International Implications of Defensive Cyber Operations

Dr. Kevin Newmeyer

Agenda

- Sovereignty & International Law
- The Purely Defensive
- Standing on the Edge
- Going on the Attack

Sovereignty

- With its origin in the absolute power of the monarch, it is a fundamental concept that establishes the relationship between individuals and the state.

Territorial Sovereignty

- Definition: Exclusive right of the state to exercise its powers within the boundaries of the state.
- Where are your servers?
- Where is your data stored?
- Where is your "cloud"?
- Where are you?

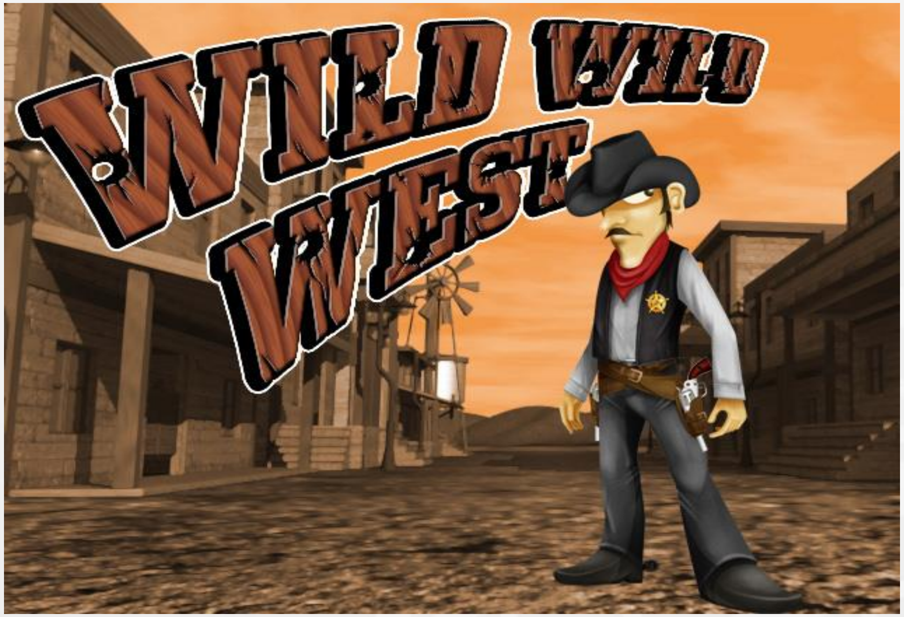
Traditional Territorial Sovereignty

- The “local” state has sovereign power over all of its territory. It gets to make the rules.
- Host state rules on privacy, data storage, and breech liability apply
- Similarly the lack of legislation may impede actions on protection of intellectual property

Extraterritorial Issues

- Can states enforce laws outside of their physical boundaries?
- The United States asserts sovereign control over its citizens (and corporations) on a global basis
  - Foreign Corrupt Practices Act
- Does it apply to cyber activities?
  - Not clear

International Law and Cyber



International Law

- Closer to Wild Wild West
- Agreement that the Law of War and International Humanitarian Law applies
- Little else
  - Cybercrime Treaty
  - Bilateral Statements
  - Developing Norms

WHAT CAN YOU DO?

Purely Defensive Actions

Defensive actions

- Encryption
- Network Segmentation
- Limited Privileges
- Active Monitoring

Key points

- They are internal, stay within your perimeter
- Cybersecurity best practices

Standing on the Edge

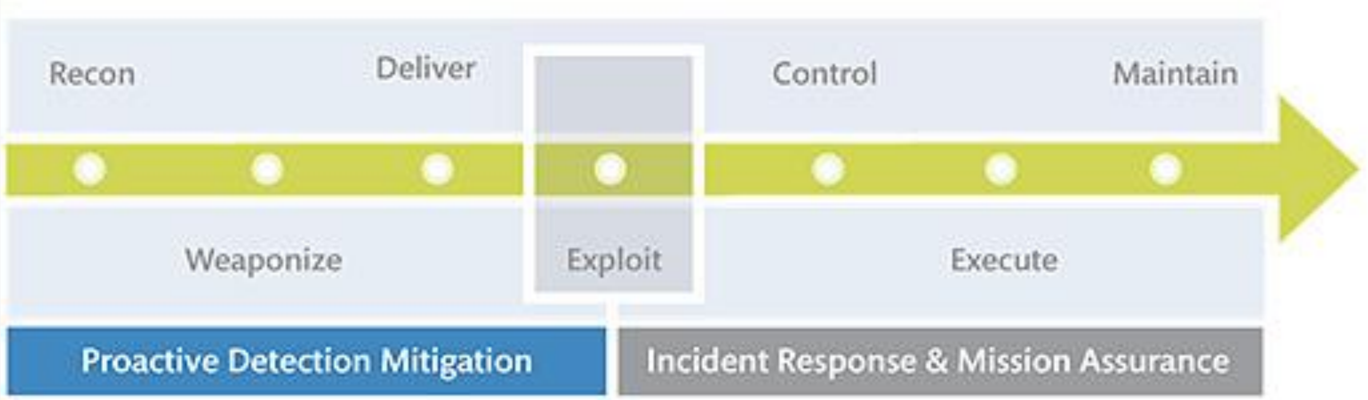
What else can be done?

