Dan Paltiel
Policy Program Manager
Truman Center for National Policy
Cyber After 2016

Politics & Policy in 2017 and Beyond

Dan Paltiel, Policy Program Manager
Truman Center for National Policy
Agenda

➡️ What is Truman?

➡️ Cyber Regulation Shortcomings

➡️ Cybersecurity Takes Center Stage

➡️ The Whole-of-Government Approach

➡️ 2017 and Beyond

➡️ Q&A
Truman Members
Cyberspace & Security Program

Cyber First Principles

Cybersecurity ensures the confidentiality, integrity, and availability of information and information systems. It enables freedom of speech, civil liberties, innovation, and free markets—principles that are proven to increase the potential for freedom and opportunity, at home and abroad.

Information networks are a tool that enables the expansion of America’s mutually supportive ideals of human rights, freedom, and opportunity. They help create the conditions for innovation and human prosperity to flourish, while ensuring U.S. national security and world stability. While new technologies can provide hope to billions, they can also be used to create instability and exploit potential vulnerabilities in networks and systems.

THE CHALLENGE

Today, hostile nations, criminal groups, and individuals seek to exploit information networks—like the Internet—to further a variety of national and ideological objectives. America’s banks, energy sector, and intellectual property continue to be routinely targeted by criminal hackers and foreign governments alike. A devastating attack on U.S. critical infrastructure would directly threaten American citizens, the U.S. economy, and America’s way of life.

The problem is growing, not shrinking. As people become more dependent upon technology, opportunities for crime, espionage, and physical disruption will increase exponentially. This trend will continue unless we are able to foster an environment where cybersecurity is the rule, not the exception.
Agenda

➤ What is Truman?

➤ Cyber Regulation Shortcomings

➤ Cybersecurity Takes Center Stage

➤ The Whole-of-Government Approach

➤ 2017 and Beyond

➤ Q&A
2012: The Debate on Capitol Hill

**Key Pillars:**
1. Critical Infrastructure
2. Information Sharing
3. Role of DHS
4. Data Breach Reporting
The Interest Groups

- Standards will raise cost to attackers
- Anonymize info
- Only share with civilian agencies
- Mandates will hurt bottom line

Federal Government
Privacy & Civil Liberties Advocates
Business (Chamber of Commerce)
## Securing Critical Infrastructure

<table>
<thead>
<tr>
<th>Stakeholder</th>
<th>CSA 2012 v.1 (Senate)</th>
<th>CSA 2012 v.2 (Senate)</th>
<th>“Market Version” (House)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Federal Government</td>
<td>😊</td>
<td>😞</td>
<td>😞</td>
</tr>
<tr>
<td>Privacy/Civil Liberties</td>
<td>😊</td>
<td>😞</td>
<td>😞</td>
</tr>
<tr>
<td>Business</td>
<td>😞</td>
<td>😊</td>
<td>😊</td>
</tr>
</tbody>
</table>
Feb 2013: POTUS Responds with an Executive Order

**Policy Results:**
- “Industry-led, government facilitated” best practices (*NIST Framework*)
- Increase USG → Industry Info Sharing
- Privacy & Civil Liberties Oversight
2014: NIST Cybersecurity Framework

• Outlines broad standards for cybersecurity
• Tech-neutral, flexible for different businesses
• Adopted by 30+ countries
• Most CI providers in US “adopting” but each doing it differently
• Good base → but not good for regulation or mandates
December 2015: Passage of CISA

Voluntary info sharing: industry → government
No PII or info “irrelevant to cybersecurity”
Remaining PII can be used to prosecute cybercrime

<table>
<thead>
<tr>
<th>Stakeholder</th>
<th>Approve?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Federal Government</td>
<td>😊</td>
</tr>
<tr>
<td>Privacy-Civil Liberties</td>
<td>😞</td>
</tr>
<tr>
<td>Business</td>
<td>😊/ 😞</td>
</tr>
</tbody>
</table>
Agenda

➡ What is Truman?

➡ Cyber Regulation Shortcomings

➡ Cybersecurity Takes Center Stage

➡ The Whole-of-Government Approach

➡ 2017 and Beyond

➡ Q&A
 Setting Rules of the Road

Conspiring to Commit Computer Fraud; Accessing a Computer Without Authorization for the Purpose of Commercial Advantage and Private Financial Gain; Damaging Computers Through the Transmission of Code and Commands; Aggravated Identity Theft; Economic Espionage; Theft of Trade Secrets

Huang Zhenyu  Wen Xinyu  Sun Kailiang  Gu Chunhui  Wang Dong
Agenda

➤ What is Truman?

