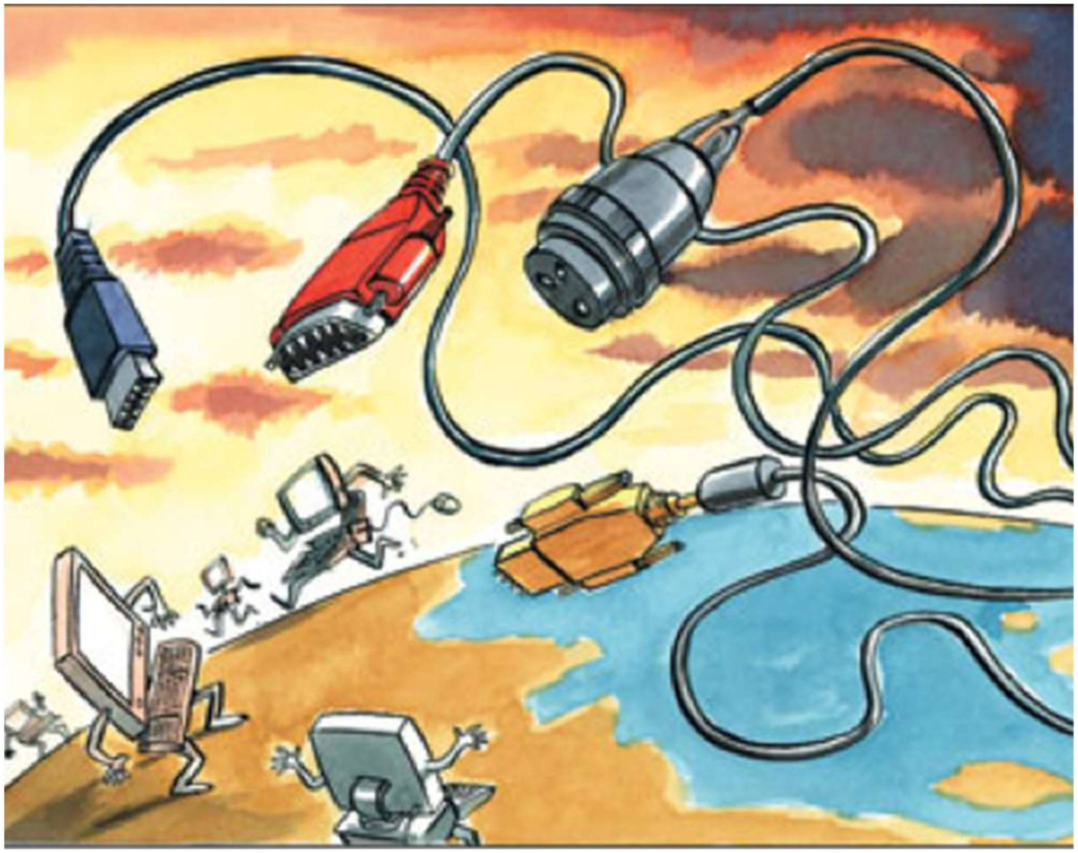
Cybersecurity: A Policy Perspective on Government Efforts to Make Cyberspace Open, Interoperable, Secure and Reliable

Senior Statesmen of Virginia

March 13, 2019



Cybersecurity Presentation Outline

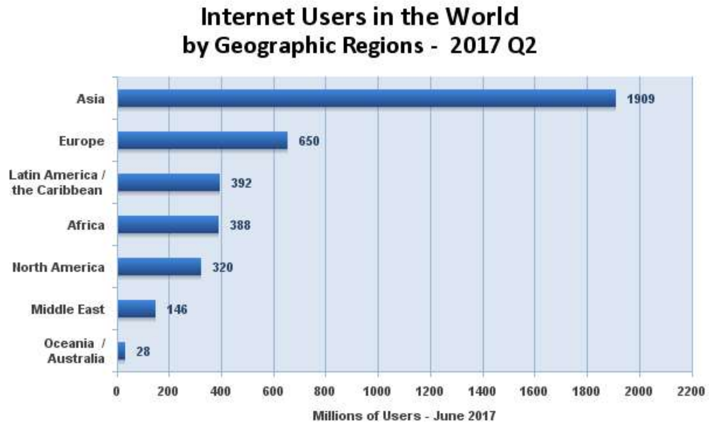
- Introduction, Threats and Definitions
- Cybersecurity and Protecting Critical Infrastructure
- Cybercrime and Digital Investigations
- Internet Governance
- Big Data and Privacy
- International Security
- Internet Freedom
- Cybersecurity in the Commonwealth of Virginia

