Cyber Policy and Practice in National Security : US Cyber Security

ICT for International Relations

International Relations, UNIKOM

2017

Cyber Space

- Merriam-Webster defines ‘cyber’ as: ‘of, relating to, or involving computers or computer networks (as the Internet)
- *Cyberspace* is more than the internet, including not only hardware, software and information systems, but also people and social interaction within these networks
- The cyber sphere is now a venue for competition among interests and interest groups, as well as an arena for conflicts and contentions surrounding the increasingly visible hand of government. We can no longer ignore the political salience of cyberspace
- Cyberspace capabilities are also a **source of vulnerability**, posing a **potential threat** to **national security** and a disturbance of the familiar international order

Cyber Security

cybersecurity = security of cyberspace

information systems
and networks

availability, integrity and secrecy of information systems and networks in the face of attacks, accidents and failures with the goal of protecting operations and assets

According to the U.S. Dept of Commerce:

n. **cybersecurity**: "information security"

n. **information security**: The protection of information against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional.

Definitions

“Cyber Security Information Act” According to H.R. 4246 (US Cyber Security)

Cybersecurity: “The **vulnerability** of any computing system, software program, or critical infrastructure to, or their ability to resist, intentional interference, compromise, or incapacitation through the misuse of, or by **unauthorized** means of, the Internet, public or private telecommunications systems or other similar conduct that **violates** Federal, State, or international law, that **harms** interstate commerce of the United States, or that **threatens** public health or safety.”

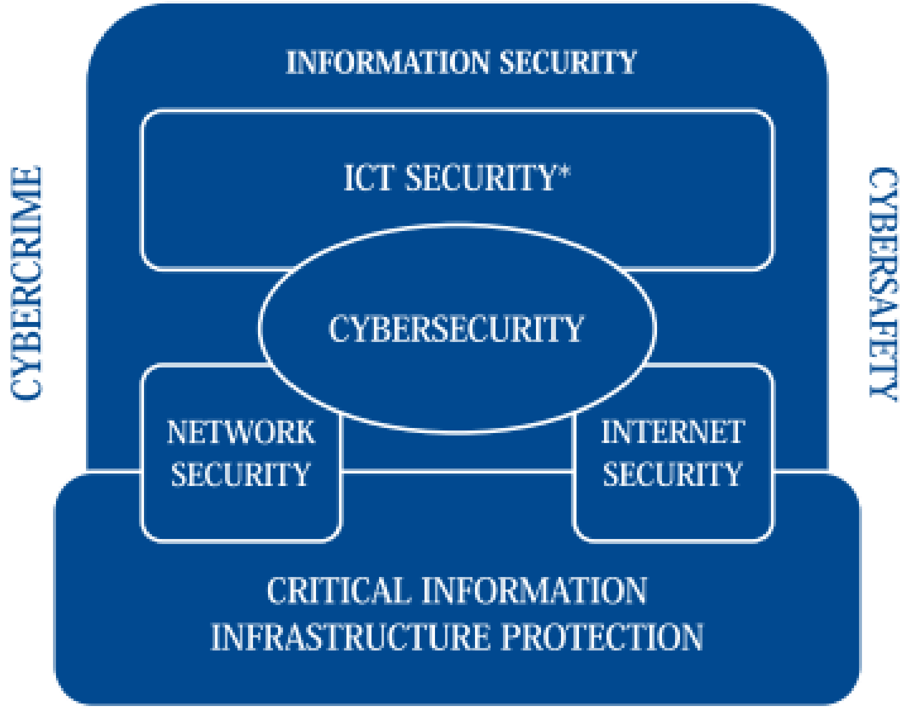
Definitions

- ITU also defined **cyber security** broadly as "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. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment"

Information, ICT & Cyber Security

- Most governments start their NCSS process by describing the importance of ‘securing information’, implementing ‘computer security’ or articulating the need for ‘information assurance’.
- **Information security** focuses on data regardless of the form the data may take: electronic, print or other forms. **Computer security** usually seeks to ensure the availability and correct operation of a computer system without concern for the information stored or processed by the computer. **Information assurance** is a superset of information security, and deals with the underlying principles of assessing what information should be protected.

