LEARNING Webinar

Welcome

This webcast is part of ACM’s commitment to lifelong learning.

- To control volume, please adjust the **master volume on your computer**.
- The **slides will advance automatically** throughout the event.
- You may **enlarge the slides** using the button in the top right corner of the screen or by dragging the corner of the slide window.
- You may **submit questions at any time** by typing your question into the Q&A box and clicking the submit button. You do not need to wait until the end of the presentation to begin submitting questions.
- The session is being **recorded** and will be **archived**.
- **Troubleshooting**

  Windows Press **F5** key

  Mac **Command + R**

  Refresh your browser / Relaunch the presentation

  Click the **“Help” widget** below the slide window.

@ACMeducation
#cybersecurity

Today’s Speakers

Herb Lin

Chief Scientist, Computer Science and Telecommunications Board, National Research Council

Jeremy Epstein

Moderator

Lead Program Officer, National Science Foundation Secure and Trustworthy Cyberspace program; ACM Senior Member

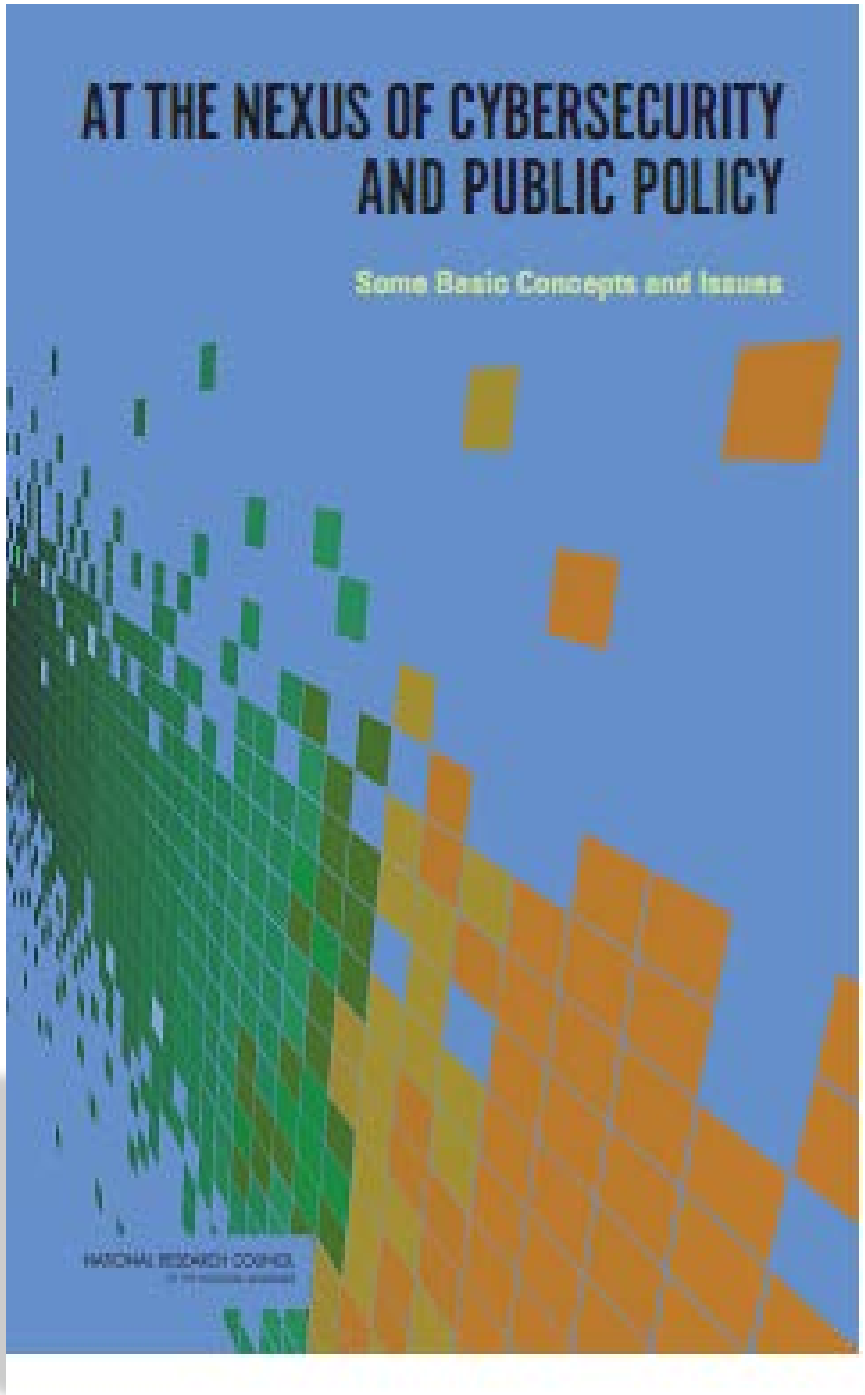
At the Nexus of Cybersecurity and Public Policy

Six Key Issues

Herb Lin

National Research Council

2014 National Research Council Report


AT THE NEXUS OF CYBERSECURITY AND PUBLIC POLICY

Some Basic Concepts and Issues

NATIONAL RESEARCH COUNCIL

Editors

David Clark

Tom Berson

Herb Lin

www.nap.edu

Online, May 5, 2014

Printed ($), June 18, 2014

About the Report

- **Builds on earlier work** by the Computer Science and Telecommunications Board (CSTB) of the National Research Council of the National Academies
- Describes **fundamental concepts** and **principles** of cybersecurity
- Discusses a **range of public policy issues**
- Explains **technical details** in an easy-to-understand manner for non-technical audiences
- Includes **input from cybersecurity experts** from government, industry, organizations, and academia

What are we talking about today?