Introduction, Threats and Definitions

Cybersecurity Issues We Will Examine

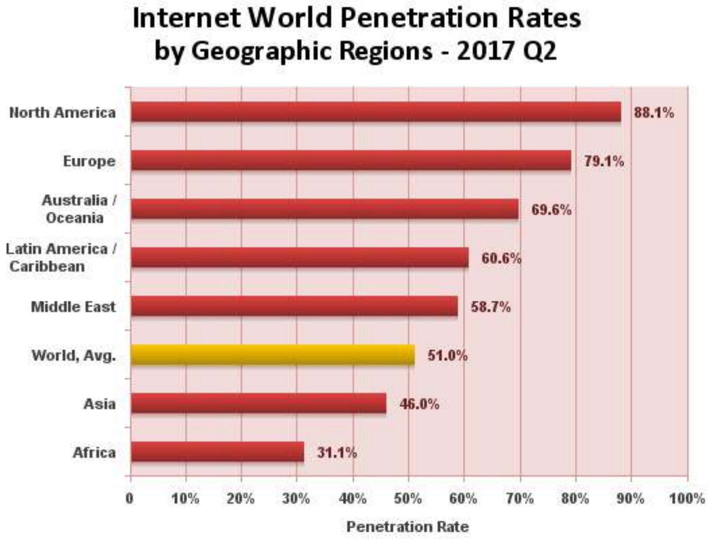
- What are the major cybersecurity threats and challenges facing us in 2019 and beyond?
- What is the policy framework for global cybersecurity issues?
- What are the U.S. Government's primary roles and responsibilities?
- What is the Commonwealth of Virginia doing to tackle cybersecurity?

The Connected World



Internet Users in the World
by Geographic Regions - 2017 Q2

Source: Internet World Stats - www.internetworldstats.com/stats.htm
Basis: 3,835,498,274 Internet users estimated in June 30, 2017
Copyright © 2017, Miniwatts Marketing Group



Internet World Penetration Rates
by Geographic Regions - 2017 Q2

Source: Internet World Stats - www.internetworldstats.com/stats.htm
Penetration Rates are based on a world population of 7,519,028,970
and 3,835,498,274 estimated Internet users in June 30, 2017.
Copyright © 2017, Miniwatts Marketing Group

Cybersecurity Threats

U.S. Intelligence Community Worldwide Threat Assessment (January 2019)

- Our adversaries and strategic competitors will increasingly use cyber capabilities – including cyber espionage, attack, and influence – to seek political, economic, and military advantage over the United States and its allies and partners.
- Foreign cyber criminals will continue to conduct for-profit, cyber-enabled theft and extortion against U.S. networks.
- Our adversaries and strategic competitors probably already are looking to the 2020 U.S. elections as an opportunity to advance their interests [and] almost certainly will use online influence operations to try to weaken democratic institutions, undermine U.S. alliances and partnerships, and shape policy outcomes in the U.S. and elsewhere.

U.S. International Strategy for Cyberspace (2011)

U.S. seeks a cyberspace that is open, interoperable, secure & reliable.

- Economy: Promoting int’l standards and innovation, open markets
- Protecting our Networks: Enhancing security, reliability & resiliency
- Law Enforcement: Extending collaboration and the rule of law
- Military: Preparing for 21st century security challenges
- Internet Governance: Promoting effective and inclusive structures
- International Development: Building capacity, security & prosperity
- Internet Freedom: Supporting fundamental freedoms and privacy

Definitions

- Internet: A global computer network providing a variety of information and communications facilities, consisting of interconnected networks – plus cellular technologies, fiber-optic cables, space-based communications and related infrastructure – using standardized communication protocols.

- Cyberspace: The realm of computer networks - and the users behind them - in which information is stored, shared and communicated online.

