



Global Cybersecurity

Presentation to CAE Forum

14 February 2018

Dr. Terry Thompson

Today's Agenda

- **Internet Governance**
- **Frameworks and Strategies**
- **Critical Infrastructure Protection**
- **Global Cyber Threats**
- **Privacy, Surveillance, Control**
- **Cybercrime, Cyber Espionage, Cyber War**



Internet Governance

Reference Questions

- When did cybersecurity become a global topic of interest?
- What was the driver?
- Which organizations led the discussion?
- What are the politics in today's global discussion about cybersecurity?
- What are the main challenges in cybersecurity governance today?

ITU Definition of Cybersecurity



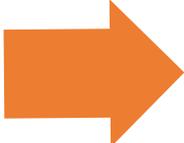
Cybersecurity – *The collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets.*

Source: ITU-T X.1205 (04/2008)

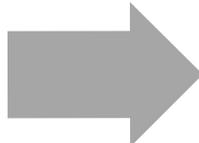
WSIS 2003 and 2005 addressed the global opportunities and challenges of the Internet



UN Resolutions 57/239 (December 2002) and 58/199 (December 2003) laid the foundation for a global culture of cybersecurity and invited member nations to a *World Summit on the Information Society (WSIS)*



Geneva, 2003



Tunis, 2005

WSIS Declaration of Principles based on leveraging ICT to achieve major UN goals:

- Eradication of extreme poverty and hunger
- Universal primary education
- Promotion of gender equality and empowerment of women
- Reduction of child mortality
- Improvement of maternal health
- Combat HIV/AIDS and other major diseases
- Ensure environmental sustainability
- Enhance chances for global peace
- And ...

The 2003 WSIS *Plan of Action* contained 10 specific actions designed to create a culture of global cybersecurity



- Promote international cooperation to share threat information, build trust, and protect data
- Governments and private sector work together to prevent, detect, and respond to cybercrime
- Governments and other stakeholders work to promote user education and awareness
- Take appropriate action on spam at national and international levels
- Revise/develop regulations to enable use of electronic documents
- Further strengthen the trust and security framework with initiatives in ICT security
- Share good practices in information security and encourage their use by all parties
- Interested countries to establish focal points for real-time incident handling and information sharing about cyber threats
- Ensure further development of technologies to enable e-commerce
- Interested countries to contribute actively to the ongoing United Nations activities to build confidence in the security of ICTs

1

States
(Nations)

2

Private
Sector

3

Civil Society

4

Intergovern-
mental
Organizations

5

International
Organizations

6

Academic,
Technical
Communities

WSIS also defined the multi-stakeholder environment required for effective Internet governance

The Internet Governance Forum (IGF) was an important outcome of the Tunis Agenda



IGF Goals

- Discuss public policy issues related to the Internet to foster its robustness and security
- Interface with intergovernmental organizations on matters of mutual interest
- Facilitate the exchange of information and best practices in science, technology, academia
- Advise and propose ways to accelerate availability and affordability of the Internet in the developing world
- Strengthen and enhance role of stakeholders in Internet governance mechanisms
- Identify emerging issues and bring them to the attention of relevant organizations
- Contribute to capacity building for Internet governance in developing countries
- Promote and assess the embodiment of WSIS principles in Internet governance
- Discuss issues related to Internet resources
- Help to find solutions to issues arising from use and abuse of the Internet
- Facilitate dialogue on cross-cutting international public policies
- Publish proceedings of the IGF

<https://www.intgovforum.org/>

Major Issues in Internet Governance

Control of the Internet

Transparency of decision-making processes

Scalability

Human rights and free speech

“Multi-stakeholder” vs. “multi-national”

Control of the Internet

- **Major concerns:**
 - Too much U.S. involvement
 - Too much UN control
- **Rationale:**
 - Internet invented in the U.S.
 - Most root zone servers in U.S.
 - U.S. Government controls ICANN and IANA (Internet Assigned Numbers Authority) function

DNS Root Servers



Source: IANA (<https://www.iana.org/domains/root/servers>)

ICANN/IANA: Global coordination of IP addresses and autonomous system numbers

Transition of IANA Functions to ICANN

- 1998: ICANN/IANA under contract to U.S. Government
- 2009: ICANN commits to multi-stakeholder governance
- 2014: U.S. announces intent to end contract with IANA
- 2016: U.S. Government contract with IANA ends; ICANN assumes control over IANA



UNITED STATES DEPARTMENT OF COMMERCE
The Assistant Secretary for Communications
and Information
Washington, D.C. 20230

AUG 16 2016

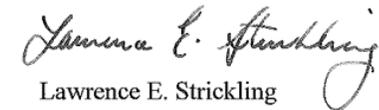
Mr. Göran Marby
President and CEO
Internet Corporation for Assigned Names and Numbers
12025 Waterfront Drive, Suite 300
Los Angeles, CA 90094-2536

Dear Mr. Marby:

On August 12, 2016, the National Telecommunications and Information Administration (NTIA) received from the Internet Corporation for Assigned Names and Numbers (ICANN) an implementation status report on the Internet Assigned Numbers Authority (IANA) stewardship transition. In the report, ICANN confirms that all the required transition tasks are completed or will be complete in advance of September 30, 2016. NTIA has thoroughly reviewed the report. Based on that review, barring any significant impediment, NTIA intends to allow the IANA functions contract to expire as of October 1.

Please feel free to contact me if you have any questions.

Sincerely,


Lawrence E. Strickling

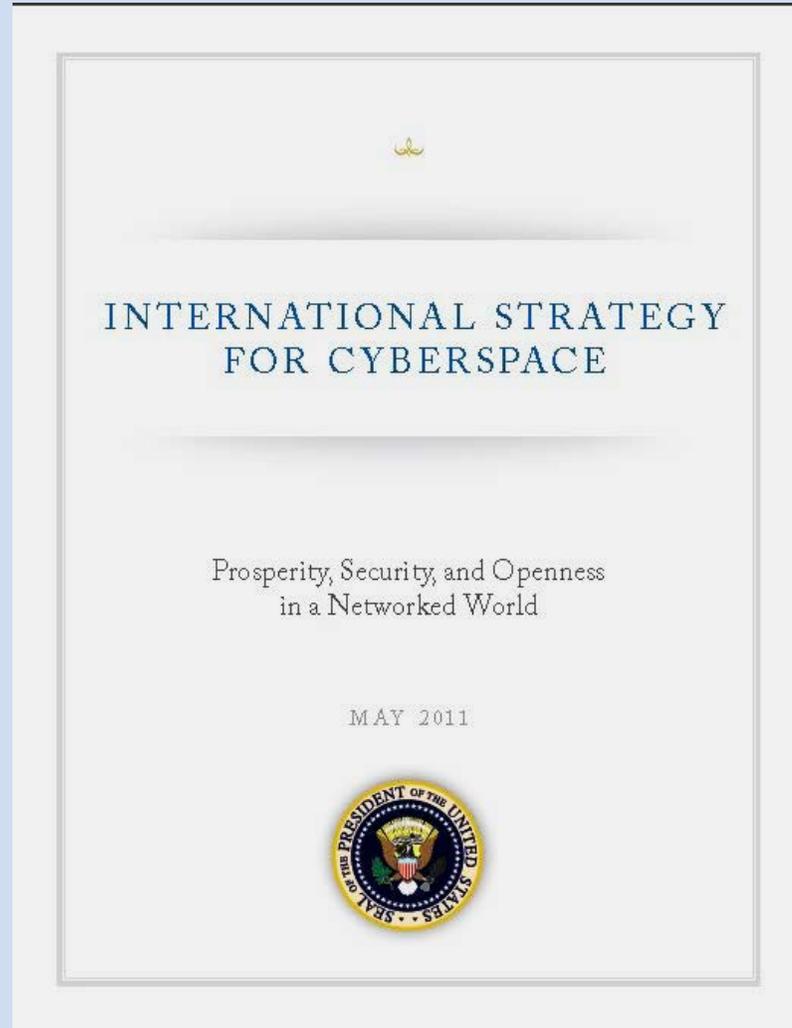
Cc: Dr. Stephen Crocker, Chairman of the Board, ICANN