A. **Why should we care about cybersecurity?**

- What is cybersecurity? What is its significance for public policy?

B. **Understanding the threats, vulnerabilities, and risks**

- What types of cyber threats and vulnerabilities exist? What does it mean to be an adversary in cyberspace?

C. **What policy approaches will help improve security?**

- Is public policy needed to address market failure? What are the major tensions between cybersecurity and other important public policies? How do U.S. public policies relate to international issues?

D. **What you should know about the 6 KEY FINDINGS from the report!**

Why should we care about cybersecurity?

What is cyberspace?

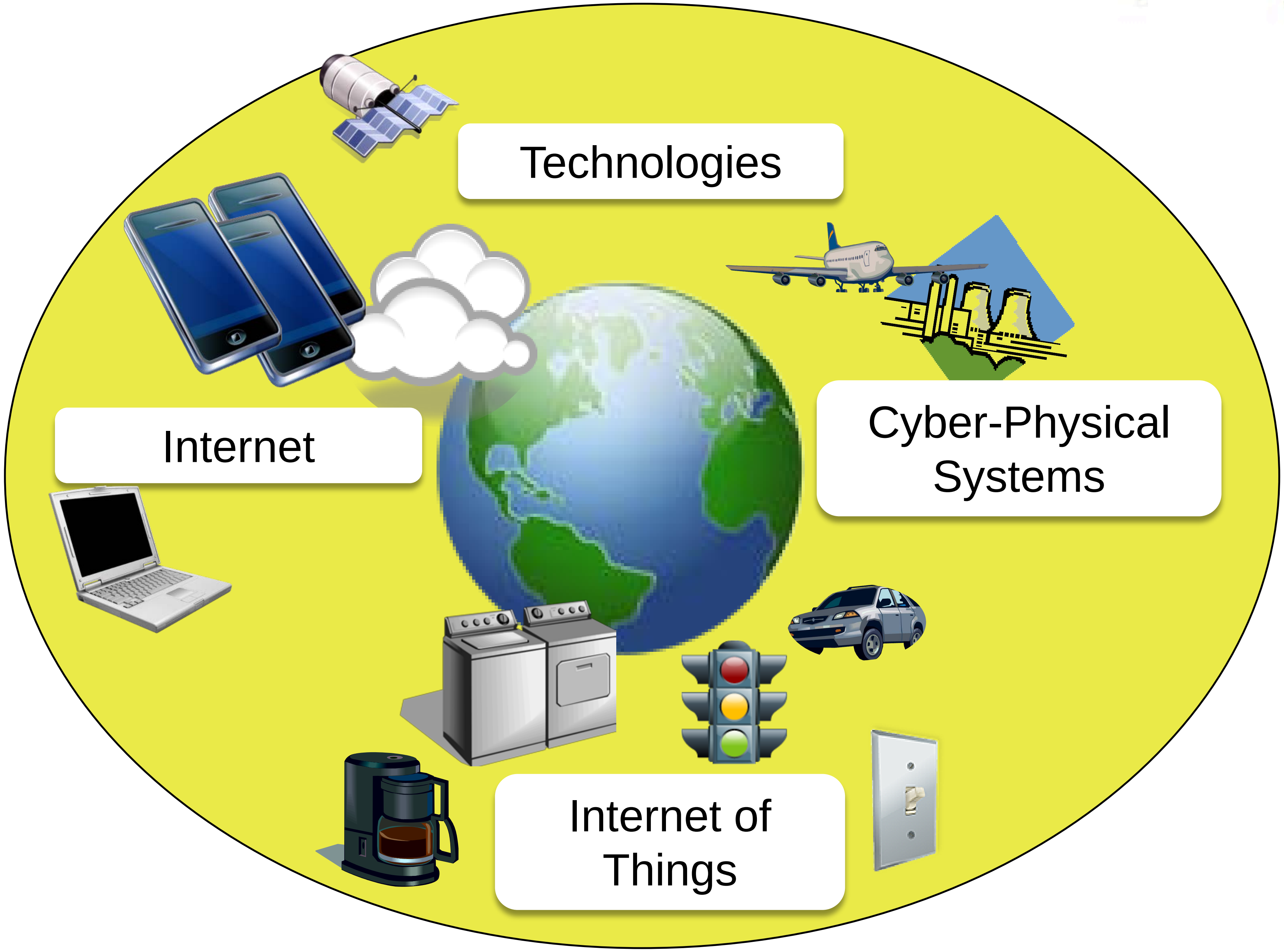
What is cybersecurity?

Some important questions at the nexus

Why should we care about cybersecurity?

What is cyberspace? | **What is cybersecurity?** | **Some important questions at the nexus**

- Artifacts based on or dependent on **computer** and **communications technology**
- Information - **data and programs** - that these artifacts use, store, handle, or process
- The various ways cyber elements are **connected**.



Technologies

Internet

Cyber-Physical Systems

Internet of Things

Why should we care about cybersecurity?

What is cyberspace?	What is cybersecurity?	Some important questions at the nexus

- Artifacts **based on** or **dependent on** computer and communications technology
- Information - data and programs - that these artifacts **use, store, handle**, or **process**
- The various ways cyber elements are **connected**.