- Cybersecurity: The process of protecting information and information systems by preventing, detecting and responding to unauthorized access, use, disclosure, disruption, modification or destruction, in order to provide confidentiality, integrity and availability.

Cybersecurity and Protecting Critical Infrastructure

Commission on Enhancing National Cybersecurity (2016)

- Areas of focus: critical infrastructure, the Internet of Things (IoT), research and development (R&D), public awareness and education, governance, workforce, state and local issues, identity management and authentication, insurance, international issues, and the role of small and medium-sized businesses.
- Trends: convergence of information technologies and physical systems, risk management, privacy and trust, global versus national realms of influence and controls, the effectiveness of free markets versus regulatory regimes and solutions, legal and liability considerations, the importance and difficulty of developing meaningful metrics for cybersecurity, automated technology-based cybersecurity approaches, and consumer responsibilities.
- Key Take-Aways: (1) Partnerships (esp. public-private) are vital; and (2) Resilience and Risk Management must be the core of cybersecurity strategies and practices.

Commission on Enhancing National Cybersecurity (2016)

Recommendations and Action Items:

- Protect, defend and secure information infrastructure and networks
- Innovate and accelerate investment for the security and growth of digital networks and the digital economy
- Prepare consumers to thrive in a digital age
- Build cybersecurity workforce capabilities
- Better equip government to function effectively & securely
- Ensure an open, fair, competitive and secure global digital economy

POTUS & Congress Cybersecurity Guidance

- Executive Order 13800 “Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure” (May 2017)
- Presidential Policy Directive 41 “U.S. Cyber Incident Coordination” (July 2016): “significant cyber incident”
- NIST Cybersecurity Framework (February 2014)
- U.S. International Strategy for Cyberspace (May 2011)

- Cybersecurity Act of 2015: information sharing, workforce

Cybercrime and Digital Investigations

Cybercrime

- Cybercrime is:
  - Illegal access to computer systems
  - Interference with data or computer systems
  - Online identity theft
  - Digital intellectual property crimes
- Computers can also be used as a tool to commit “traditional” crimes
- The components of combating cybercrime: substantive offenses, investigative authorities/capabilities, international cooperation
- U.S. is a party to the Budapest Convention on Cybercrime

Digital Criminal Investigations

- Digital “fingerprints”: IP address / phone number
- Stored data: Subscriber data, Traffic data, Content data
- Real-time data: Traffic data, Content data
- Computer forensics

	Historical	**Prospective**
Non-content	Stored Communications Act	
Content	Stored Communications Act	Wiretap Act

