DEVIATION FROM THE NORMS:

The Necessity And Challenges Of A Norms-based Approach To Digital Offense

Andrea Little Limbago
February 1, 2017
WHAT TARGETS ARE OFF LIMITS?

- Intellectual Property
- Privacy & Civil Liberties
- Critical Infrastructure
- Elections
STATE OF THE SECURITY LANDSCAPE (P1.)

SCALING DATA BREACHES

- **SONY PICTURES**: 47,000 in 2014
- **OFFICE OF PERSONNEL MANAGEMENT**: 21 MILLION in 2015
- **ASHLEY MADISON**: 37 MILLION in 2015
- **TARGET**: 40 MILLION in 2013
- **EBAY**: 145 MILLION in 2014
- **YAHOO**: 1 BILLION in 2016
STATE OF THE SECURITY LANDSCAPE (P2.)

RISE OF THE BOT AND AUTOMATION

GLOBAL INTERNET POPULATION BY 2016
FREEDOM OF THE NET STATUS

FOTN assesses 88 percent of the world’s internet user population.

Source: https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html
WHEN IT COMES TO DIGITAL OFFENSE

RULES OF THE ROAD

AKA

Norms n.
Shared expectations of appropriate behavior.
THE PURSUIT OF NORMS

US DEPARTMENT OF STATE
International Cybersecurity Strategy:
Deterring Foreign Threats and Building Global Cyber Norms

BLACK HAT
“Are we at the beginning of a sea change in what the international community decides is acceptable behavior? It doesn’t have to be a treaty; it can just be a norm. The next administration is going to have to drive those norms of behavior.”

Jeff Moss, founder of Black Hat & DEF CON, 2016 Dark Reading article

SINO-AMERICAN AGREEMENT

MICROSOFT

UK CYBERSECURITY STRATEGY
A BRIEF HISTORY OF U.S. DIGITAL OFFENSE RESPONSES

1986
The Computer Fraud and Abuse Act

1996
First major US public attribution: Moonlight Maze

2013
Microsoft and FBI take down Citadel botnet

2014
Indictment of 5 PLA Officers for Cyber Espionage

2015
Sanctions against North Korea following Sony hack
Microsoft and FBI take down global Dorkbot

2016
Indictment of 7 Iranians for attacks on dam, banks
Election attacks attributed to Russia, sanctions, persona non grata and diplomatic evictions

THIRTY YEARS OF DIGITAL OFFENSE WITHOUT ANY NORM FORMATION
Norms n.
Shared expectations of appropriate behavior.
EXAMPLE: SEATBELT USAGE

1968 – National Highway Safety Bureau requires lap belts

Battles over regulation and civil liberties infringements

ENTRENCHMENT
In US, 87% of adults wear seatbelts all the time, despite it being a secondary law in ~1/3 of states

CASCADE
Widespread research supporting the number of lives seatbelts could save:
• From 1983-1990, usage went from 14% to 50%
• Between 1983-89, 34 states enacted mandatory usage laws

EMERGENCE

ENDGAME.
NORM PROPAGATION S-CURVE

KEY CHALLENGE WITH DIGITAL OFFENSE NORM EMERGENCE:

LEADERSHIP VACUUM

- Norm entrepreneur/leadership required
- Currently a state of competition
- Lack of universally-accepted norms
NORM PROPAGATION S-CURVE

KEY CHALLENGE WITH DIGITAL OFFENSE NORM CASCADE: COLLECTIVE ACTION PROBLEM

- Nation-states
- Criminal Groups
- Hactivists
- Lone Wolves
- Corporations
- Terrorist Groups

CASCADEN

ENDGAME.
NORM PROPAGATION S-CURVE

KEY CHALLENGE WITH DIGITAL OFFENSE
NORM ENTRENCHMENT:

COMPLIANCE

Dwell Time  Attribution  State Secrets
THE INFLECTION POINT

Requires greater **U.S.** leadership and private sector activism and support to push forth global norms in favor of a resilient, secure and free internet

**CYBER SOVEREIGNTY**

- Autocracy
- Surveillance
- Censorship

**MULTI-STAKEHOLDER MODEL**

- Democracy
- Freedom
- Civil Liberties
MULTI-STAKEHOLDER MODEL

Building an open, secure and resilient global internet through consensus among interested groups, including corporations and nation-states

CHARACTERISTICS

- Global internet freedoms
- Balancing security and privacy
- Social integration
- Focus on what is “off limits”
CYBER SOVEREIGNTY

COMPLETE GOVERNMENT CONTROL OF THE INTERNET WITHIN THEIR BORDERS, INCLUDING ECONOMIC, SOCIAL AND POLITICAL INFORMATION

CHARACTERISTICS

- Disguised as nationalistic to protect against adversaries
- Surveillance state
- Censorship & filtering
- Propaganda and disinformation
COMPETING NORMS: FROM THEORY TO PRACTICE

Multi-Stakeholder Model
- ICANN
- United Nations GGE
- G20
- NATO’s Article V

Limited Intervention
- UK Investigatory Powers Act
- US rule 41
- Regulating algorithms

Cyber Sovereignty
- Shanghai Cooperation Organization code of conduct
- The great firewall
- Iranian national intranet
- Social media censorship across the globe
FORUM SHOPPING: FORUMS FOR NORM DIFFUSION

**TRADITIONAL FORUMS**

- INTERNATIONAL GOVERNMENTAL ORGANIZATIONS
- BILATERAL AGREEMENTS
- NON-GOVERNMENTAL ORGANIZATIONS & ADVOCACY GROUPS

**THE MODERN VIRTUAL FORUM**
“What we’ve also tried to do is to start creating some international norms about this to prevent some sort of cyber arms race,... And my approach is….putting some guardrails around the behavior of nation-states, including our adversaries, just so that they understand that whatever they do to us we can potentially do to them.”

Former President Barack Obama’s end-of-year press conference, December 16, 2016
THE INFLECTION POINT: WHICH MODEL WILL PREVAIL?

CYBER SOVEREIGNTY

MULTI-STAKEHOLDER MODEL
Thanks!

andrea@endgame.com
@limbagoa