- the term ‘ICT security’ is often used to describe this concern. In general, ICT security is more directly associated with the technical origins of computer security, and is directly related to ‘information security principles’ including the confidentiality, integrity and availability of information resident on a particular computer system



Many countries are defining what they mean by cyber security in their respective national strategy documents. More than 50 nations have published some form of a cyber strategy defining what security means to their future national and economic security initiatives. When the term 'defence' is paired with 'cyber' it usually is within a military context, but also may take into account criminal or espionage considerations

This level of dependence makes the Internet a target for **asymmetric attack** and a weak spot for **accidents and failures**

A solution to this problem will require both the right **technology** and the right **public policy**.

This is the cybersecurity challenge.

US Cyber Policy

- The US has been in the vanguard of developing cyber security policy and strategy.
- Quadrennial Diplomacy and Development Review (2015). The Department established a Coordinator for Cyber Issues (S/CCI) to ensure unified and effective State Department and interagency efforts to promote an open, interoperable, secure, and reliable information and communications infrastructure.
- USCYBERCOM, Cyber Mission Forces (CMF), US Computer Emergency Response Teams (CERTs), Department of Homeland Security (DHS), Defense Cyber Crime Center (DC3)
- The goal is a global information and telecommunications infrastructure that supports international commerce, strengthens international security, and fosters free expression and innovation.