Internet Governance

Internet Governance Key Concepts

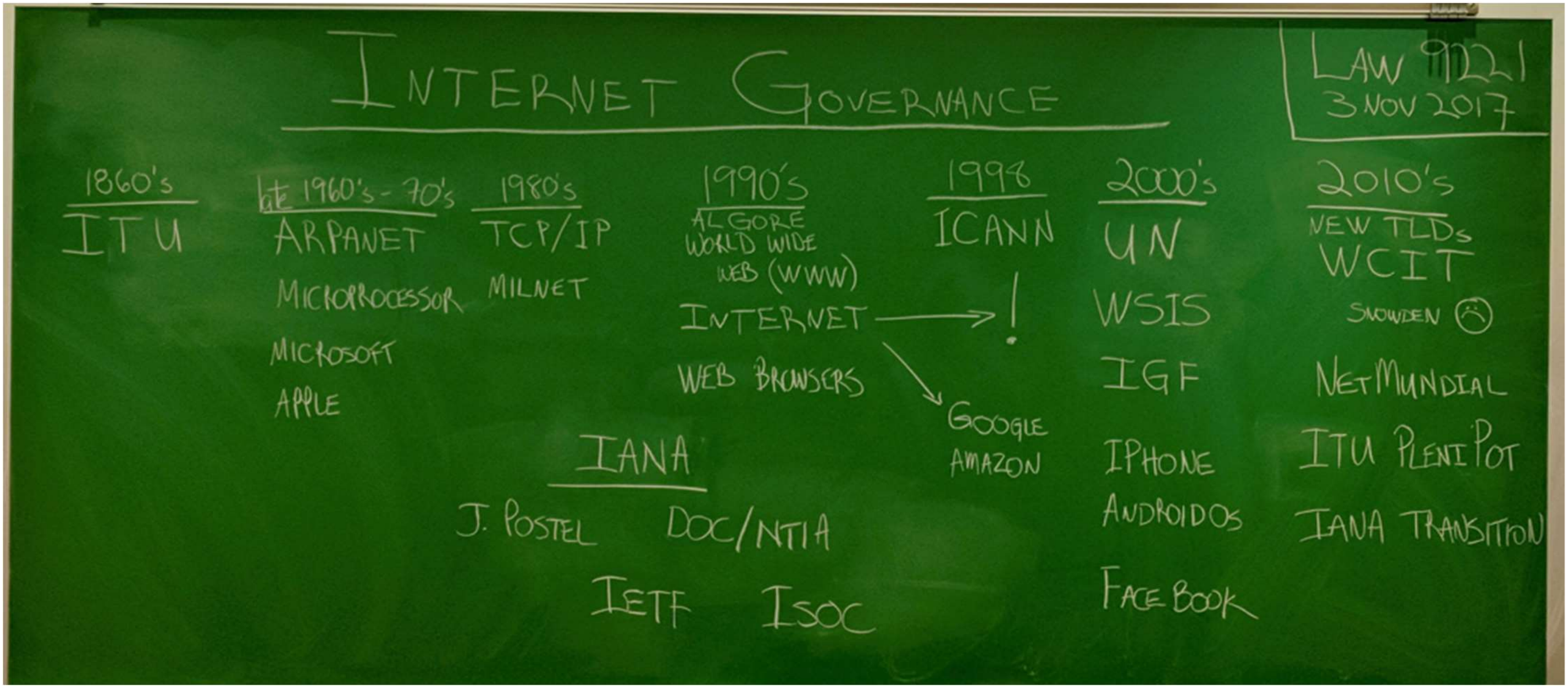
- Multi-stakeholder vs. Multi-lateral
- Technical standards & bodies
- IP addresses and their allocation … IPV6
    - 128.143.33.150 = www.virginia.edu
- Domain Name System (DNS)
- Top-Level Domains (TLDs) .com, gov. edu, org … plus many more starting in 2012

Internet Governance Definition & Key Functions

- Internet Governance defined: The administration and coordination of the technologies necessary to keep the Internet operational and the enactment of substantive policy around these technologies.

- Key functions of the Internet governance ecosystem:
    - Administration of critical Internet resources (e.g., names & numbers)
    - Establishment of Internet technical standards (e.g., TCP/IP, HTTP)
    - Access and interconnection coordination
    - Cybersecurity governance
    - Policy role of private information intermediaries
    - Architecture-based intellectual property rights enforcement

A Short History of Internet Governance



INTERNET GOVERNANCE

LAW 9221
3 NOV 2017

1860's
ITU

late 1960's - 70's
ARPANET
MICROPROCESSOR
MICROSOFT
APPLE

1980's
TCP/IP
MILNET

1990's
AL GORE
WORLD WIDE WEB (WWW)
INTERNET → !
WEB BROWSERS

IANA
J. POSTEL
DOC/NTIA
IETF
ISOC

1998
ICANN
!
GOOGLE
AMAZON

2000's
UN
WSIS
IGF
IPHONE
ANDROID OS
FACEBOOK

2010's
NEW TLDs
WCIT
SNOWDEN ☹
NETMUNDIAL
ITU PLENIPOT
IANA TRANSITION

Destabilizing Internet Governance Trends*

- A loss of trust in cyberspace
- Domain Name System as a proxy for broader geopolitical conflict
- Uncertainty over transition of U.S. oversight
- Attempts to overlay national borders on the global Internet
- Resurgence of proprietary and content-discriminatory approaches

- *Thanks to Professor Laura Denardis

Big Data and Privacy

U.S. National Security Strategy on Data

“Data, like energy, will shape U.S. economic prosperity and our future strategic position in the world. The ability to harness the power of data is fundamental to the continuing growth of America’s economy, prevailing against hostile ideologies, and building and deploying the most effective military in the world.” (page 3)