Reminder



WSIS defined the multi-stakeholder environment required for effective Internet governance

The U.S. International Strategy for Cyberspace (2011)



Key Principles

- Open, secure, reliable, and interoperable Internet
- Stability through norms of responsible behavior
- **Multi-stakeholder governance of the Internet**
- Cybersecurity capacity building
- Interoperable and secure technical standards
- International collaboration on cyber defense
- Enhanced collaboration in law enforcement
- International military collaboration to protect against cyber threats

Global Conference on Cyber Space (GCCS)

- Initiated by the United Kingdom in 2011
- Multi-stakeholder meetings focusing on:
 - Practical cooperation in cyberspace
 - Capacity building
 - Development of acceptable norms of behavior in cyberspace
- Five conferences held so far
 - London 2011
 - Budapest 2012
 - Seoul 2013 (“Seoul Framework for Commitment to Open and Secure Cyberspace”)
 - The Hague 2015
 - New Delhi 2017 <https://gccs2017.in/>

China created the World Internet Conference to push for multi-national governance of the Internet



Chinese President Xi Jinping addresses the World Internet Conference in Wuzhen, China

- Annual conference since 2014
- Held in Wuzhen, Zhejiang Province
- President Xi Jinping advocates “internet sovereignty” – the right of each nation to develop, manage, and govern the Internet
- 2016 conference attended by 1,600 people from 110+ countries
- Shanghai Cooperation Organization (上海合作组织) supports multi-national Internet governance (2011, 2015)

ITU Attempts to Overturn Multi-stakeholder Model at World Conference on International Communications (WCIT)



- Treaty-level conference on international telecommunications
- Held in Dubai in December 2012; 193 countries attended
- UN/ITU role enhanced in draft treaty sent to delegates
 - DNS system to be managed by UN
 - Global monitoring of communications for fraud, cybercrime
 - Government restrictions on internet traffic allowed
- U.S. and EU come out against the proposal
- ITU redraft supported by 89 countries
 - U.S., Canada, Japan, UK, India did not sign



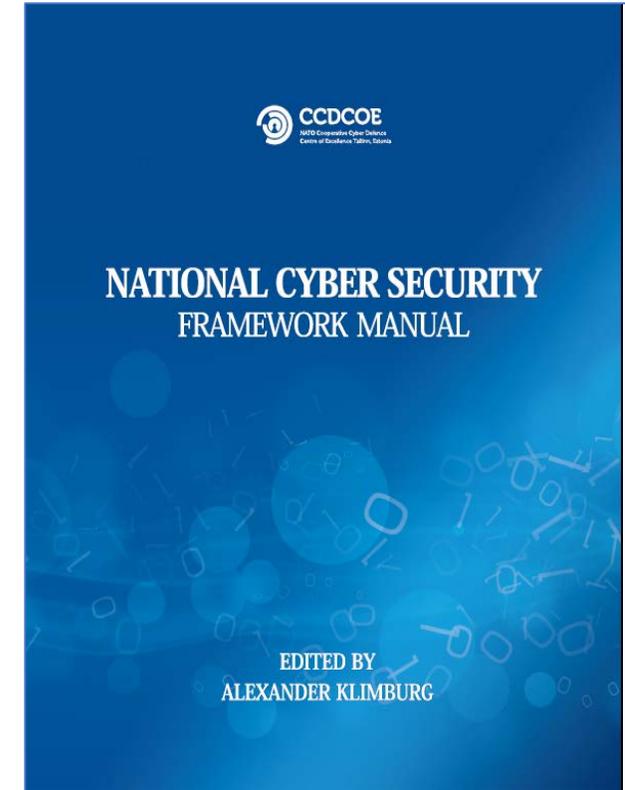
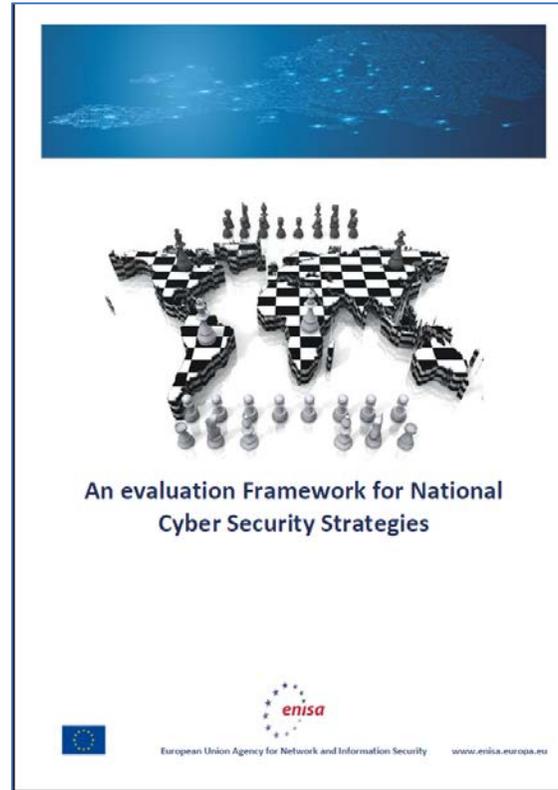
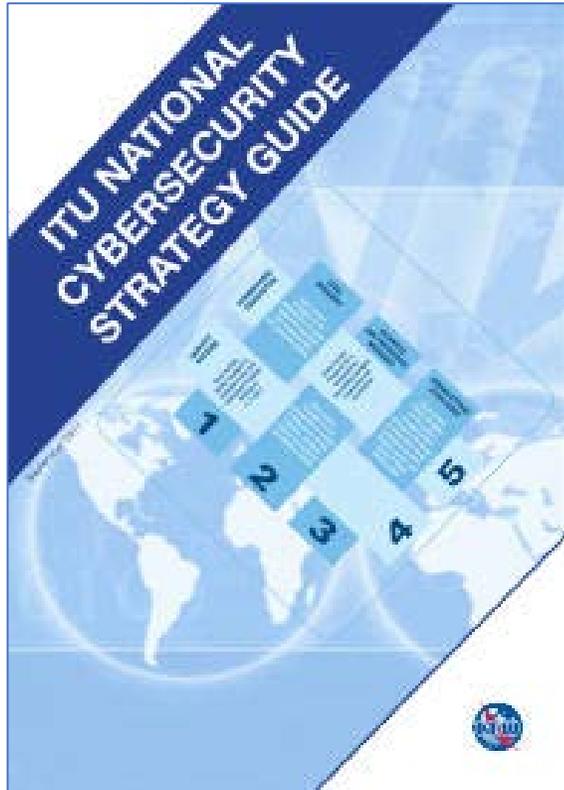
Given this background, will we have a global Internet...

The background is a complex, futuristic digital interface. It features a central circular hub with a keyhole-like shape, surrounded by concentric rings and various data patterns. The color palette is primarily dark blue and teal, with some lighter blue highlights. The overall aesthetic is high-tech and data-driven.

Strategies, Frameworks, Countries, Regions

Reference Questions

- What is a cybersecurity strategy?
- What are the features and characteristics of a national strategy?
- What are some examples?
- What about regional organizations?



