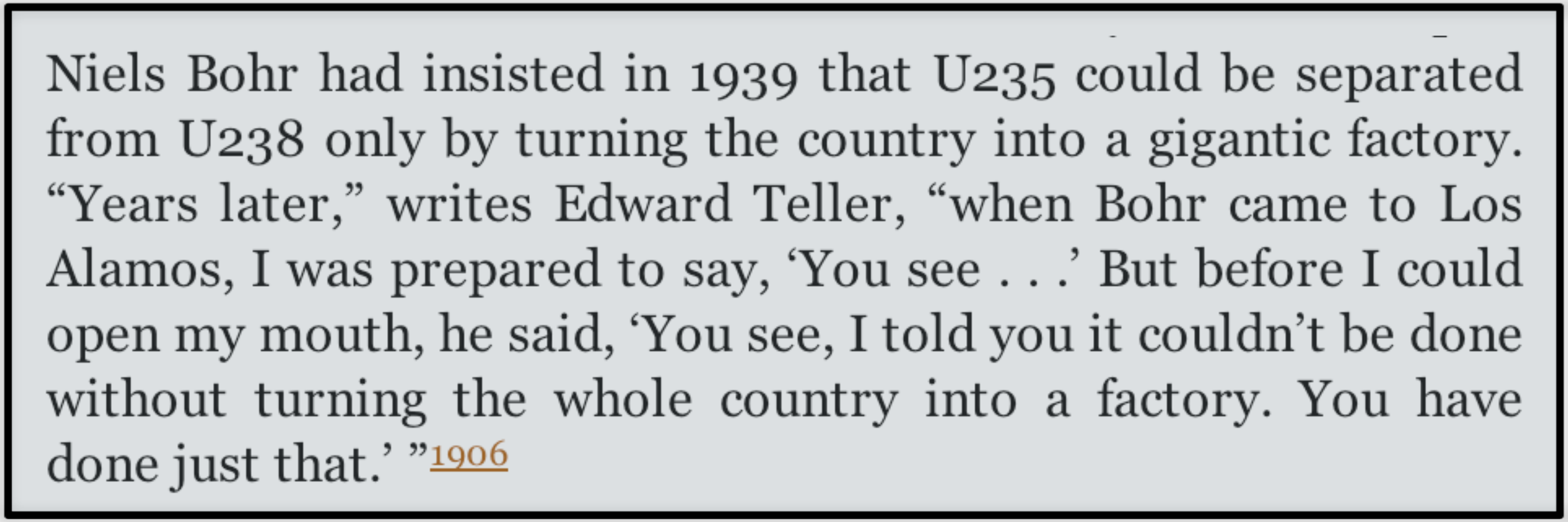
- The Oak Ridge K-25 plant, shown in scale at right, was just one part of the enrichment effort

- (Los Alamos was only about 7%, but it has all the name recognition…)



http://blog.nuclearsecrecy.com/2013/05/24/inside-k-25/

Producing Uranium-235



Niels Bohr had insisted in 1939 that U235 could be separated from U238 only by turning the country into a gigantic factory. “Years later,” writes Edward Teller, “when Bohr came to Los Alamos, I was prepared to say, ‘You see . . .’ But before I could open my mouth, he said, ‘You see, I told you it couldn’t be done without turning the whole country into a factory. You have done just that.’ ”[1906]

Richard Rhodes, *The Making of the Atomic Bomb*

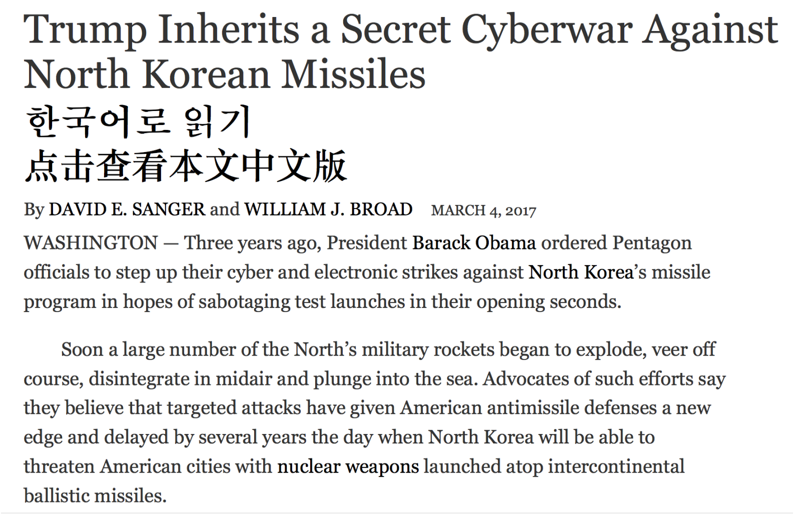
Enter Cyber

- Computers are *cheap* and getting cheaper
- A modest data center is much smaller than a campus, and doesn’t consume huge amounts of electricity
- All you need is knowledge and experience

What's At Risk?

- Banking
  - The US military had plans to hack Iraq's banking system during Gulf War II to freeze Saddam Hussein's funds
- Telecommunications
  - They did attack Iraq's phone network, which affected neighboring countries, too
- More: fuel, transportation, most industries, etc.

