Latest & Greatest Security Solutions

Clueless users

1b. Defence Overview

Jin Hong

jin.hong@uwa.edu.au

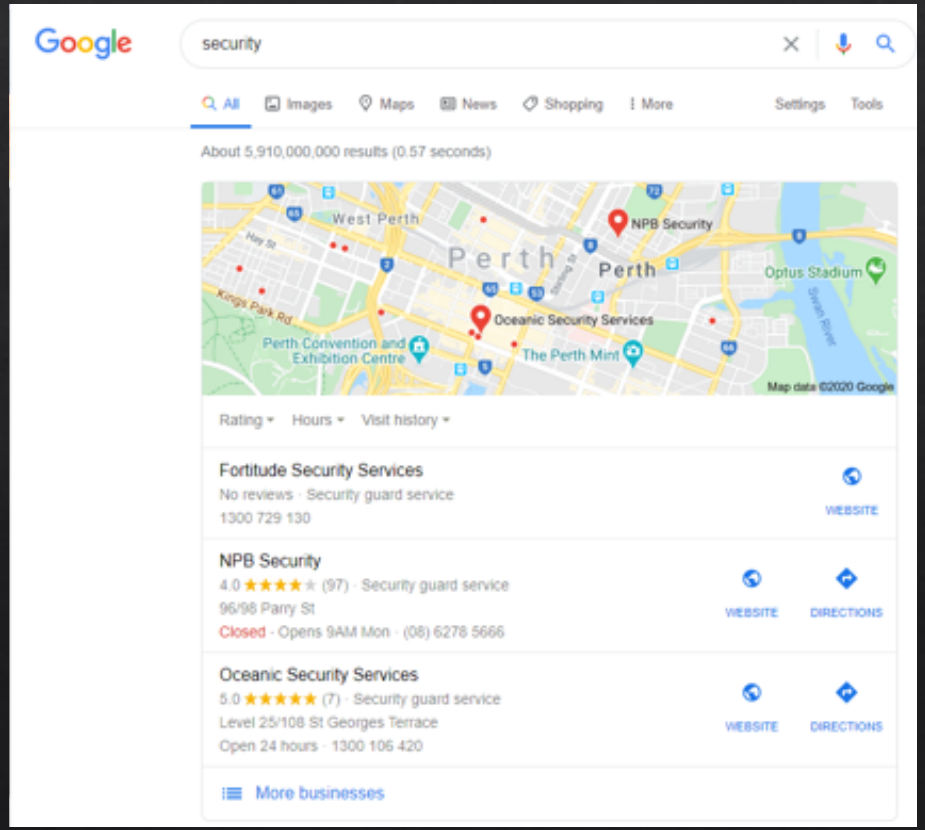
Introduction: outline

- What is security?
- Security objectives
- Defense overview
- Security management
- Cybersecurity

Quick stop: Terminology

Term	Meaning
Risk	The potential for an unwanted or adverse **outcome** resulting from an incident, event, or occurrence, as determined by the **likelihood (or the potential)** that a particular threat will exploit a particular vulnerability, with the associated consequences.
Vulnerability	A characteristic or specific **weakness** that renders an organization or asset (such as information or information system) open to exploitation by a given threat or susceptible to a given hazard.
Exploitation	A technique to breach the security of a network or information system in **violation** of security policy.
Threat	A circumstance or event (including accidental and non-human related) that has or indicates the **potential** to exploit vulnerabilities and to adversely impact (create adverse consequences for) organizational operations, organizational assets (including information and information systems), individuals, other organizations, or society.
Asset	A person, structure, facility, information, and records, information technology systems and resources, materials, process, relationships, or reputation allowing entities (e.g., individuals, businesses and governments) to achieve social, economic, and other objectives of **value**.

Security – what is it?



"**Security** is the degree of resistance to, or protection from, harm. It applies to any vulnerable and/or valuable asset, such as a person, dwelling, community, item, nation, or organization." - Wikipedia

Security – what is it?