There are several frameworks for developing and evaluating national cybersecurity strategies

#ITEM	ELEMENTS OF A NATIONAL CYBERSECURITY PROGRAM (1)
1	Top Government Cybersecurity Accountability Top government leaders are accountable for devising a national strategy and fostering local, national and global cross-sector cooperation
2	National Cybersecurity Coordinator An office or individual oversees cybersecurity activities across the country
3	National Cybersecurity Focal Point A multi-agency body serves as a focal point for all activities dealing with the protection of a nation's cyberspace against all types of cyber threats
4	Legal Measures Typically, a country reviews and, if necessary, drafts new criminal law, procedures, and policies to deter, respond to, and prosecute cybercrime.
5	National Cybersecurity Framework Countries typically adopt a framework that defines minimum or mandatory security requirements on issues such as risk management and compliance

#ITEM	ELEMENTS OF A NATIONAL CYBERSECURITY PROGRAM (2)
6	Computer Incident Response Team (CIRT) A strategy-led program contains incident-management capabilities with national responsibilities. The role analyzes cyber threat trends, coordinates response, and disseminates information to all stakeholders
7	Cybersecurity Awareness and Education A national program should exist to raise awareness about cyber threats
8	Public-Private Sector Cybersecurity Partnership Governments should form meaningful relationships with the private sector
9	Cybersecurity Skills and Training Program A program should help train cybersecurity professionals
10	International Cooperation Global cooperation is vital due to the transnational nature of cyber threats

Brief in text, but broad in scope, and not updated frequently

Connected to larger national goals and strategies, e.g. national security strategy

Describe the importance of ICT to the national interest

Characterize the threat environment

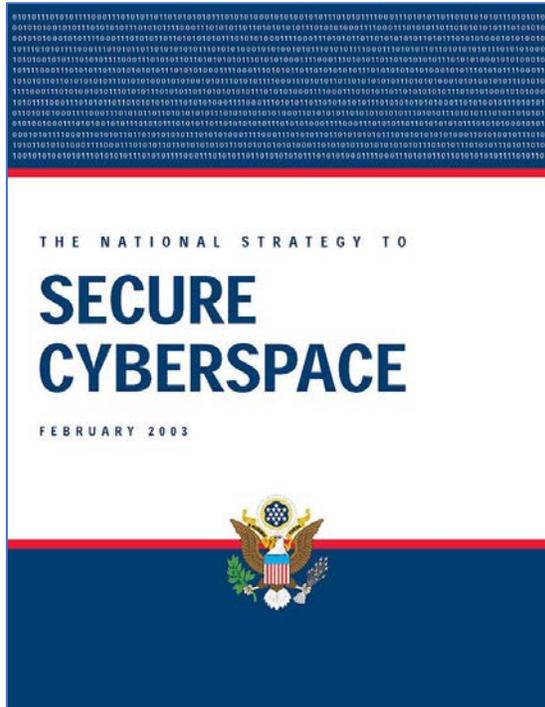
Provide the national plan for addressing cybersecurity

Identify roles and responsibilities for governmental and other organizations

List goals, actions, and deadlines for components of the national plan

Most national cybersecurity strategies share common characteristics

U.S. National Strategy to Secure Cyberspace (2003)



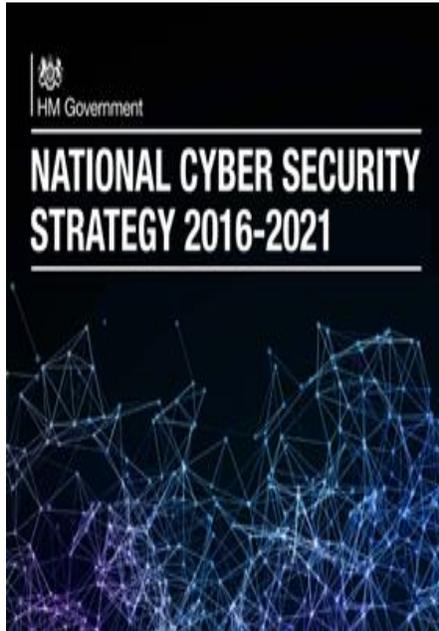
Key Assumption

“The Federal government could not – and, indeed should not – secure the computer networks of privately owned banks, energy companies, transportation firms, and other parts of the private sector. ... Each American who depends on cyberspace, the network of information networks, must secure the part that they own or for which they are responsible.”

Key Priorities

- Create national cyberspace security response system
- National cybersecurity threat and vulnerability reduction
- National cybersecurity awareness and training program
- Secure Government cyberspace
- Establish position of national cyberspace security coordinator
- National security and international cyberspace security cooperation

The 2016 UK National Strategy acknowledges past accomplishments, while focusing on remaining needs



Primary Objectives

Defend UK Cyberspace

Deter Adversaries

Develop Capabilities

International Cooperation

- Updated to accommodate new threats, e-commerce
- “Much has been achieved, but we are still not ahead of the threat.”
 - Too many insecure networks, even in critical infrastructure
 - Cybersecurity risks not properly addressed by the market
 - Too many data breaches
 - Not enough trained cyber specialists
- **Collective effort needed: government, business, citizens**
- **More centralized government approach**
 - Levers and incentives (investment, regulation, education)
 - Expanded technology and law enforcement
 - Technology development, including “active defense”
 - National Cyber Security Centre (NCSC) established

The Government’s ambition is for the UK to be the world’s leading digital nation.

China's National Cybersecurity Strategy

(From unofficial English translation, December 2016)



Major Opportunities

- New channels for people to obtain information
- New spaces for production and life
- Innovation-driven economic development
- Improved cultural exchange
- New areas for national sovereignty

Major Challenges

- Political stability
- Threats to critical infrastructure and economic security
- Harm to cultural security
- Online terrorism
- Growing threat of arms race in cyberspace

Strategic Tasks

- Defend sovereignty in cyberspace
- Safeguard national security
- Protect critical information infrastructure

Objectives

- Promote peaceful use of Internet
- Improve cyber defenses to control risks
- Standards, openness for global economy
- Multilateral, transparent Internet
- Protect privacy and social order

Principles

- Respect sovereignty in cyberspace
- Peaceful use of cyberspace
- Strengthen rule of law in cyberspace
- Balance modernization with security

- Strengthen online culture
- Attack cyber terrorism and cybercrime
- Perfect network governance

European Union/ENISA

- Facilitates information sharing and exchange of best practices
- Wide range of expertise on relevant topics
- Cybersecurity strategy framework serves as a model for many countries
- EU Cybersecurity Agency will focus on threats, information sharing, and exercises
- Cybersecurity “safety labels” for ICT products
- Denmark: Names first “Tech Ambassador” to Silicon Valley





Critical Infrastructure Protection

Reference Questions

- What is “critical infrastructure?”
- How does cybersecurity relate to critical infrastructure?
- Do all countries identify the same critical infrastructure sectors?

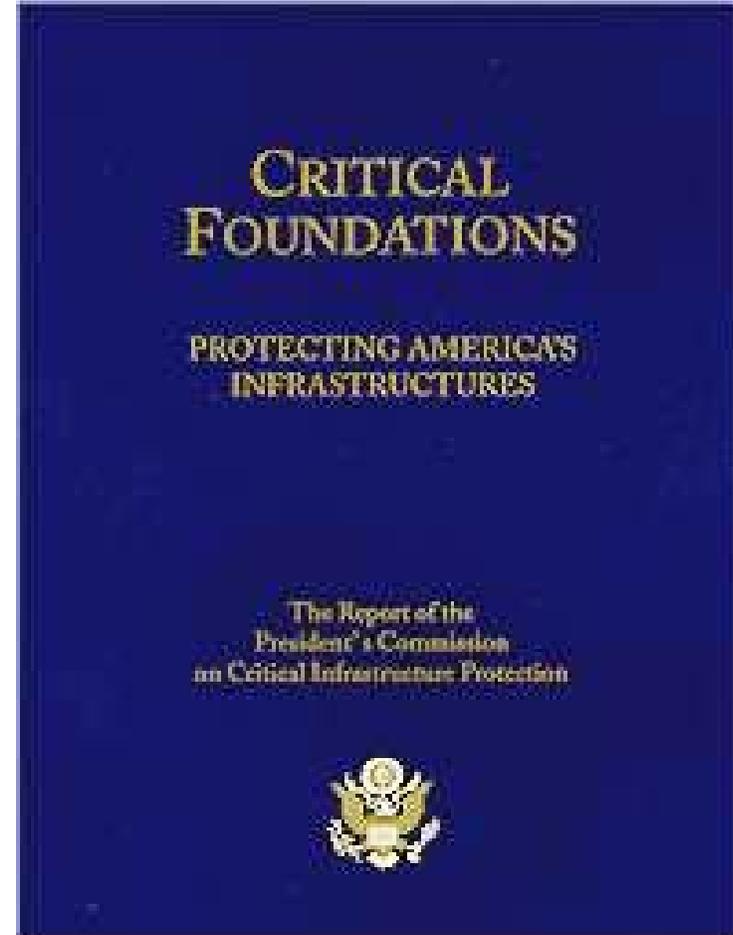
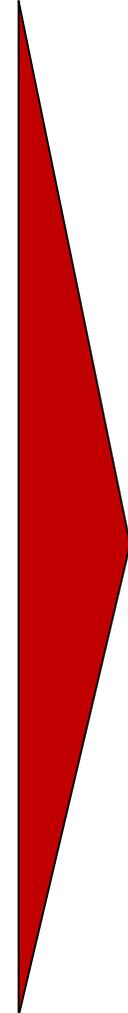
What is “Critical Infrastructure?”