The prevention and/or reduction of the negative impact of events in **cyberspace** that can happen as the result of DELIBERATE ACTIONS against information technology by a **hostile** or **malevolent** actor.

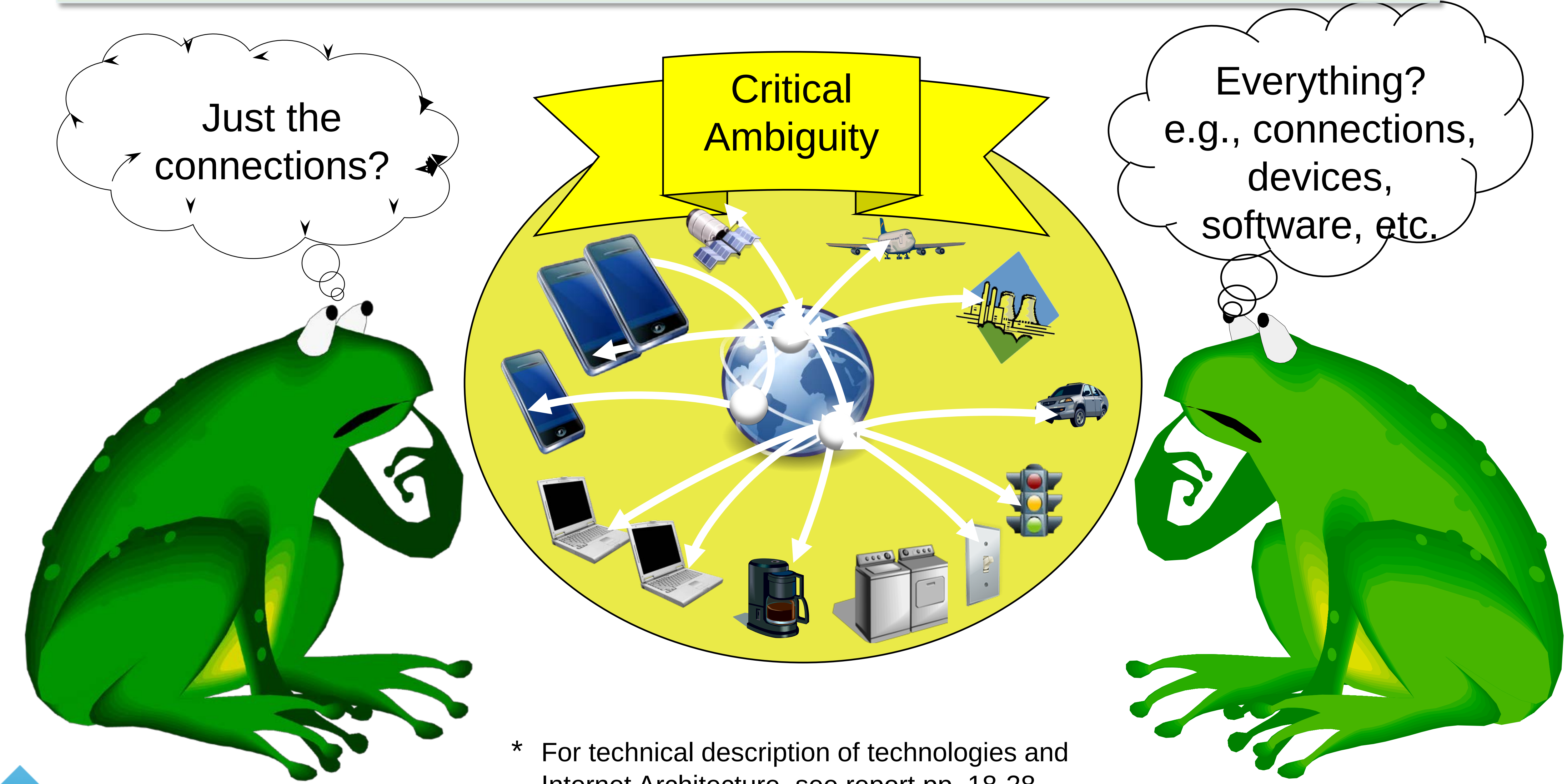
Why should we care about cybersecurity?

What is cyberspace?

What is cybersecurity?

Some important questions at the nexus

What is the scope of INTERNET security?



Just the connections?

Critical Ambiguity

Everything? e.g., connections, devices, software, etc.

* For technical description of technologies and Internet Architecture, see report pp. 18-28

Why should we care about cybersecurity?

What is cyberspace?

- Artifacts **based on** or **dependent on** computer and communications technology
- Information - data and programs - that these artifacts **use, store, handle**, or **process**
- The various ways cyber elements are **connected**.

What is cybersecurity?

The prevention and/or reduction of the negative impact of events in **cyberspace** that can happen as the result of **deliberate actions** against information technology by a **hostile** or **malevolent** actor.

Some important questions at the nexus

- How much reduction or prevention is enough?
- Who decides?
- What counts as negative impact or deliberate action?
- Whose information technology?
- What makes an actor hostile or malevolent?
- What does enhancing cybersecurity mean for civil liberties, privacy, innovation, the economy, and more?

Association for Computing Machinery

Advancing Computing as a Science & Profession

Why should we care about cybersecurity?

What is cyberspace? | What is cybersecurity? | Some important questions at the nexus

Why are policy leaders concerned?

- Cybercrime
- Loss of privacy
- Activism
- Appropriation of intellectual property
- Espionage
- Denials of service
- Destruction of or damage to physical property and/ or critical infrastructure
- Loss of public confidence

IMPACTS

- Economics
- Innovation
- Civil Liberties
- International Relations

Understanding the threats, vulnerabilities, and risks

- What are the major types of cyber threats?
- What types of vulnerabilities exist?
- Who is an adversary in cyberspace?