➤ Cyber Regulation Shortcomings

➤ Cybersecurity Takes Center Stage

➤ The Whole-of-Government Approach

➤ 2017 and Beyond

➤ Q&A
2015: Info Sharing + Sanctions

- **February**: Development of info sharing and analysis organizations (ISAOs)
  - Streamline classified info sharing

- **April**: Authorizes sanctions to be put in place against malicious cyber-enabled activity vs:
  - Critical Infrastructure
  - Disruption to computer network
  - Economically-motivated cyber espionage
Feb 2016: Cyber National Action Plan

- Creates cyber commission + Federal CISO
- DHS lead in private sector cyber
- Plans to modernize federal IT
- Mandates federal incident response
Cyber National Action Plan

$19 billion in FY17 budget (35% increase) → CNAP dead on arrival?
## PPD-41: Cyber Incident Response

<table>
<thead>
<tr>
<th>IMPACT</th>
<th>None</th>
<th>Unlikely</th>
<th>Some</th>
<th>Likely</th>
<th>Significant</th>
<th>Imminent Threat</th>
</tr>
</thead>
<tbody>
<tr>
<td>LEVEL</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
</tbody>
</table>

- **LEVEL 0**: No government response
- **LEVEL 5**: Government Response

---

**Unified Coordination Group (UCG)**

- **Threat Response**
- **Intelligence Support**
- **Asset Response**
So where does that leave industry?

- Discovery of malicious breach **188 days**
- 81% of victims do not discover themselves
- Attacker’s ROI for exploit kit → **1,425%**

- FBI under-resourced
- Fear of liability
Cyberspace is still the “Wild West”

→ Passive defense is not sufficient in all cases
## Active Cyber Defense Spectrum

<table>
<thead>
<tr>
<th>LEVEL OF SEVERITY</th>
<th>TYPE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Intelligence Gathering</td>
<td>Ex-ante gathering, online forums, reverse-engineer exploits</td>
</tr>
<tr>
<td>2</td>
<td>Active Defense Measures/ Mitigation</td>
<td>Sandbox, honeynet, monitor traffic, beacon files</td>
</tr>
<tr>
<td>3</td>
<td>Investigation/Attribution</td>
<td>Trace IP, fingerprint servers, infiltrate underground markets, hop points, hacking email accounts/C2 nodes</td>
</tr>
<tr>
<td>4</td>
<td>”Hacking Back” / Retaliatory Measures</td>
<td>Destructive attacks, sinkhole</td>
</tr>
</tbody>
</table>

→ **What does the Computer Fraud and Abuse Act allow?**
Agenda

➤ What is Truman?

➤ Cyber Regulation Shortcomings

➤ Cybersecurity Takes Center Stage

➤ The Whole-of-Government Approach

➤ 2017 and Beyond

➤ Q&A
What’s Next?

• Inaccessible Data
• Are We Keeping Pace with Threats?
• Interference in U.S. elections
• Divided Congress
• And a new administration...
“Going Dark”/Encryption Debate

Security

Security
This matter is before the Court pursuant to an application pursuant to the All Writs Act, 28 U.S.C. § 1651, by Assistant United States Attorneys Tracy Wilkison and Allen Chiu, requesting an order directing Apple Inc. ("Apple") to assist law enforcement agents in enabling the search of a digital device seized in the course of a previously issued search warrant in this matter.

For good cause shown, IT IS HEREBY ORDERED that:

1. Apple shall assist in enabling the search of a cellular telephone, Apple make: iPhone 5C, Model: A1532, P/N:MGFG2LL/A, S/N:PPMNQ3MTG2DJ, IMEI:358820052301412, on the Verizon Network, (the
Secure Messaging Apps
Dear customers!

Dec. 23, 2015, from 15:35 - 16:30, third parties were made illegal entry into information-technological system of remote access to equipment telecontrol substations of 35-110 kV JSC "Kyivoblenenergo."

As a result, it was disconnected 7 (seven) 110 kV substations and 23 (twenty three) substation 35 kV. This led to the repayment of about 80,000 different categories of customers on the reliability of electricity supply.

Electricity was restored to all consumers employees of the Company at 18:56 the same day.

We apologize for the situation and thank you for your understanding.

PJSC "Kyivoblenenergo"
Hacking As Political Interference
Divided Congress and 2016
Ways To Move Forward

- Develop new tools to hold malicious actors accountable
- Clarify liability when companies defend themselves
- Protect small businesses that can’t afford good security