- Honeypots
- Defensive engagements
- Bringing in allies

Issues with Honeypots

- Engaging with the adversary to see what they are doing and how
- You are monitoring, do you have to disclose and get consent?
- Entrapment?

Defensive Engagements


Recon
Deliver
Control
Maintain
Weaponize
Exploit
Execute
Proactive Detection Mitigation
Incident Response & Mission Assurance

Leverage honeypots and other data collection
Reverse engineering of malware
Evaluating current events for threat indication

Goal is to anticipate next threat/attack to mitigate beforehand

Ref: MITRE Cyber Attack Lifecycle

Bringing in Allies

- Information sharing
- Domestic and International
- Law enforcement

Going on the attack

What are the options?

- Data markers
- Network manipulation/Active Deception
- Hacking back

Legal issues

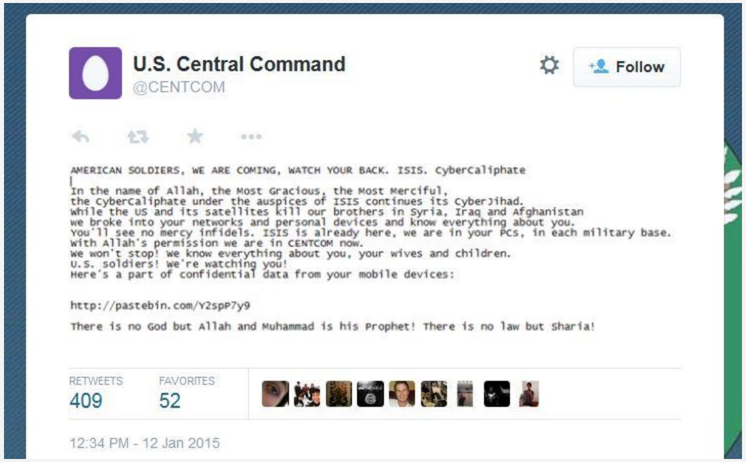
- Electronic Crimes Act
- Computer Fraud and Abuse Act
- Armed attack or active defense?

- Attribution problem

It is happening

- At 2012 BlackHat, 36% of respondents admitted retaliation hacking
- But it is not without risk
  - Legal Issues
  - Counter-Counter Attack
- What crosses the line to use of force?

Armed attack in cyberspace?



U.S. Central Command
@CENTCOM

AMERICAN SOLDIERS, WE ARE COMING, WATCH YOUR BACK. ISIS. CyberCaliphate

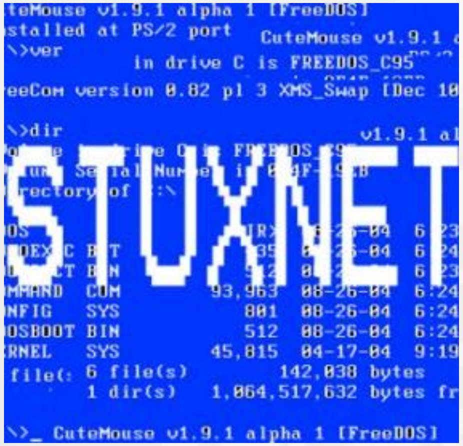
In the name of Allah, the Most Gracious, the Most Merciful,
the CyberCaliphate under the auspices of ISIS continues its CyberJihad.
While the US and its satellites kill our brothers in Syria, Iraq and Afghanistan
we broke into your networks and personal devices and know everything about you.
You'll see no mercy infidels. ISIS is already here, we are in your PCs, in each military base.
With Allah's permission we are in CENTCOM now.
We won't stop! We know everything about you, your wives and children.
U.S. soldiers! We're watching you!
Here's a part of confidential data from your mobile devices:

http://pastebin.com/Y2spP7y9

There is no God but Allah and Muhammad is his Prophet! There is no law but Sharia!

RETWEETS 409 FAVORITES 52

12:34 PM - 12 Jan 2015



What is Use of Force in Cyberspace

- Key Conclusions UN Group of Experts
  - States may not knowingly allow cyber infrastructure located in their territory to be used for acts that adversely affect other States.
  - States may be responsible for cyber operations directed against other States, even though those operations were not conducted by the security agencies.
    - Prohibition on Patriotic Hackers
  - The prohibition on the use of force in international law applies fully to cyber operations. Though international law has no well-defined threshold for determining when a cyber operation is a use of force, the International Group of Experts agreed that, at a minimum, any cyber operation that caused harm to individuals or damage to objects qualified as a use of force.
  - Cyber operations that merely cause inconvenience or irritation do no qualify as a use of force

Conclusions

- As the actions get more aggressive, the rules become more murky
- Technology has far outstripped policy
- The landscape continues to change

QUESTIONS?