It’s Cyber All the Way Down



Trump Inherits a Secret Cyberwar Against North Korean Missiles

한국어로 읽기

点击查看本文中文版

By DAVID E. SANGER and WILLIAM J. BROAD MARCH 4, 2017

WASHINGTON — Three years ago, President Barack Obama ordered Pentagon officials to step up their cyber and electronic strikes against North Korea’s missile program in hopes of sabotaging test launches in their opening seconds.

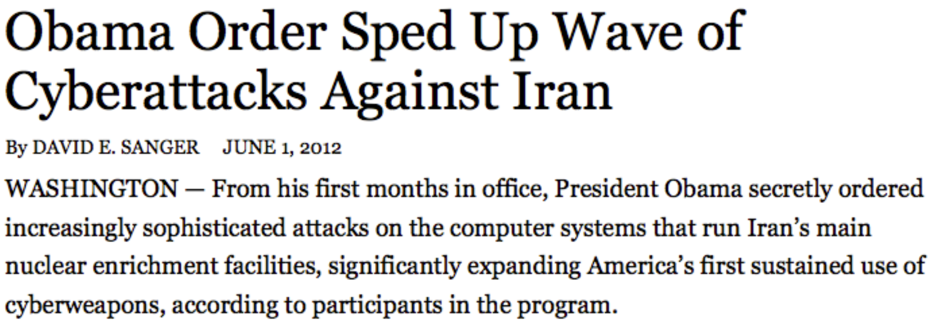
Soon a large number of the North’s military rockets began to explode, veer off course, disintegrate in midair and plunge into the sea. Advocates of such efforts say they believe that targeted attacks have given American antimissile defenses a new edge and delayed by several years the day when North Korea will be able to threaten American cities with nuclear weapons launched atop intercontinental ballistic missiles.

https://www.nytimes.com/2017/03/04/world/asia/north-korea-missile-program-sabotage.html

- Today, *everything* has a computer component
- Computer attacks can disable physical infrastructure
- A car is a mobile datacenter; an airplane is a flying datacenter

Stuxnet Woke Up the World

- Stuxnet (apparently developed by the US and Israel) successfully attacked Iran's nuclear program
- Iran was taken aback—but they quickly realized that they could do it, too
- They rapidly developed their own offensive capability
- So did North Korea



Obama Order Sped Up Wave of Cyberattacks Against Iran

By DAVID E. SANGER JUNE 1, 2012

WASHINGTON — From his first months in office, President Obama secretly ordered increasingly sophisticated attacks on the computer systems that run Iran's main nuclear enrichment facilities, significantly expanding America's first sustained use of cyberweapons, according to participants in the program.

http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html

North Korea?

- The older major cyber powers—the US, Russia, China, Israel, France—are all high-tech countries
- Iran has long had an excellent educational system
- But North Korea—a country mostly disconnected from the Internet?

Computers are Computers

- Most of the world runs Windows—in the US, China, Iran, and probably North Korea
- Hacking Windows in the US is the same as hacking it in North Korea
- All it took was the will to develop the capability—the basic skills needed are readily learnable online
- Hacking teams cost a lot less than nuclear reactors or uranium enrichment centrifuges…

Attributed to North Korea

- A destructive attack on South Korea's banking computers
- An attack on Sony Pictures, stealing email, unreleased films, and more
- The theft of $80 million via the SWIFT banking network, and an attempt to steal $1 billion
  - That was thwarted by a typo….

Attributed to Iran

- A destructive attack on computers belonging to Saudi Aramco
- A DDoS (distributed denial of service) attack on US banks
- Attacks against a small dam in Westchester County, NY

The Evil Empire Strikes Back

- Fundamentally, computers manipulate information
- News is information
- So: fake news stories, Twitter bots, and more—all attributed to Russia—can boost a candidate
- And then there's hacking…

Hacking an Election

- Two different Russian intelligence agencies hacked the DNC computers
  - Apparently, neither knew what the other was up to
- John Podesta's email account was hacked, too
- Information was selectively released to hurt Clinton
- GOP computers were hacked—but that information was never published by WikiLeaks…
- France and Germany are being targeted now, and there are reports that Russia influenced the Brexit vote

Defending Against Nation-States

- Should a commercial organization be expected to defend itself against a foreign government?
  - Should a corporation have its own antiaircraft guns to defend against a foreign air raid?
- Do corporations or political parties have the skills?
- But—can Cybercommand defend domestic US computers without monitoring all (domestic!) Internet links?

Attribution

- Attribution used to be very hard—but we now know how to do it
- Today's techniques: common software modules, modus operandi, HUMINT
  - But watch out for reuse
- The first two techniques require experience and continuity
- HUMINT often requires an intelligence agency
- But when done properly, attribution is doable and reliable

Other Cyber Activities

- Nations with the ability are using hacking to commit espionage
    - This is *not* against international law
- Nation-state espionage to benefit commercial entities
- Some nations "prepare the battlefield"—they hack computers today in case they need them for future attacks

Deterrence Doesn't Work Well

- No one knows anyone else's capabilities
- (One purpose of nuclear tests: to demonstrate your capability to the other side)
- No one knows how reliable cyber weapons would be if used en masse
  - Many of them seem to require constant care and feeding
  - Patches and reconfigurations can block older attacks

Where Are We?

- Today, offense is easier than defense
- More or less any country that wants to can develop a cyber attack capability—but large-scale defense is *very* difficult
- Possession of weapons doesn't cause wars—that requires an underlying causus belli—but there is lots of preexisting international tension
- Cyber weapons are asymmetric—if you're not wired, you're not vulnerable