Understanding the threats, vulnerabilities, and risks

What are the major types of cyber threats?

What types of vulnerabilities exist?

Who is an adversary in cyberspace?

Exploitation – unauthorized exfiltration of information (violation of confidentiality)

Attack – unauthorized exfiltration of information

- **Deny availability of service** (violation of availability)
- Damage or destroy **information stored in or transiting** through that system or network (violation of integrity)
  - May cause physical damage as a result

Cyber threats can **damage** or **destroy** information **at rest** or **in transit**.

Association for Computing Machinery

Advancing Computing as a Science & Profession

Understanding the threats, vulnerabilities, and risks

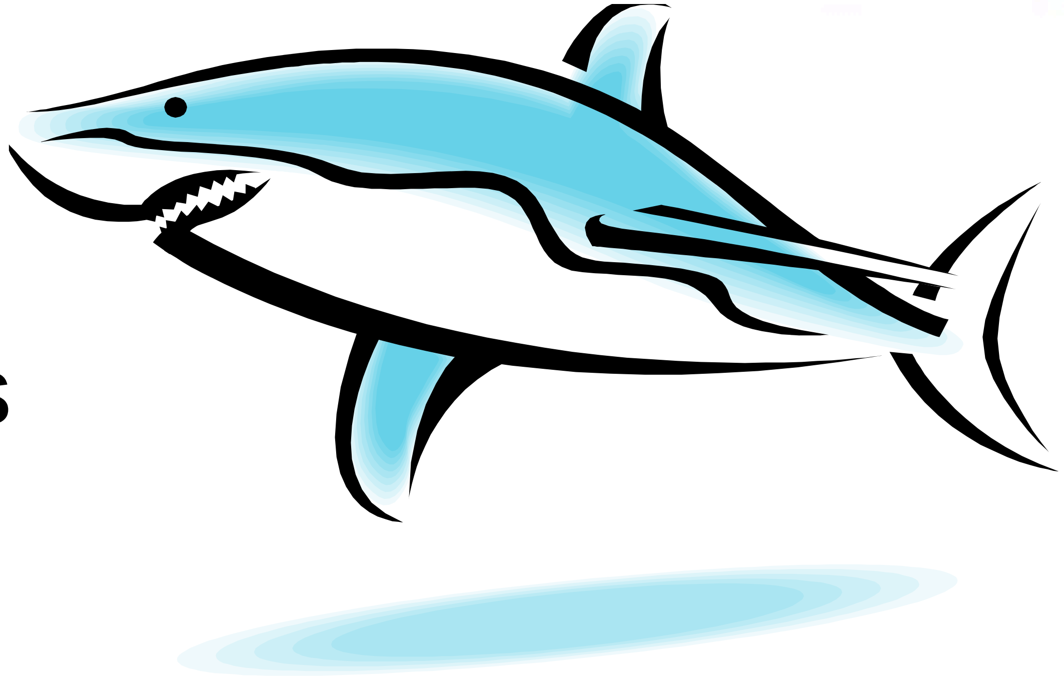
What are the major types of cyber threats?

- **Any** hostile or unfriendly **action** taken against a computer system or network.
- **Any** hostile or unfriendly **cyber action** taken against a computer system or network.
- **Only** hostile or unfriendly action taken against a computer system or network intended to **cause a denial of service** or **damage to** or destruction of information **stored in** or **transiting through** that system or network.

What types of vulnerabilities exist?

- People
- Systems
- Components
- Connections

Who is an adversary in cyberspace?