- Essential services that underpin society and serve as the backbone for the nation's economy, security, and health
- Power we use in our homes, the water we drink, the transportation that moves us, the stores we shop in, and the communication systems we rely on to stay in touch with friends and family
- *Assets, systems, and networks, whether physical or virtual, so vital that their incapacitation or destruction would have a debilitating effect on national security, national economic security, national public health or safety, or any combination thereof*

Source: <https://www.dhs.gov/what-critical-infrastructure>

Bombings of the Murrah Building in Oklahoma City (1995) and Khobar Towers in Saudi Arabia (1996) led to serious thinking about critical infrastructure protection



PCCIP "Marsh Commission" report, October 1997

**The Marsh
Commission
identified
cybersecurity
elements of
critical
infrastructure
protection**

Cyber threats to critical infrastructure are a growing concern

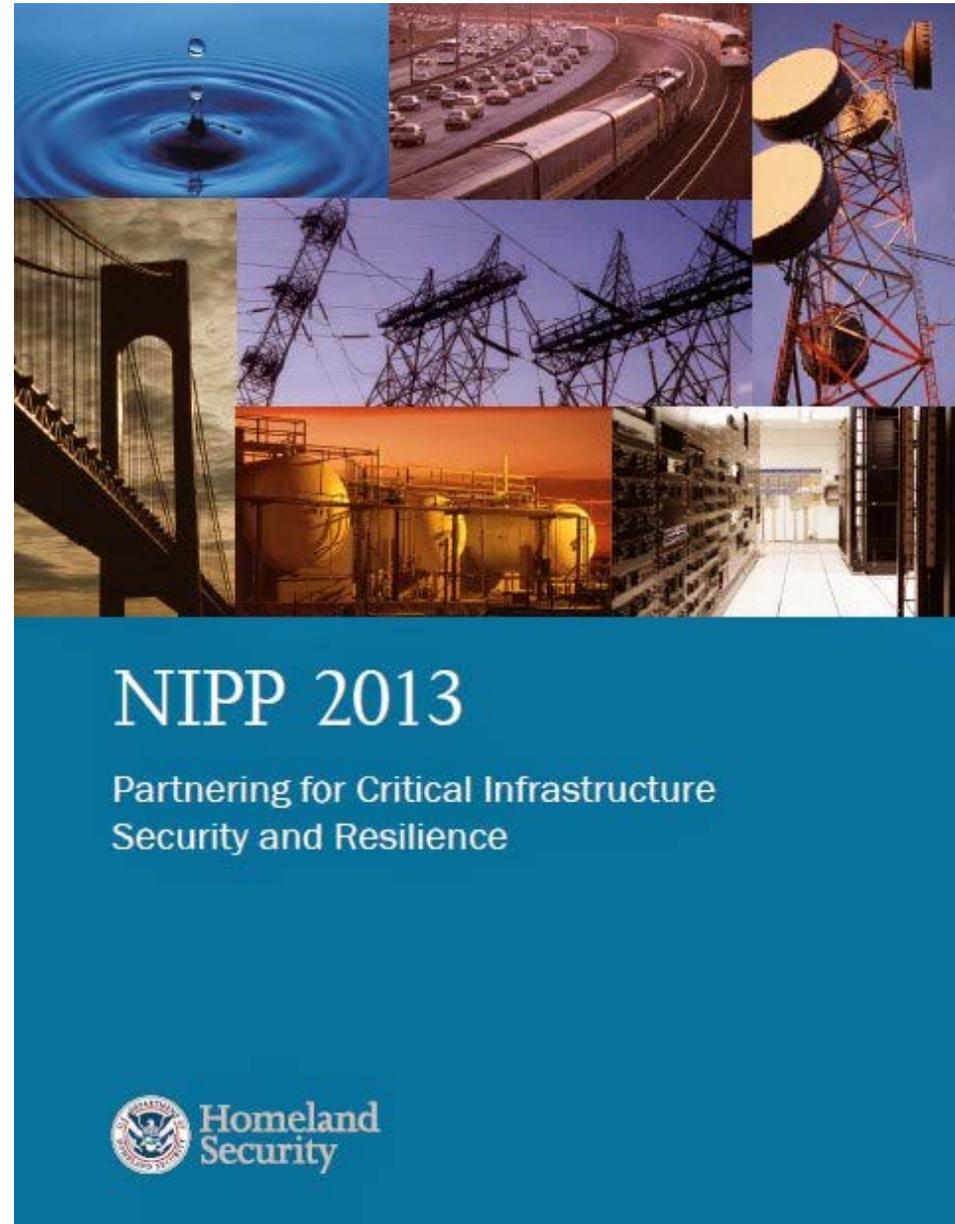
Public-private partnerships are key to critical infrastructure protection

Information sharing is the most immediate need

A national focal point for critical infrastructure is required

The National Infrastructure Protection Plan (NIPP) is the U.S. strategy for CIP

(Previous editions in 2006, 2009)



The United States has identified 16 critical infrastructure sectors



Courtesy of DHS

Banking and Finance

Central Government/Government Services

Telecommunications/Information and Communications Technologies

Emergency/Rescue Services

Energy/Electricity

Health Services

Food

Transportation/Logistics/Distribution

Water

Most countries have identified “core sectors” in their Critical Infrastructure Protection policy

Let's look at CI sectors in a few countries

Hungary



- Information and Telecommunications Systems
- Energy
- Water Supply
- Transport
- Public Health
- Food Supply
- Banking and Financial Sector
- Industry
- Government Institutions
- Public Safety and Homeland Defense

S. Korea



- E-Government and Government Services
- National Security
- Emergency/Disaster Recovery Services
- National Defense
- Media Services ,e.g. Broadcasting
- Financial Service
- Gas and Energy, e.g. Power Plants

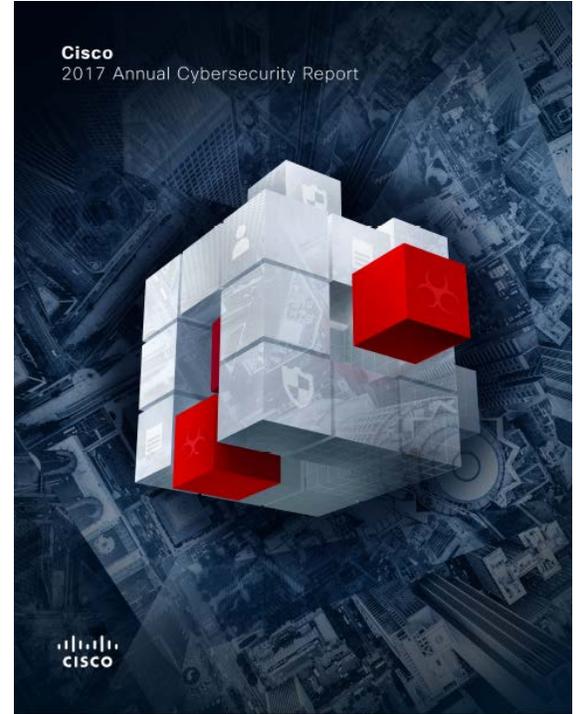
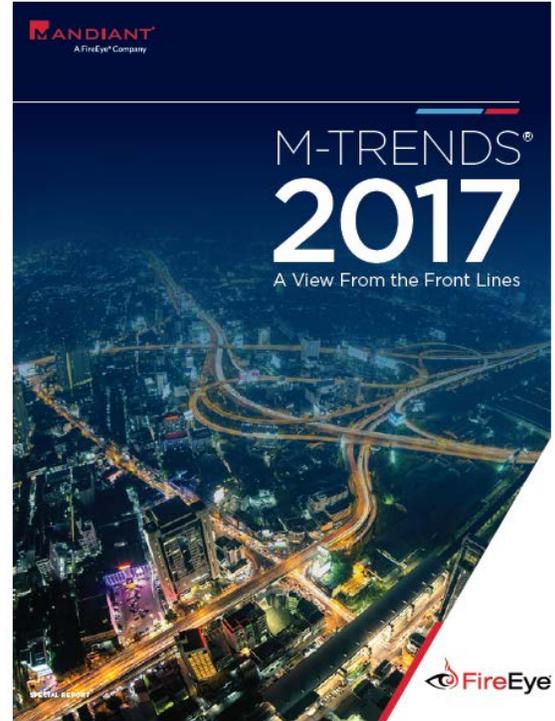
India