Big Data Defined

- Big Data Report (Exec. Office of the President, May 2014)
- “Big Data is big in two different senses. It is big in the quantity and variety of data that are available to be processed. And it is big in the scale of analysis (termed “analytics”) that can be applied to those data, ultimately to make inferences and draw conclusions.” President’s Council of Advisors on Science and Technology (PCAST) report on “Big Data and Privacy: A Technological Perspective” (May 2014)
- The “3 V’s” of Big Data: Volume, Variety and Velocity

Big Data Report Recommendations

- Preserving Privacy Values: Maintaining our privacy values by protecting personal information in the marketplace, both in the United States and through interoperable global privacy frameworks;
- Educating Robustly and Responsibly: Recognizing schools as an important sphere for using big data to enhance learning opportunities, while protecting personal data usage and building digital literacy/skills;
- Big Data and Discrimination: Preventing discrimination enabled by big data;
- Law Enforcement and Security: Ensuring big data's responsible use in law enforcement, public safety, and national security; and
- Data as a Public Resource: Harnessing data as a public resource, using it to improve the delivery of public services, and investing in research and tech that will further power the big data revolution.

U.S. Privacy Laws & Regulations

- U.S. Constitution, Fourth Amendment: In 1967, the Supreme Court ruled in *Katz v. United States*, that an individual’s subjective expectations of privacy are protected when society regards them as reasonable.
- The U.S. does not have a broad, general law governing privacy rights.
- The U.S. does have sector specific privacy laws, such as:
    - Fair Credit Reporting Act (FCRA)
    - Health Insurance Portability and Accountability Act (HIPAA)
    - Family Educational Rights and Privacy Act (FERPA)
- The Privacy Act and Freedom of Information Act apply to personal data the U.S. Government collects and maintains on individuals.

European Union (EU) General Data Protection Regulation (GDPR)(May 2018)

GDPR expanded EU’s protections for personal data & use:

- Expanded extraterritoriality: Applies to all companies globally that process personal data of EU residents
- Penalties: Fines up to 4% of annual global revenue
- Consent: Companies no longer able to use long, illegible terms and conditions full of legalese; must be as easy to withdraw consent as to give it

EU GDPR Data Subject Rights

- Breach Notification: Data breach notifications are mandatory within 72 hours
- Right to Access: Individuals have the right to be informed whether, where and for what purpose their data is being processed & receive an electronic copy
- Right to be Forgotten: Enshrines the right for an individual to have their data erased if no longer relevant, consent withdrawn, etc.
- Data Portability: Individual has the right to receive a machine readable copy of their data and transfer it to another processor
- Privacy by Design: Data protection must be built into systems
- Data Protection Officers: Large-scale data processors required to create internal data processing compliance programs overseen by a Data Protection Officer

International Security

What is a Cyber Attack?

A cyber-attack consists of any action taken to undermine the functions of a computer network for a political or national security purpose.