Association for Computing Machinery

Advancing Computing as a Science & Profession

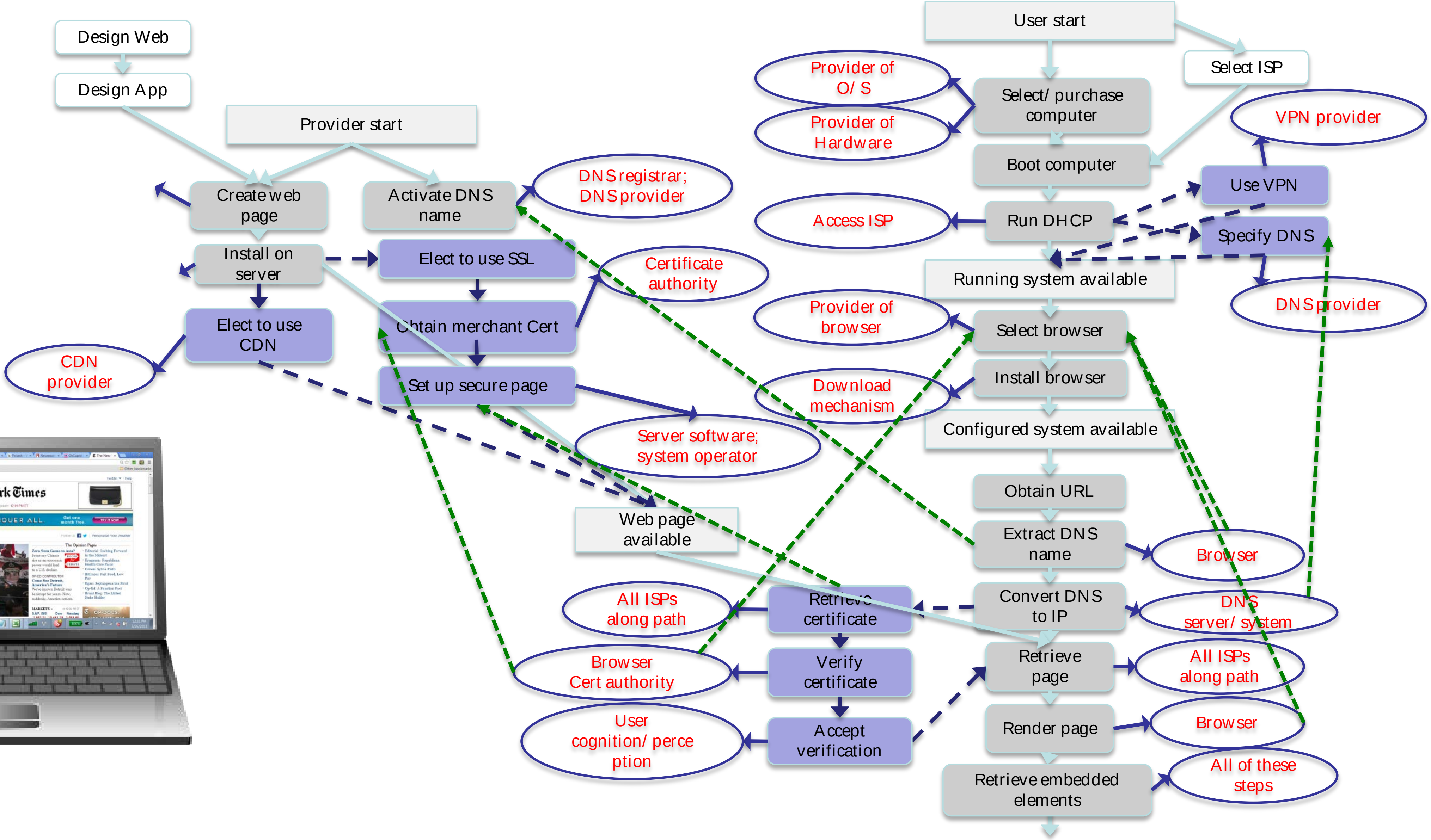
Understanding the threats, vulnerabilities, and risks

What are the major types of cyber threats?

What types of vulnerabilities exist?

Who is an adversary in cyberspace?