- Banking and Finance
- Space
- Insurance
- Petroleum, Gas
- Civil Aviation
- Defense
- Telecommunications
- Law Enforcement
- Atomic Energy
- Power
- Ports
- Railways

Global Cyber Threats





Symantec, Verizon, Mandiant, and Cisco publish annual cyber threat reports that provide data on major threats and trends

Major trends in cyber threats (2015-17)

- Fewer zero-day attacks, more “living off the land”
- Targeted attacks focused on financial heists
 - Carbanak, Banswift, Odinaff groups main players
- Ransomware attacks on the rise
 - Average ransom demand increased from \$294 (2015) to \$1,077 (2016)
- IoT attacks becoming more common
 - 2x more attacks against IoT devices in 2016
- PowerShell used for mailbox harvesting
- Social media interference in elections



What tactics do they use?

62% of breaches featured hacking.

51% over half of breaches included malware.

81% of hacking-related breaches leveraged either stolen and/or weak passwords.

43% were social attacks.

14% Errors were causal events in 14% of breaches. The same proportion involved privilege misuse.

8% Physical actions were present in 8% of breaches.

Who are the victims?

24% of breaches affected financial organizations.

15% of breaches involved healthcare organizations.

12% Public sector entities were the third most prevalent breach victim at 12%.

15% Retail and Accommodation combined to account for 15% of breaches.

Who's behind the breaches?

75% perpetrated by outsiders.

25% involved internal actors.

18% conducted by state-affiliated actors.

3% featured multiple parties.

2% involved partners.

51% involved organized criminal groups.

What else is common?

66% of malware was installed via malicious email attachments.

73% of breaches were financially motivated.

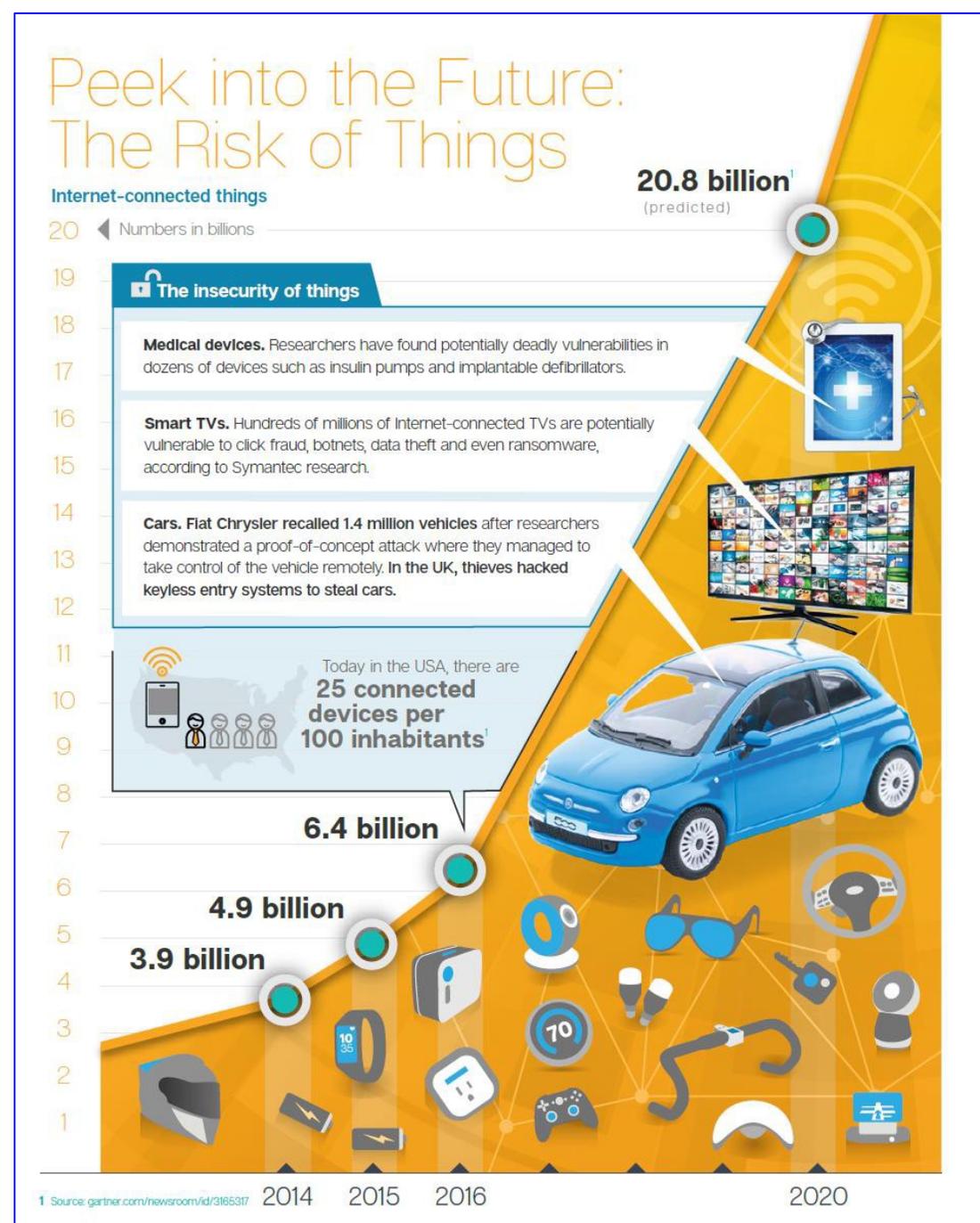
21% of breaches were related to espionage.

27% of breaches were discovered by third parties.

“Attack the Humans”

Can you trust your car?

- Gartner estimates that there are almost 6.5 billion devices connected to the Internet
- More than 20 billion devices worldwide projected by 2020
- Vehicles, home automation are big growth areas
- Most IoT devices lack security, making them vulnerable to botnet recruitment
- Mirai malware turns IoT devices into bots for use in DDoS attacks



2018 Cyber Threat Predictions

- Ransomware attacks will increase, especially against big companies
- Cloud services will be more targeted
- More business email compromises and tax scams
- IoT devices increasingly targeted: drones, cars, medical devices
- More mobile malware
- Increased social media manipulation in elections
- Attacks on blockchain and digital currency
- Malware inserted into software supply chains more often



PRIVACY

A person in a dark suit is pointing at a digital interface. The interface features a grid of hexagonal icons. The word 'PRIVACY' is written in large, glowing blue letters at the top. The icons include a padlock, a person in a hat, a Wi-Fi symbol, and a document with a checkmark. The background is a blurred blue and white pattern.