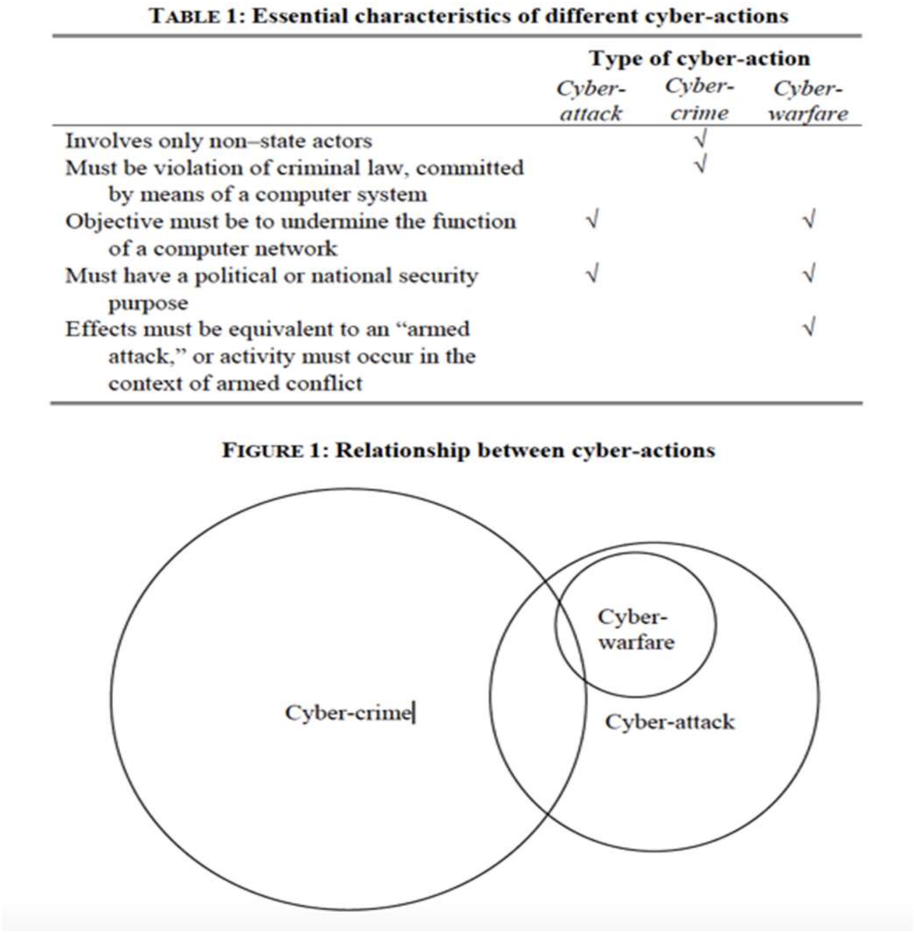


TABLE 1: Essential characteristics of different cyber-actions

	Type of cyber-action		
	Cyber-attack	*Cyber-crime*	*Cyber-warfare*
Involves only non–state actors		√	
Must be violation of criminal law, committed by means of a computer system		√	
Objective must be to undermine the function of a computer network	√		√
Must have a political or national security purpose	√		√
Effects must be equivalent to an "armed attack," or activity must occur in the context of armed conflict			√

FIGURE 1: Relationship between cyber-actions

Law of War and Cyber Attack

- *Jus ad Bellum* is the law that regulates the use of force by States.
- *Jus in Bello* is the law that governs how States may conduct their military operations during an armed conflict and provides protections for various specified persons, objects and activities.
- Geneva Conventions - last revised in 1949 - address status of combatants, protected persons and related issues.
- The United Nations Charter entered into force on 24 October 1945; Article 1(1) of the UN Charter states that the primary purpose of the United Nations is “To maintain international peace and security …”