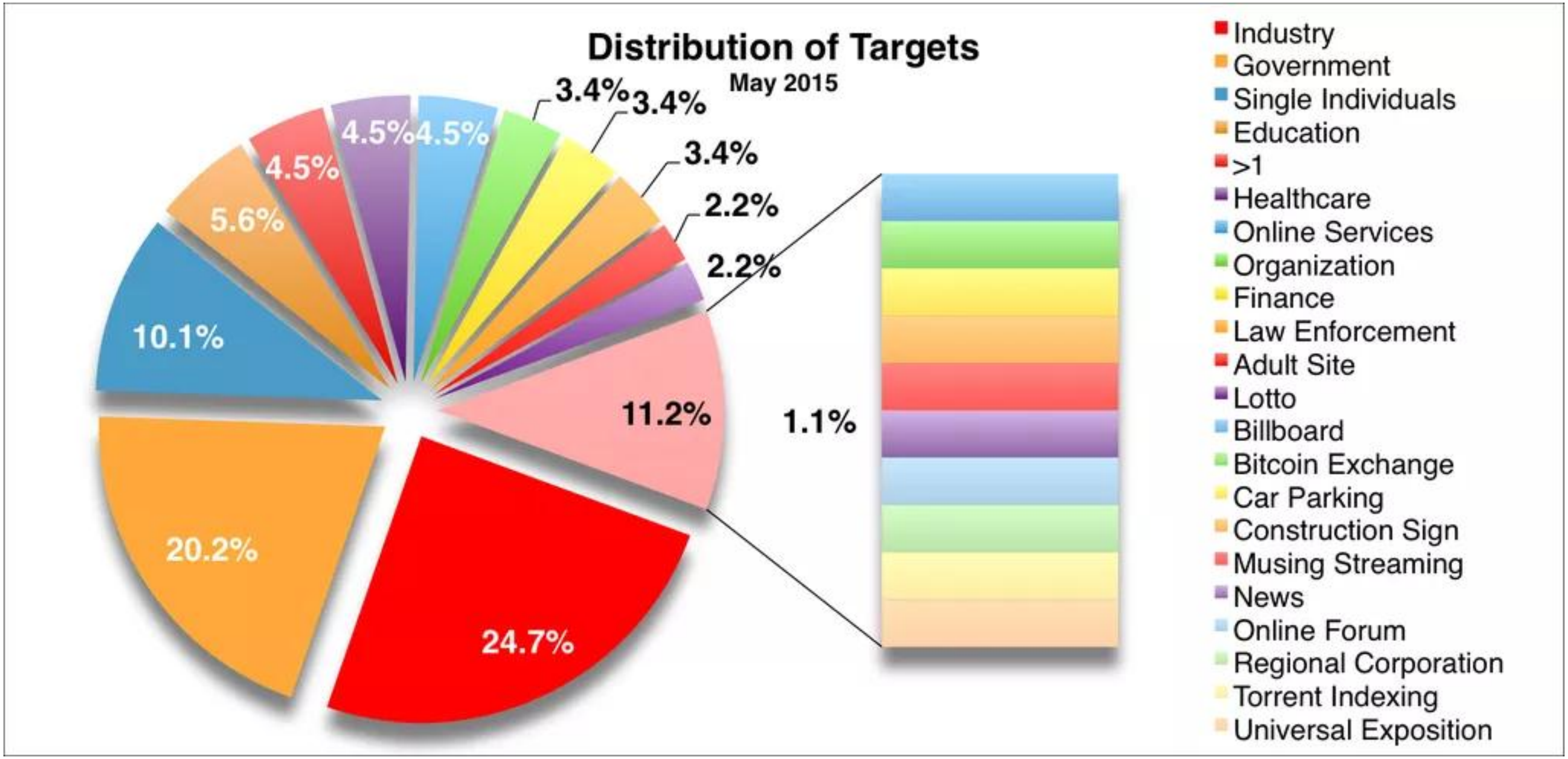
Cyber Attacks

- The Internet was not originally designed with security in mind. Without strong investments in cybersecurity and cyber defenses, data systems remain open and susceptible to rudimentary and dangerous forms of exploitation and attack.
- Malicious actors use cyberspace to steal data and intellectual property for their own economic or political goals. And an actor in one region of the globe can use cyber capabilities to strike directly at a network thousands of miles away, destroying data, disrupting businesses, or shutting off critical systems.

