Cyber Conflict and Geopolitics

DR. ALEXA ROYDEN

QUEENS UNIVERSITY OF CHARLOTTE

Examples of Significant Cyber Attacks

Cyber attacks on government agencies, defense and high tech companies, or economic crimes with losses of more than a million dollars.

Chinese hackers were found to have compromised the EU’s communications systems, maintaining access to sensitive diplomatic cables for several years

The United States, in coordination with Australia, Canada, the UK, and New Zealand, accused China for conducting a 12-year campaign of cyber espionage targeting the IP and trade secrets of companies across 12 countries. The announcement was tied to the indictment of two Chinese hackers associated with the campaign.

Examples of Significant Cyber Attacks

U.S. Navy officials report that Chinese hackers had repeatedly stolen information from Navy contractors including ship maintenance data and missile plans.

Security researchers discover a cyber campaign carried out by a Russia-linked group targeting the government agencies of Ukraine as well as multiple NATO members

Researchers report that a state-sponsored Middle Eastern hacking group had targeted telecommunications companies, government embassies, and a Russian oil company located across Pakistan, Russia, Saudi Arabia, Turkey, and North America

Italian oil company Saipem was targeted by hackers utilizing a modified version of the Shamoon virus, taking down hundreds of the company’s servers and personal computers in the UAE, Saudi Arabia, Scotland, and India

Examples of Significant Cyber Attacks

Researchers report that a state-sponsored Middle Eastern hacking group had targeted telecommunications companies, government embassies, and a Russian oil company located across Pakistan, Russia, Saudi Arabia, Turkey, and North America

Italian oil company Saipem was targeted by hackers utilizing a modified version of the Shamoon virus, taking down hundreds of the company's servers and personal computers in the UAE, Saudi Arabia, Scotland, and India

North Korean hackers have reportedly targeted universities in the U.S. since May, with a particular focus on individuals with expertise in biomedical engineering

Examples of Significant Cyber Attacks

The Security Service of Ukraine blocked an attempt by the Russian special services to disrupt the information systems of Ukraine's judicial authority

The Czech security service announced that Russian intelligence services were discovered to have been behind attacks against the Czech foreign ministry in 2017

Chinese hackers breached the systems of an American hotel chain, stealing the personal information of over 500 million customers

WHY HIGHLIGHT THESE ATTACKS?

From: Center for Strategic and International Studies, Cybersecurity and Governance

What is Cyber Warfare?

The use of computer technology to disrupt the activities of a state or organization, especially the deliberate attacking of information systems for strategic or military purposes.

Examples:

- Denial of service attacks
- Computer viruses
- Disinformation campaigns

STUXNET

- World’s first cyber weapon
- Conceived by US and Israel in 2005/06
- Largest and most expensive malware development in history
- Attacked Iran’s air-gapped Natanz nuclear facility
- Infected through technician’s PCs
- Targeted physical processes (centrifuge operation)

Legitimized cyber weapons

Start of a new cyber arms race

Possible targets: key infrastructures, hospital equipment, cars

Major Players

- Primary Aggressors: China, Russia, North Korea, Iran
- Primary Victims: US, South Korea, India, UK, Israel
- All major states involved in cyber conflict
- Increasing number of aggressors are not major powers
- Non state actors, like ISIS, engage in cyber warfare

Why Have States Embraced Cyber Warfare?

- Increasingly level playing field - not low barrier to entry, but lower
- Death of 1,000 hacks > distract, undermine, compromise opponent
- Lack of international law defining and delimiting cyber conflict
- When is it an act of war?
- What is a proportional response?
- Allows aggressors large undefined operating environment with little threat of significant retaliation

Russia And US Elections

- Disinformation is a common strategy
- May 2014 Ukrainian Presidential Election
  - Hacked emails, alter vote tallies, DNS, and malware attacks to undermine election legitimacy (key: goal not to win)
- 2017 ODNI confirmation of Russia’s support for Trump/Stein/Sanders
  - Hacking of DNC and emails
  - Intrusion in voter registration systems
  - Social media propaganda, including: suppressing African American votes, alienating progressive voters, arousing conservative voters (BLM, immigration), linking Trump with Christian values

No, The US Is Not Prepared

- Tremendous public and private sector capabilities/vulnerabilities
- Other states capabilities exceed our ability to defend
- Requires extensive coordination with the private sector
- Private sector distrust of US gov’t (Snowden, Going Dark, Maven)
- Initial caution, and then disorganization from the Executive branch
- We do not prioritize or resource in the same way we prioritize and resource traditional security threats, because
- We don’t understand them

How the US Can Catch Up

- Obviously, we need to prioritize and resource cyber security, BUT
- We also need a clear strategic focus for the broader cyber domain upon which US and global society runs
- Senator Ben Sasse’s call for a bipartisan national commission
- Full spectrum SWOT analysis > threat, response
- KEY: We can’t pretend it’s not happening

Want More Information?

- Cyberwar, Kathleen Hall Jamieson
- Cybersecurity and Cyberwarfare: What Everyone Needs to Know, P.W. Singer and Allan Friedman