Viewing a Webpage – what has to happen

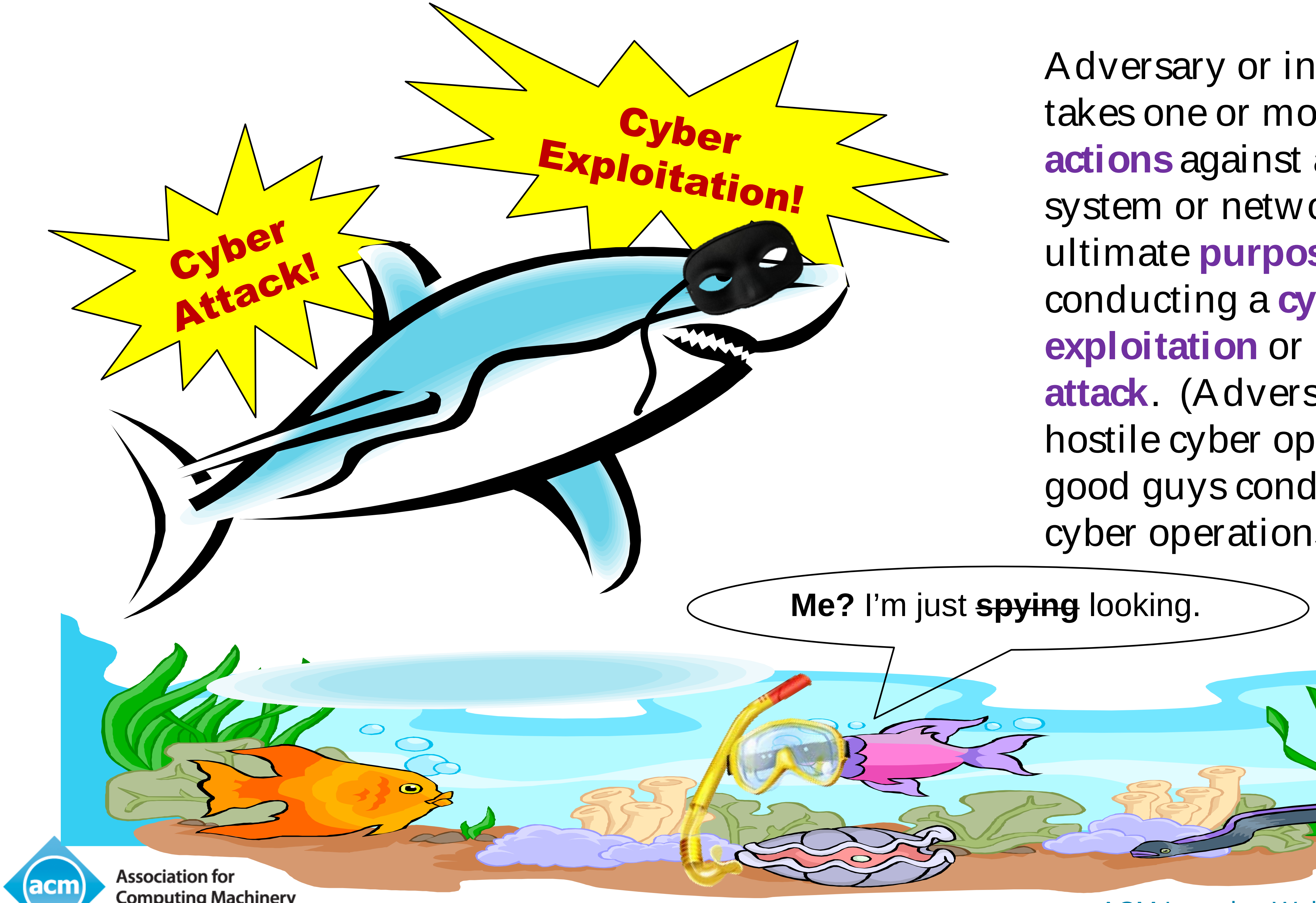


Understanding the threats, vulnerabilities, and risks

What are the major types of cyber threats?

What types of vulnerabilities exist?

Who is an adversary in cyberspace?



Adversary or intruder who takes one or more **unfriendly actions** against a computer system or network for the ultimate **purpose** of conducting a **cyber exploitation** or a **cyber attack**. (Adversaries conduct hostile cyber operations; good guys conduct offensive cyber operations.)

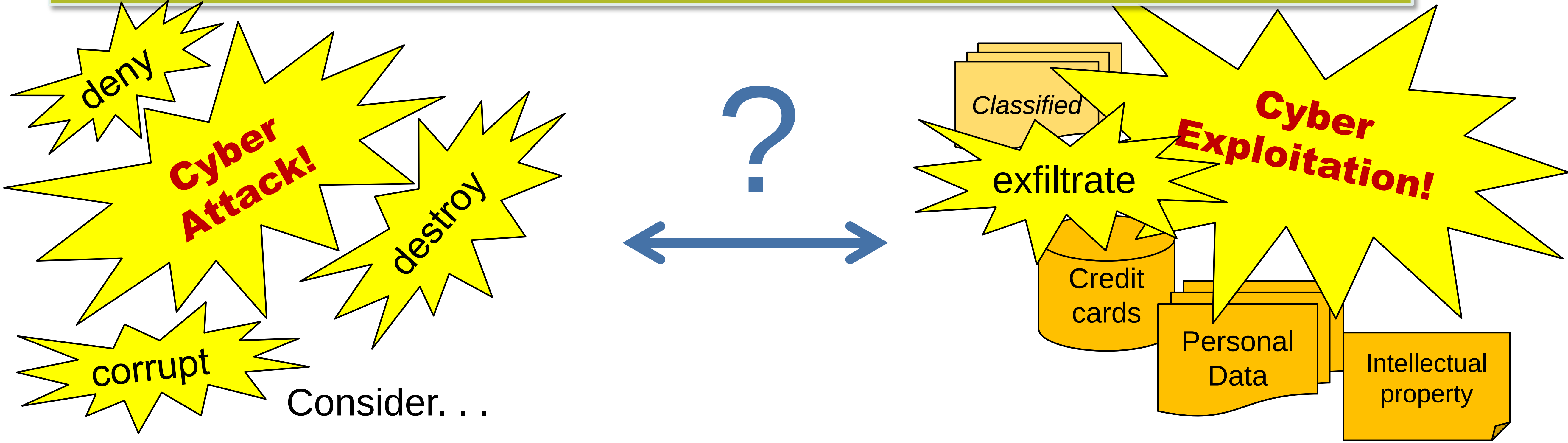
Understanding the threats, vulnerabilities, and risks

What are the major types of cyber threats?

What types of vulnerabilities exist?

Who is an adversary in cyberspace?

Do we know what the adversary's objective is?



Consider. . .

- Attack and exploitation may be **indistinguishable**.
- Most cyber threats have involved cyber exploitation.
- No known cyber attack has resulted in death.
  - However, computer malfunctions have caused death.
- A few cyberattacks have resulted in loss of or damage to property.
  - e.g. Stuxnet

Understanding the threats, vulnerabilities, and risks

What are the major types of cyber threats?

What types of vulnerabilities exist?

Who is an adversary in cyberspace?

Do we know who the adversary is?

Could the adversary or intruder be. . .

- **Lone hackers** seeking fame and glory
- **Criminals** acting on their own for profit
- **Organized crime** (e.g., drug cartels)
- **Terrorists** (perhaps state-sponsored)
- **Nation-states**

Note well:

- **For-hire** hacking services
- **High-end attackers** ($, talent, time, support)
- **Insider threats**

Understanding the threats, vulnerabilities, and risks

What are the major types of cyber threats? | What types of vulnerabilities exist? | Who is an adversary in cyberspace?

How can we improve cybersecurity?

Approaches to **weaken** the adversary's **ability and willingness** to be a cyber threat:

1. Reduce reliance on IT
2. Detection
3. Defense
4. Recovery and Resilience
5. Offensive operations for defensive purposes (retaliate, disrupt, pre-empt)
6. Offensive operations to weaken adversaries (gather intelligence, sabotage, build military capacity)

Understanding the threats, vulnerabilities, and risks

What are the major types of cyber threats? | What types of vulnerabilities exist? | Who is an adversary in cyberspace?

Cybersecurity is more than technology.

- **Economics**

  Conflicting interests and incentives among cybersecurity actors and stakeholders; market failure in cybersecurity
- **Psychology**

  Social engineering and deception; usable security; decision-making under uncertainty
- **Organization**

  Responsibility and authority; red teams and penetration testing; expertise throughout organization
- **Personnel security**
- **Security policies**

What policy approaches will help improve security?