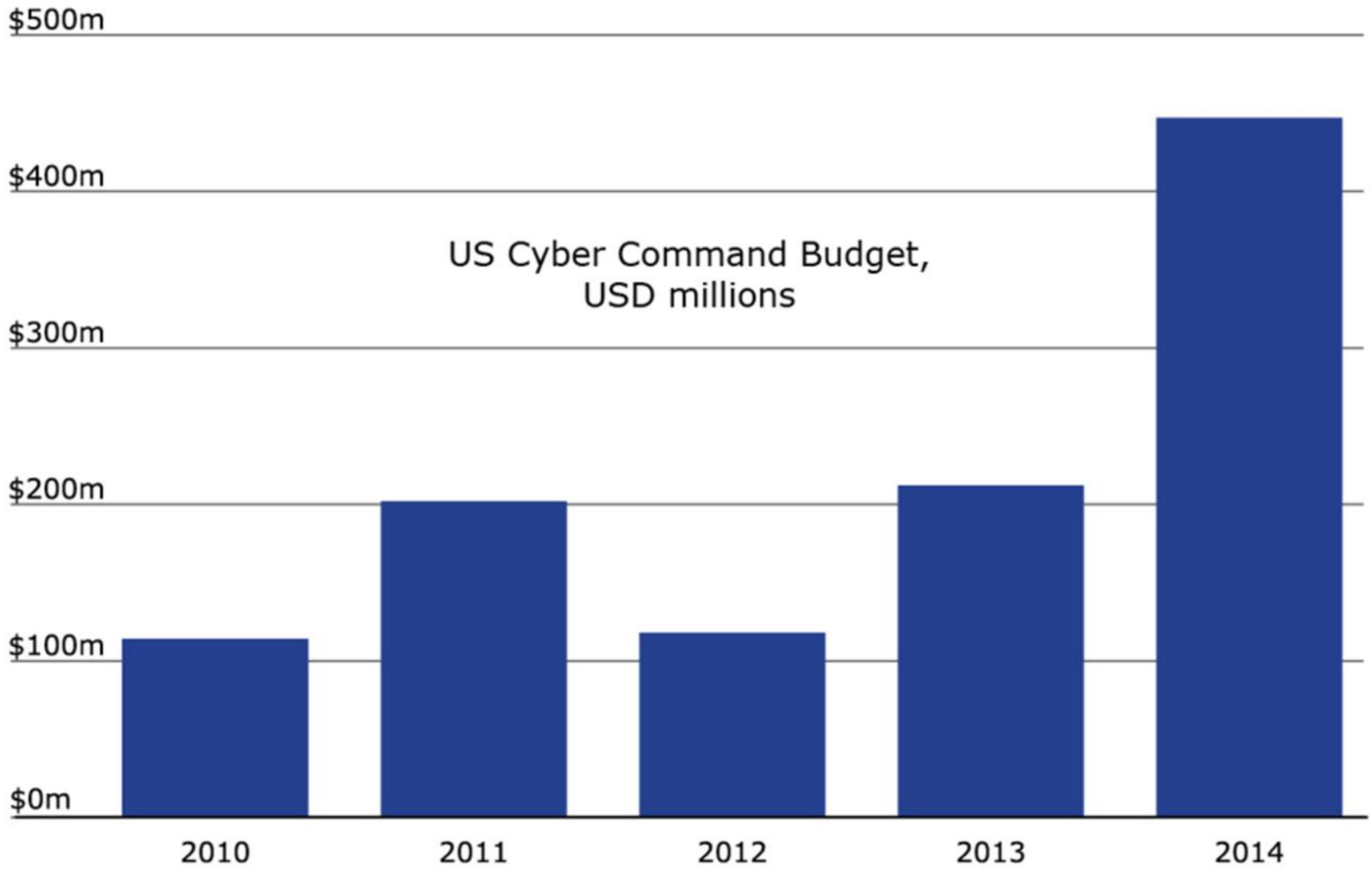
Slammer Worm

- **January 2003**
  Infects 90% of vulnerable computers within 10 minutes
- **Effect of the Worm**
  - Interference with elections
  - Cancelled airline flights
  - 911 emergency systems affected in Seattle
  - 13,000 Bank of America ATMs failed
- **Estimated ~$1 Billion in productivity loss**

- In 2009, Aurora Operation , hackers seeking source code from Google, Adobe and dozens of other high-profile companies used unprecedented tactics that combined encryption, stealth programming and an unknown hole in Internet Explorer
- WikiLeaks has posted a video on its website which it claims shows the killing of civilians by the US military in Baghdad in 2007.
- In August 2012, hackers attacked the networks of Saudi Aramco, destroying data on some 30,000 of the company’s computers.
- Then in November, Chevron revealed that it had been infected by Stuxnet, the malware the United States in November, 2014, North Korea conducted a cyberattack against Sony Pictures Entertainment