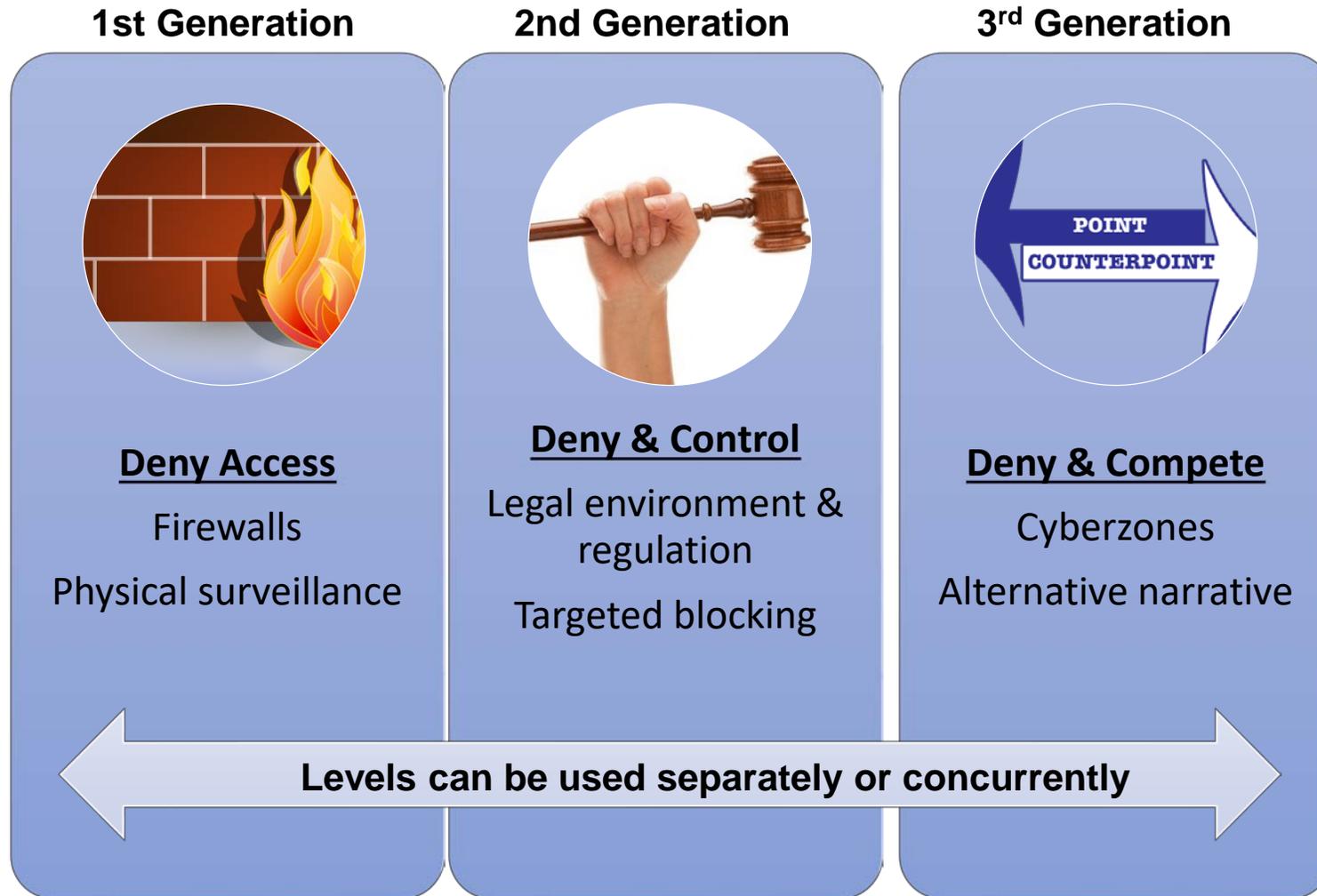
Privacy, Surveillance, Control

Information Management
in the Digital Age

Reference Questions

- What is privacy in the information age?
- Do all countries treat privacy the same way?
- What controls are deployed on the Internet?
- What is the level of free expression on the Internet?

Internet controls have evolved from simple to sophisticated and are used in various combinations



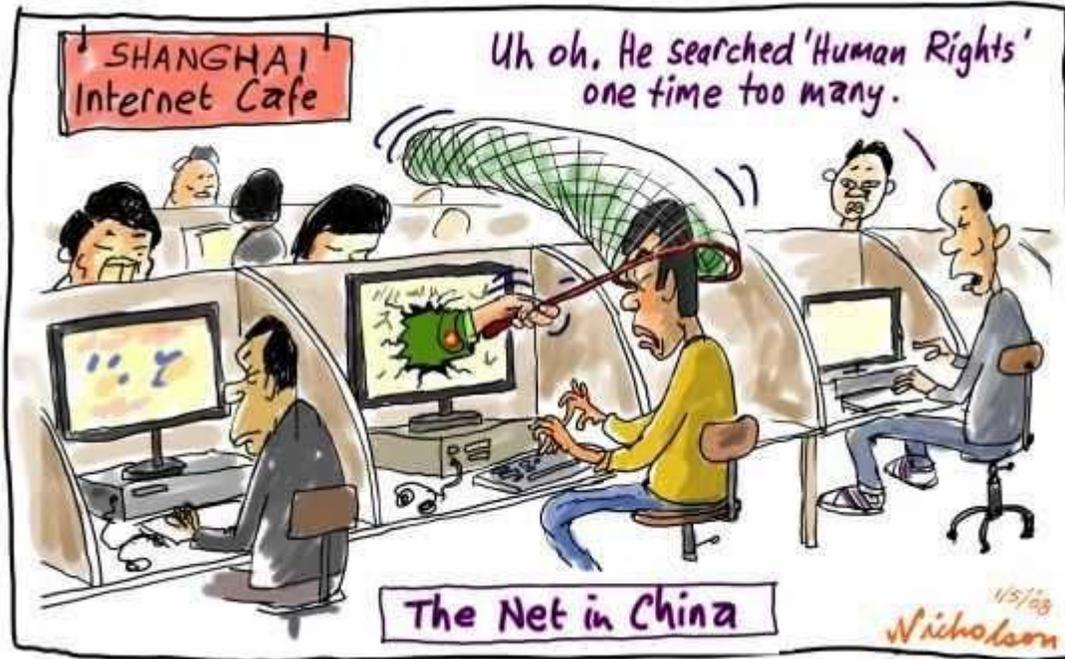
Source: Ronald Deibert, et al., ed, *Access Controlled* (MIT Press, 2010)

In some countries, you get a block page whenever you try to access a prohibited site



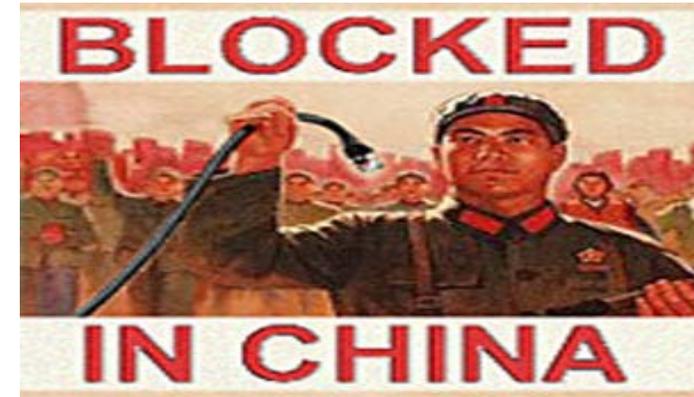
Typical block page in Qatar

China has many sophisticated mechanisms to control access and content



Mechanisms:

- ▶ Great Firewall of China ("Golden Shield")
- ▶ IP blocking, DNS tampering, keyword tampering
- ▶ Censorship and self-censorship
- ▶ Kill switches (internet and mobile telephony)
- ▶ Network monitors, using e.g. biometrics
- ▶ Registration of users; self-censorship