Is policy needed to address market failure?

What are the policy tensions?

What are the international policy issues?

What policy approaches will help improve security?

Is policy needed to address market failure? | What are the policy tensions? | What are the international policy issues?

Marketplace does not provide adequate cybersecurity for the country.

- **Decision makers** discount future possibilities so much that they see **no need for present-day action**.
- **Costs of action** beyond immediate business needs are **high** and **not obviously necessary**.
- **Costs of inaction** are **not borne by relevant** decision makers.

Market Failure?

How to measure economic losses due to inadequate cybersecurity?

How to address market failure?

How to assign responsibility for cybersecurity?

Association for Computing Machinery

Advancing Computing as a Science & Profession

What policy approaches will help improve security?

Is policy needed to address market failure?

What are the policy tensions?

What are the international policy issues?

Which approach to deal with market failure is best?

Public-sector mechanisms

- Procurement regulations
- Tax and other financial incentives
- Public recognition
- Voluntary standards setting by government
- Liability protections
- Liability enforcement
- Direct regulation
- Legislation
- International agreements
- Mutual cooperation
- And more. . .

Marketplace mechanisms

- Voluntary industry mechanisms
- Standards setting and certification
- "Trusted" suppliers and tested components
- Insurance

What policy approaches will help improve security?

Is policy needed to address market failure?	What are the policy tensions?	What are the international policy issues?
Anti-trust	Privacy, Civil Liberties	Innovation

- **Information sharing** for coordinated responses to large-scale cyber assault raises **anti-trust** and **privacy** issues.
- **Blocking malware** traffic may violate **privacy**.
- **Strong authentication** may limit **free expression** and **anonymity**.
- **Rapid cyber response** may impact **due process**.

Which public policy is best?
All possible mechanisms are controversial.

What policy approaches will help improve security?

Is policy needed to address market failure?	What are the policy tensions?	What are the international policy issues?
Anti-trust	Privacy, Civil Liberties	Innovation

Innovation and first-to-market advantages work to **inhibit** design and implementation for **cybersecurity.**

Security can:

- add complexity, time, and cost.
- conflict with performance and functionality.
- be hard to value by customers.
- be in tension with other attributes.
  - e.g. ease of use, interoperability, backwards compatibility

Which public policy is best?
All possible mechanisms are controversial.

Integrating security from the start can:

- imply good understanding of system specifications for functionality.
- be hindered by false starts that multiply costs.

What policy approaches will help improve security?

Is policy needed to address market failure?

What are the policy tensions?

What are the international policy issues?

Internet Governance

Surveillance

Norms of Behavior

Global IT Supply Chain

Offensive Operations in Cyberspace

Internet Governance

- Scope is controversial.
- Disputes are often over content regulation in the name of Internet security.
  - e.g. Should packet-level authentication in the basic Internet protocols be required?

Surveillance

- Weaken cybersecurity to facilitate surveillance?
- Limit access to weaknesses?

Norms of Behavior in Cyberspace

- Espionage
- Arms control

Global Supply Chain for Information Technology

Role of Offensive Operations in Cyberspace

What you should know about the 6 KEY FINDINGS from the report!

#1 Is there a fix in our future?

#2 What will bring results?

#3 Which activities are best?

#4 What will promote accountability?

#5 What will be the tradeoffs?

#6 What's next for policy discussions?

What you should know about the 6 KEY FINDINGS from the report!

#1 Is there a fix in our future? | **#2 What will bring results?** | **#3 Which activities are best?**

#1 Cybersecurity is a **never-ending battle**.

A permanently decisive solution to the problem will **not** be found in the foreseeable future.

What you should know about the 6 KEY FINDINGS from the report!

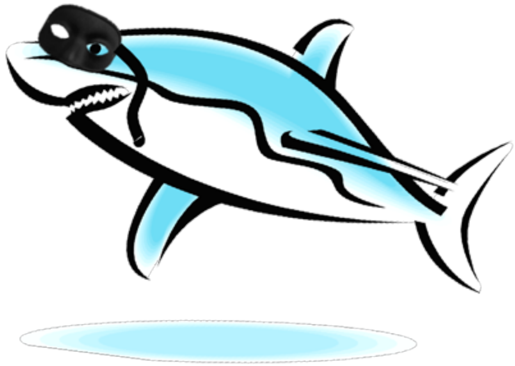
#1 Is there a fix in our future?

#2 What will bring results?

#3 Which activities are best?

#2

Improvements to the cybersecurity posture of individuals, firms, government agencies, and the nation will have **considerable value** in **reducing the loss** and **damage** that may be associated with cybersecurity breaches.



What you should know about the 6 KEY FINDINGS from the report!

#1 Is there a fix in our future?

#2 What will bring results?

#3 Which activities are best?