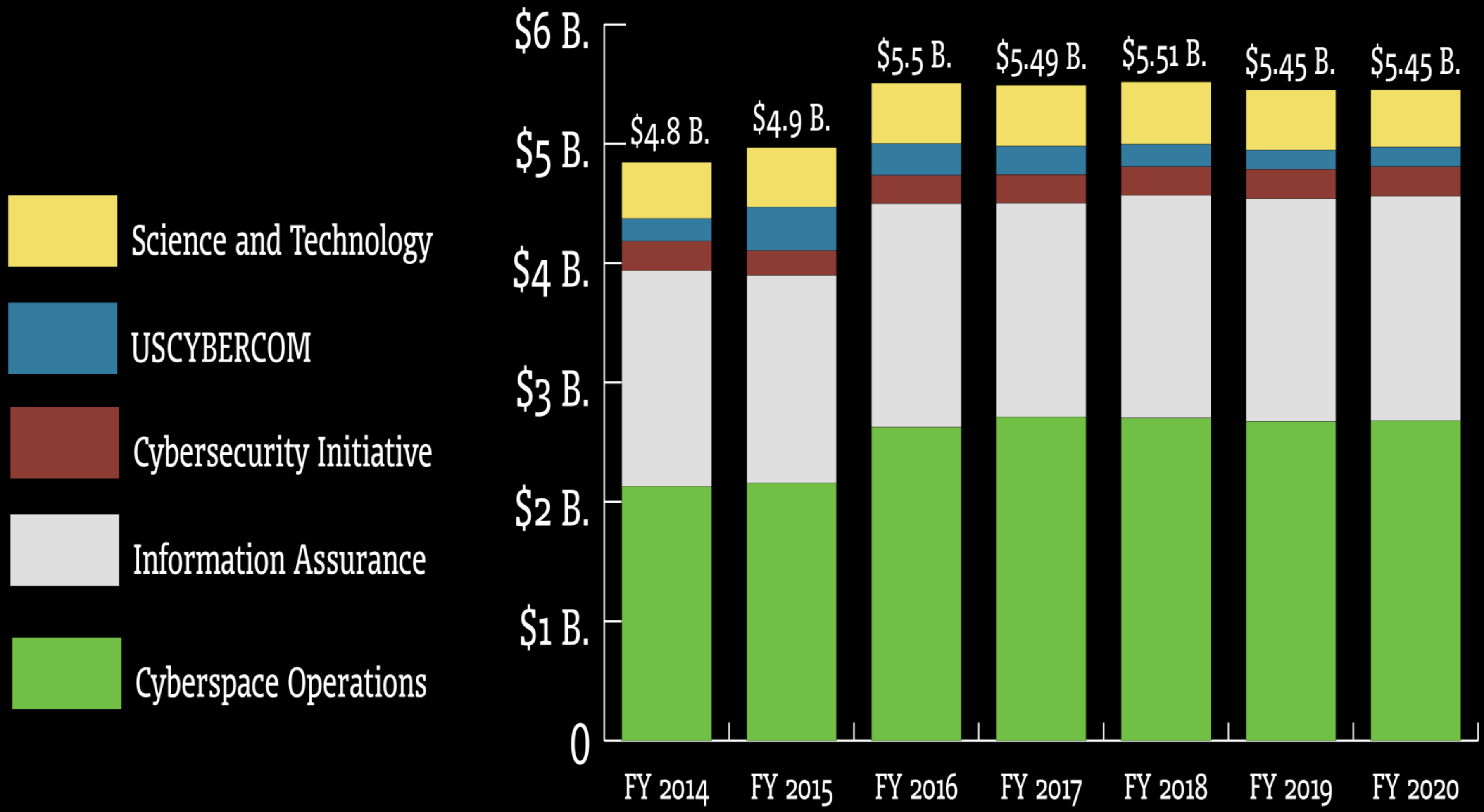

Distribution of Targets
May 2015
24.7%
20.2%
10.1%
5.6%
4.5%
4.5%
4.5%
3.4%
3.4%
3.4%
2.2%
2.2%
11.2%
1.1%
Industry
Government
Single Individuals
Education
>1
Healthcare
Online Services
Organization
Finance
Law Enforcement
Adult Site
Lotto
Billboard
Bitcoin Exchange
Car Parking
Construction Sign
Musing Streaming
News
Online Forum
Regional Corporation
Torrent Indexing
Universal Exposition

A soaring cyber-security budget



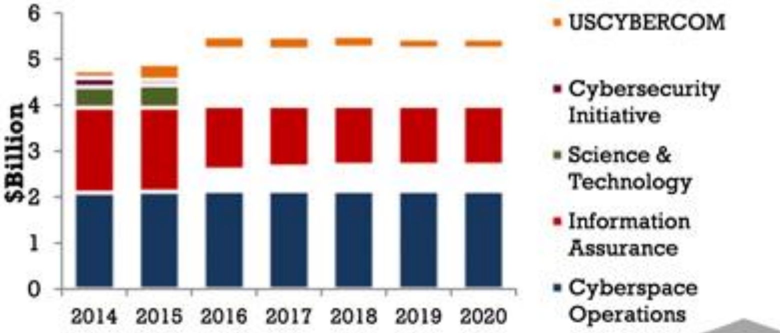
Source: Washington Post (2010-2013), House Appropriations Committee (2014)