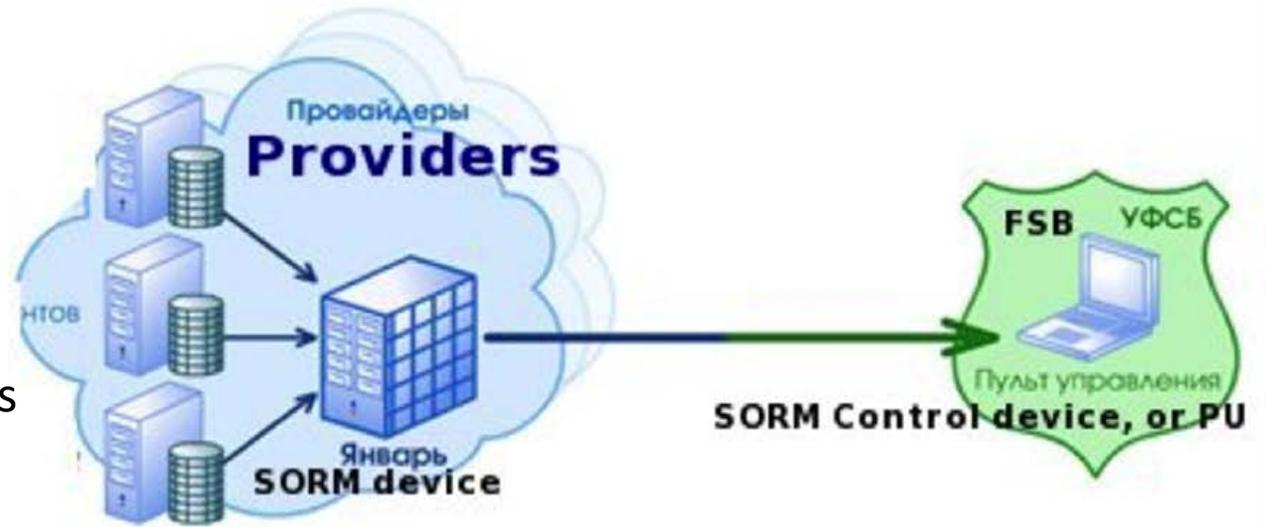


Categories:

- Current news (censored as well as blocked); foreign press
- Anything subversive or critical of the government
- Human rights information
- Some economic and demographic information
- Political, social, cybercrime, pornography, on-line gambling etc.

Russia uses a comprehensive approach to Internet surveillance and control

- **Three generations of controls**
 - SORM I, II, and III
 - Technology installed in ISPs and managed by the Federal Security Bureau (FSB)
- **Physical and virtual surveillance facilitated by laws and technology**
 - Single Register (2012) is a blacklist of websites provided by three government agencies
 - Data localization law (2015)
- **Targets include political activists, journalists, terrorists**
- **Cyberzones established (e.g. Chechnya), with alternative narratives**



SORM (System of Operational-Investigative Measures)

Freedom House has published annual reports on Internet freedom since 2011



- **Founded in 1941**
 - Watchdog organization dedicated to global expansion of freedom and democracy
- **Promotes civil liberties, human rights, and democratic change**
- **Advocate** for U.S. and like-minded governments opposing dictatorship and oppression
- ***Freedom in the World***
 - Flagship publication since 1973

2017 *Freedom on the Net*

- 65 countries, 87% of Internet users
- Decline in Internet freedom for seventh year
- Focus on manipulation of democracy through social media
- Online content manipulation practiced by many countries
- Mobile connectivity blocked for political and security reasons
- Physical attacks against journalists and netizens increased dramatically

Manipulating Social Media
to Undermine Democracy
November 2017



FREEDOM
ON THE NET
2017



It's all about the data!

Data breaches lead to more regulation and localization

More Regulation

- **EU - General Data Protection Regulation (GDPR)**
 - 72-hour notification requirement
 - Fines to €20m or 4% revenue
- **New York – Department of Financial Services (DFS)**
 - 72-hour notification requirement
 - Multiyear implementation
- **China, Singapore, Canada developing regulations**

New Laws

- **Russia, China laws on the books**
- **India, Brazil developing laws**
- **Many countries have some localization laws**
 - Health care, financial records





Cybercrime, Cyber Espionage, Cyber War

Cybercrime is the commission of a crime using a computer or network to do something illegal

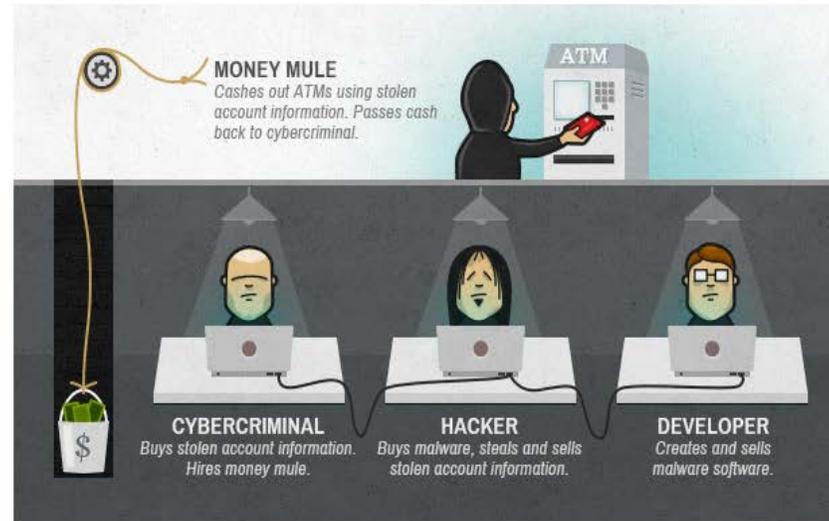
- Cybercrime has surpassed illegal drug trafficking as a criminal moneymaker
- Identity theft occurs every 3 seconds through some form of cybercrime
- More than \$450 billion lost globally to cybercrime each year
- In 2015, U.S. industry sectors lost lots of money due to cybercrime:
 - Financial services: \$28.3 million*
 - Energy and utilities: \$27.6 million
 - Defense and aerospace: \$23.2 million
 - Technology: \$16.5 million
 - Communications: \$14.9 million
 - Services: \$12.9 million
 - Transportation: \$12 million
 - Retail: \$12 million



Bank robbery - how times have changed



THEN



NOW



Banking network fraud incidents have spread around the world. Incidents have struck banks in Asia, Ukraine, Ecuador and India with losses totaling more than \$100 million. These widespread events indicate that financial criminals see these networks as ripe for manipulation.

-- M-Trends 2017



Theft of \$81 million via phishing attack on the SWIFT network (Banswift)



North Korea's Reconnaissance General Bureau, Bureau 121



WannaCry ransomware attacks against medical sector in UK

Nation-state attacks are the latest development in cybercrime and business disruption



Major countries with known cyber espionage capabilities:

- United States
- China
- Russia
- United Kingdom
- Israel
- South Africa

**Cyber Espionage: 21st
Century Tradecraft for Spies**

For China, industrial policy drives economic development and cyber espionage

- **Economic Development**
 - Growth of ICT industry
 - “863 Program” (National High Tech Research and Development Plan)
 - **“MLP” (National Medium- and Long-term Plan for Science and Technology Development 2006-2020)**
 - Policies, regulations, and standards promote “indigenous innovation”
- **Cyber Espionage**
 - Cyber hacking trends focused on U.S. and western industry after 2006
 - Much cyber espionage focused on ICT industry and other areas important to Chinese economic development