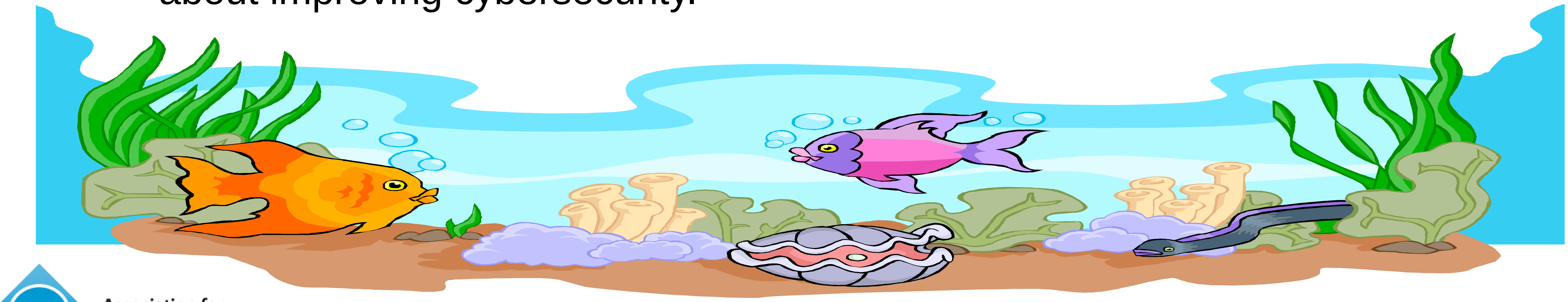
#3 Improvements to cybersecurity call for **two distinct** kinds of activity.

EXISTING
Knowledge

Efforts to more effectively and more widely use what is known about improving cybersecurity.

NEW
Knowledge and Research

Efforts to develop new knowledge about cybersecurity.



Association for Computing Machinery

Advancing Computing as a Science & Profession

What you should know about the 6 KEY FINDINGS from the report!

#4 What will promote accountability?

#5 What will be the tradeoffs?

#6 What's next for policy discussions?

#4 **Publicly available information** and **policy actions** have been **insufficient** to motivate an adequate sense of **urgency** and **ownership** of cybersecurity problems afflicting the United States as a country.

What you should know about the 6 KEY FINDINGS from the report!

#4 What will promote accountability?

#5 What will be the tradeoffs?

#6 What's next for policy discussions?

#5 **Cybersecurity is important** to the country, but the United States has other interests as well, some of which conflict with the imperatives of cybersecurity.

Trade-offs are inevitable and will have to be accepted through the country's **political and policy-making processes**.

What you should know about the 6 KEY FINDINGS from the report!

#4 What will promote accountability?

#5 What will be the tradeoffs?

#6 What's next for policy discussions?

#6 The use of **offensive operations in cyberspace** as an instrument to advance U.S. interests raises many important **technical**, **legal**, and **policy** questions that have **yet to be aired publicly** by the U.S. government.

For more information…

Herb Lin

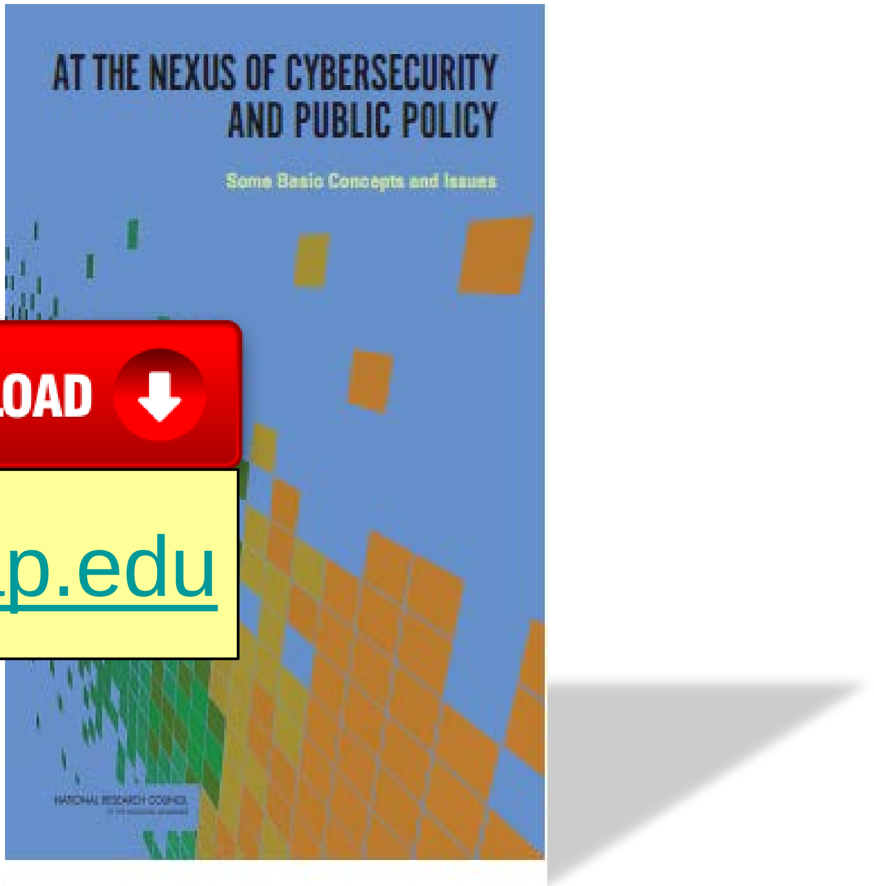
Chief Scientist
Computer Science and Telecommunications Board
National Research Council

202-334-3191

hlin@nas.edu

www.cstb.org

www.nas.edu



AT THE NEXUS OF CYBERSECURITY AND PUBLIC POLICY

Some Basic Concepts and Issues

NATIONAL RESEARCH COUNCIL

FREE DOWNLOAD

www.nap.edu

Question and Answer

Herb Lin

Chief Scientist, Computer Science and Telecommunications Board, National Research Council

Jeremy Epstein

Moderator

Lead Program Officer, National Science Foundation Secure and Trustworthy Cyberspace program; ACM Senior Member