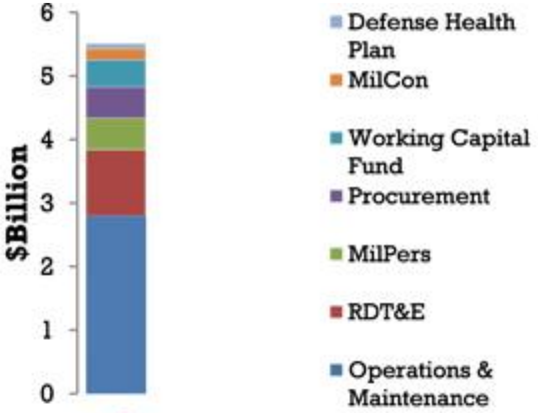
Total Defense Department Cyber Spending



Nextgov | nextgov.com

Source: *Defense Department*



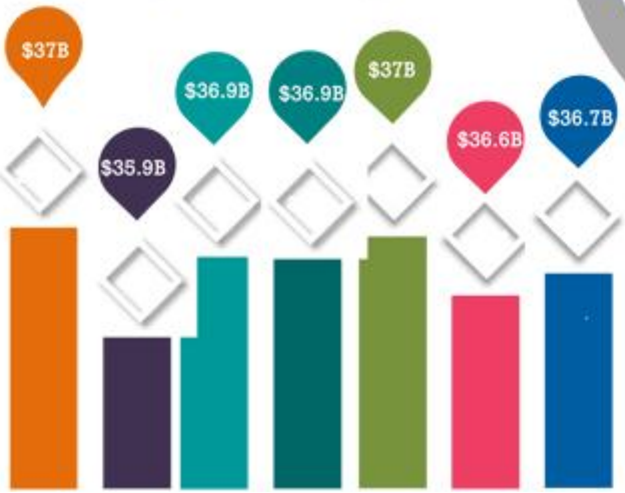


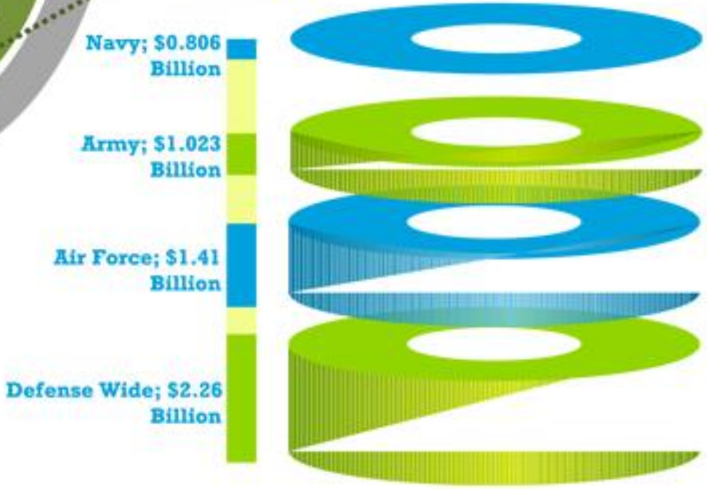
Total Defense Department Cyber Spending

Composition of FY2016 Cyber Budget

Department Breakdown of FY2016 Cyber Budget

Defense Department IT Budget





(1) The National Strategy to Secure Cyberspace (2003)

- The National Strategy to Secure Cyberspace established three strategic objectives for national cyberspace security: preventing cyber attacks against national critical infrastructures; reducing national vulnerability to cyber attacks; and minimising damage and recovery time from cyber attacks that do occur

(2)Department of Defense Strategy for Operating in Cyberspace (2015)

- It focuses on building capabilities for effective cybersecurity and cyber operations to defend DoD networks, systems, and information; defend the nation against cyberattacks of significant consequence; and support operational and contingency plans
- Cyber Security Activities : Information sharing and interagency coordination, build bridges to the private sector, Building alliances, coalitions, and partnerships abroad.
- Three Primary Missions in Cyberspace : (1) DoD must defend its own networks, systems, and information.(2) DoD must be prepared to defend the United States and its interests against cyberattacks of significant consequence. (3) DoD must be able to provide integrated cyber capabilities to support military operations and contingency plans

3. Department Of State International Cyberspace Policy Strategy (2016)

- President's 2011 U.S. International Strategy for Cyberspace (International Strategy), efforts to promote norms of state behavior in cyberspace, alternative concepts for norms promoted by certain other countries, threats facing the United States, tools available to the President to deter malicious actors, and resources required to build international norms.
- The Strategy, prepared by the Department of State, is being submitted to the Committee on Foreign Relations of the United States Senate and the Committee on Foreign Affairs of the House of Representatives.
- to promote an open, interoperable, secure, and reliable information and communications infrastructure that supports international trade and commerce, strengthens international security, and fosters free expression and innovation."

International Cyberspace Policy Strategy (2016) Accomplishments

- Digital economy
- International Security
- Promoting Cybersecurity Due Diligence
- Combating Cybercrime
- Internet Governance
- Internet Freedom
- International Development and Capacity Building
- Global, Cross-Cutting Cyber Issues
- Mainstreaming Cyber Issues within the Department of State