U.S. Department of Defense Cyberspace Objectives

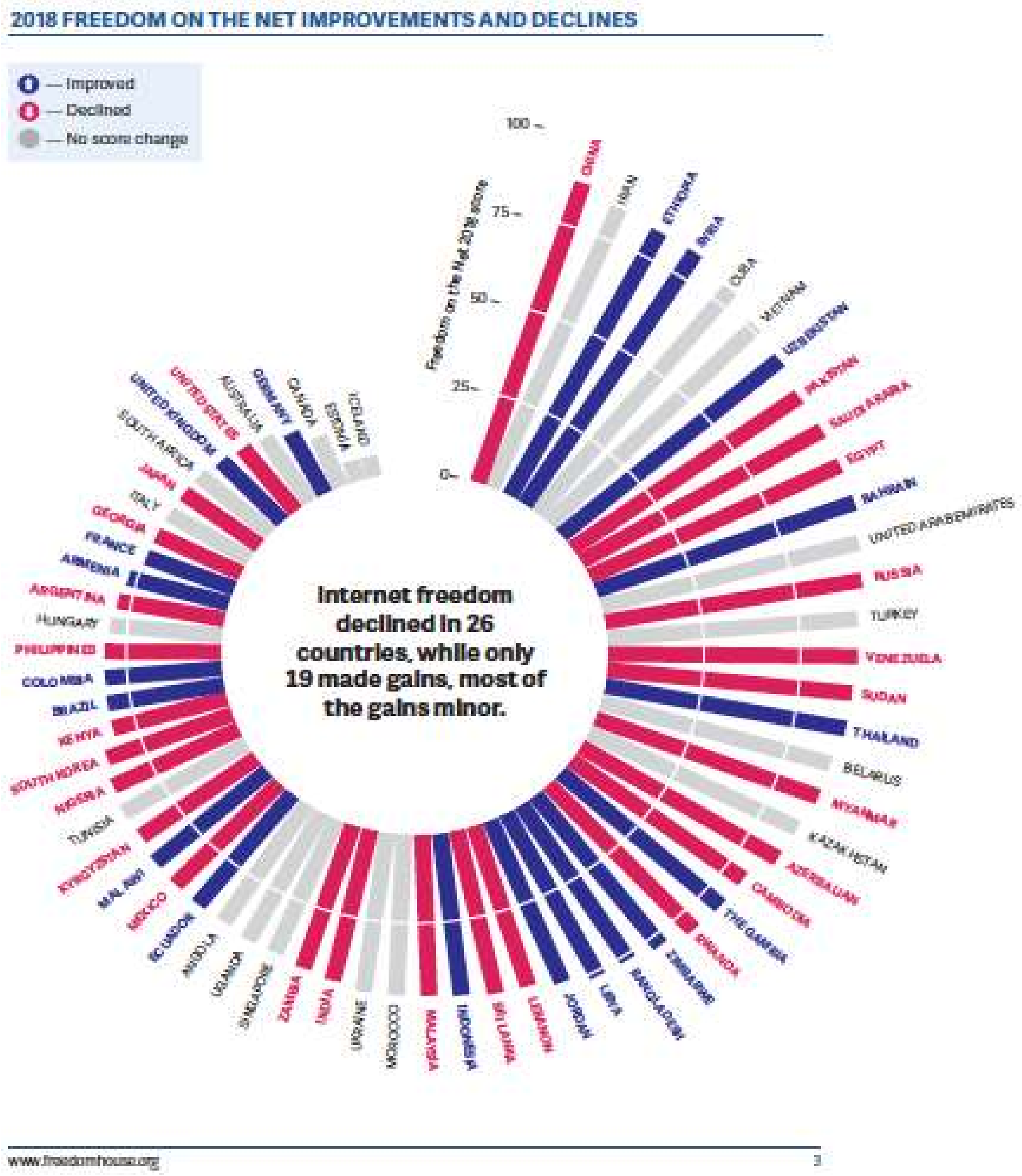
- Ensure the Joint Force can achieve its missions in a contested cyberspace environment;
- Strengthen the Joint Force by conducting cyberspace operations that enhance U.S. military advantages;
- Defend U.S. critical infrastructure from malicious cyber activity that alone, or as part of a campaign, could cause a significant cyber incident;
- Secure DoD information and systems against malicious cyber activity, including DoD information on non-DoD-owned networks; and
- Expand DoD cyber cooperation with interagency, industry and international partners

Cyberspace Treaty?

- There are numerous bilateral and multilateral agreements between/among the major global powers
  - U.S. – Russia (2013) and U.S. – China (2015)
  - Russia – China (2016)
  - Shanghai Cooperation Organization “International Code of Conduct for Information Security” (2011, revised 2015)
  - Budapest Cybercrime Convention (2001)
- What about a UN Treaty for cyberspace?

Internet Freedom

Freedom House 2018 Freedom on the Net Rankings



2018 FREEDOM ON THE NET IMPROVEMENTS AND DECLINES

www.freedomhouse.org 3

Cybersecurity in the Commonwealth of Virginia

National Governors Association Cyber Initiatives

Four primary cybersecurity focus areas for states:

- Fusion centers add cybersecurity missions by leveraging homeland security, emergency management, information technology and law enforcement capabilities
- Workforce development to address needs of business community and state government
- Energy systems/infrastructure cybersecurity
- Coordinating state and federal government cyber efforts with a focus on information sharing

Former Virginia Governor McAuliffe was chair of NGA 2016-2017 and made cybersecurity his signature issue.

Virginia State Govt. Cybersecurity Initiatives

- Virginia Cyber Security Commission (2014)
- Virginia Cybersecurity Strategy (2016)
- cyberva.virginia.gov cyber portal
- Virginia Information Technologies Agency (VITA)
- Attorney General of Virginia
- Virginia Department of Public Safety
- Virginia Fusion Center within Virginia State Police
- Virginia National Guard: NGCS + local government cyber assessments
- Virginia Department of Emergency Management

Questions?

Thomas Dukes

Adjunct Professor, University of Virginia School of Law and Batten School of Leadership and Public Policy

tdukes@law.virginia.edu