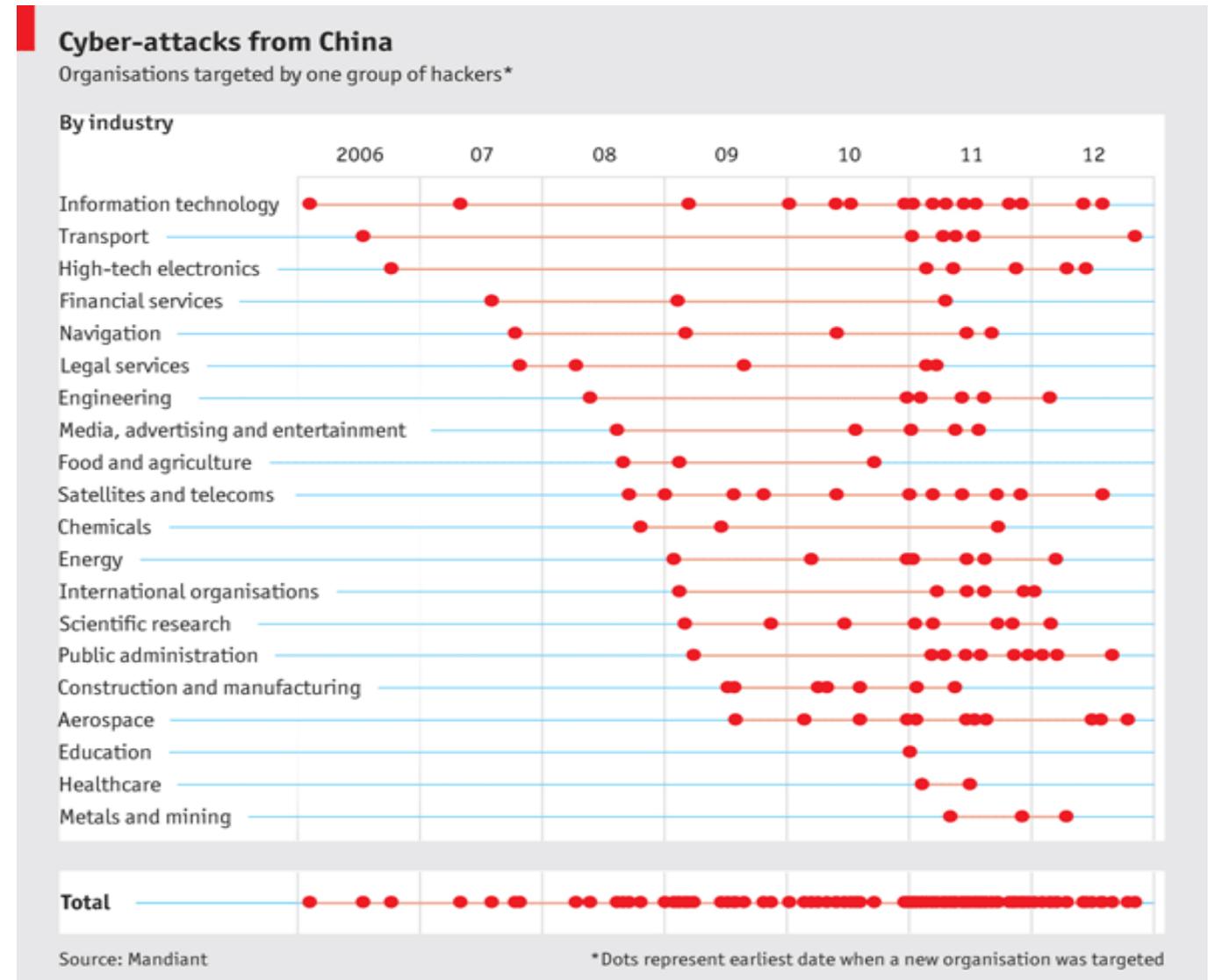


China's cyber espionage is driven by economic plans

MLP Priorities (2006-2020)

- ▶ Agricultural science and technology
- ▶ Basic Science
- ▶ S&T infrastructure development
- ▶ Innovation and S&T culture
- ▶ Ecology, environmental S&T
- ▶ Energy, resources and ocean S&T
- ▶ Human resources for S&T
- ▶ Input and management of S&T
- ▶ Law and policies for S&T development
- ▶ Manufacturing development S&T
- ▶ Modern services industry
- ▶ National defense S&T
- ▶ Overall strategy for S&T development
- ▶ Population and health S&T
- ▶ Public security S&T
- ▶ Transportation S&T

Targets of Chinese Cyber Attacks





In 2015, China and the U.S. agree to end economic cyber espionage against each other

Cyber War



Russia focuses on cyber espionage for “information operations” and to prepare the cyber battlefield

- **Cyberwar**
 - Part of “war” in general
- **Information operations**
 - Disrupt West and maintain power
- **Cyber attacks support information operations when needed**
- **Organizations**
 - APT28 (Fancy Bear) – CNE vs. European government and military
 - APT29 (Cozy Bear) – CNE vs. Western governments, industry, academia
- **Russian Information Operations**
 - Louisiana chemical plant (2014)
 - French TV (2015)
 - U.S. Presidential Election (2016)
 - German election (2017)
 - French election (2017)



2016 Election: The Russians are coming!

- Hack of Democratic National Committee
- Release of DNC emails
- Botnet assault on social media
- Possible penetration of voting machines in 20+ states



China plans to use the power of information systems to offset superior adversary forces

- **Activist cyber strategy and doctrine**

- National security: “There can be no national security without cyber security.”
- Deterrence to prevent attacks on China
- Offensive operations to exploit vulnerabilities of adversary’s infrastructure

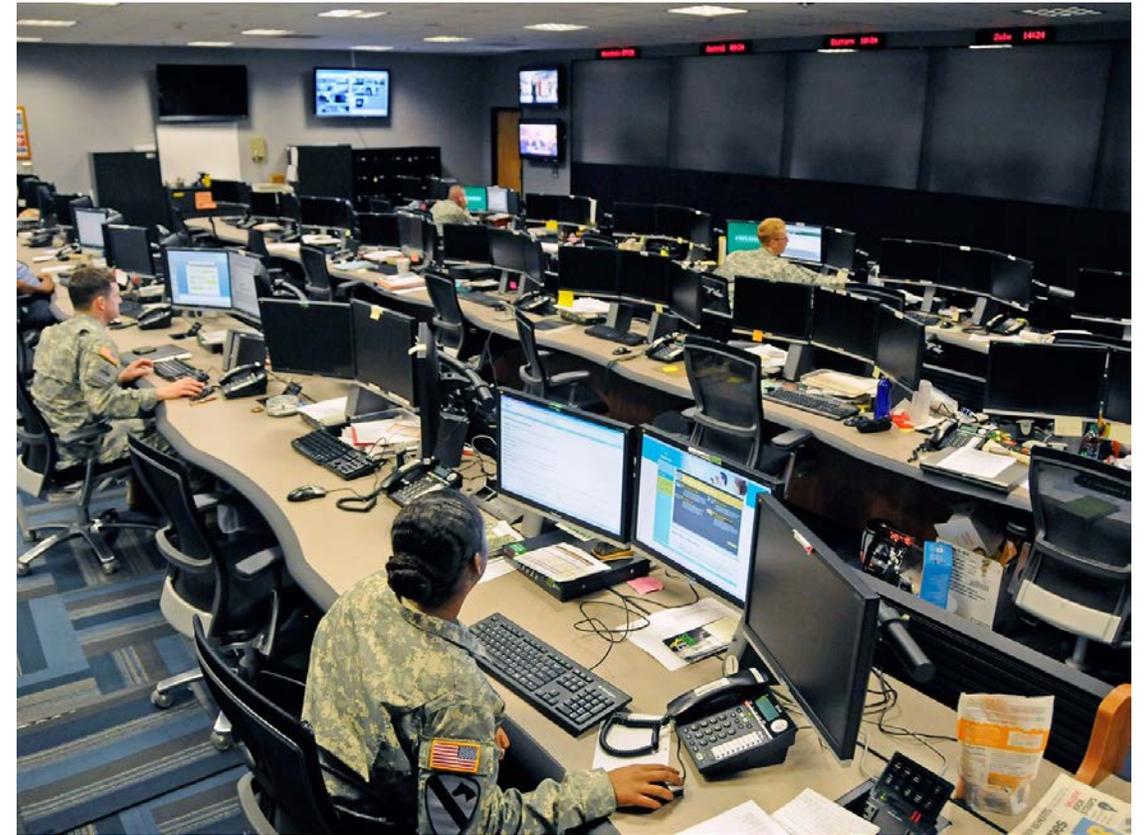
- **Citizen support for national effort**

- Cyber Militia
- Red Hacker forces

- **Strategic Support Force**

- Established 1 Jan 2016
- Includes former 2PLA, 3PLA, 4PLA
- Focus on digital battlefield and “active defense” to protect Chinese sovereignty
- Key part of “integrated strategic deterrent”
- Linked to MPS and MSS





Today: Cyber War in a Time of Peace

Summary: Global Cybersecurity

Good

- Over 3 billion people connected to the Internet
- Economic development
- More information available to more people
- Critical infrastructure protection

Bad

- Cybercrime
- Malware growth and evolution
- Cyber espionage

Ugly

- Fake news on social media
- Bot wars on truth