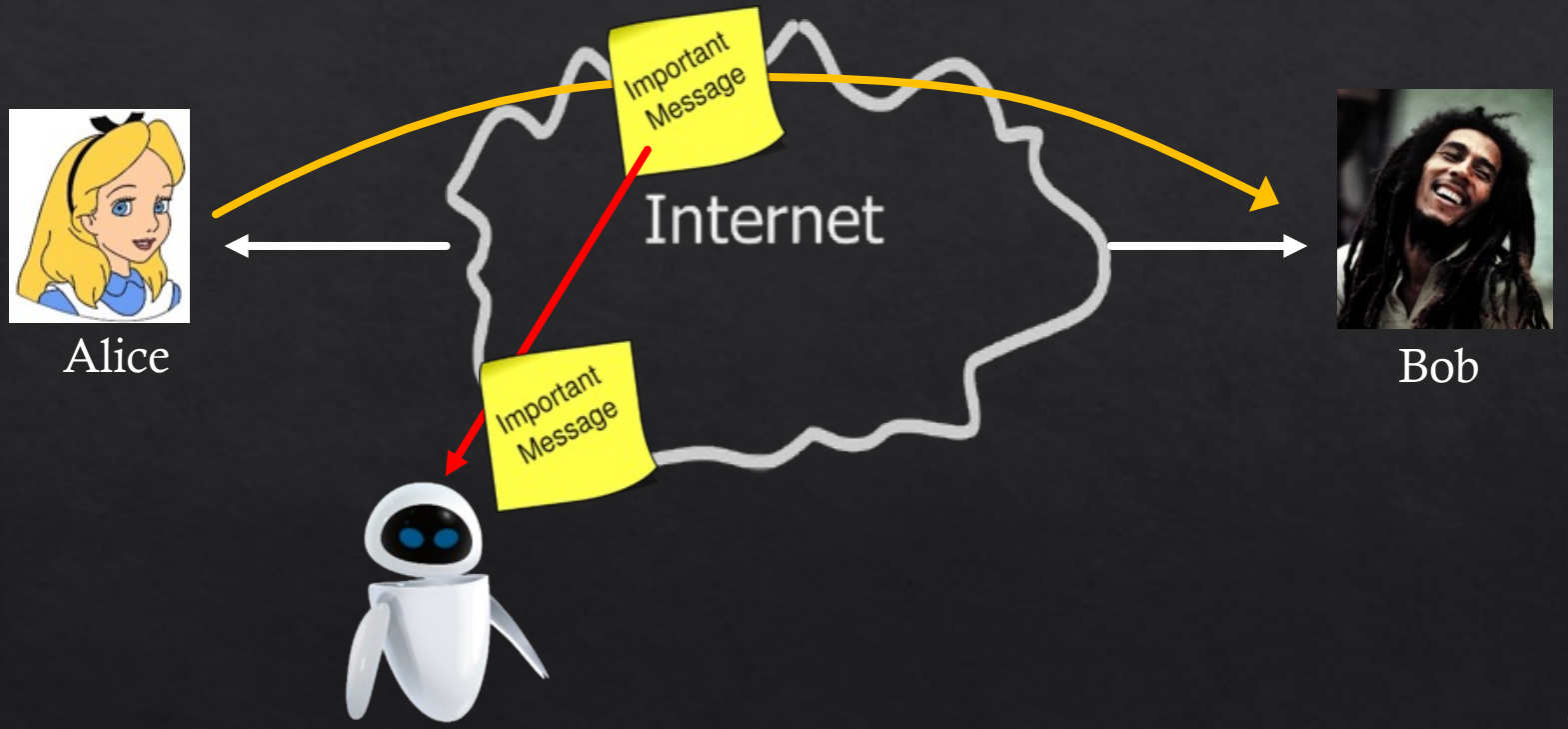
- The three foundational components in information security
  - Confidentiality – information is only available to those authorized; e.g., privacy
  - Integrity – information cannot be modified or damaged by others
  - Availability – information is always (or to some degree of always) accessible

The CIA Triad

Not this one!

The standard is ISO/IEC 27000:2018

Confidentiality

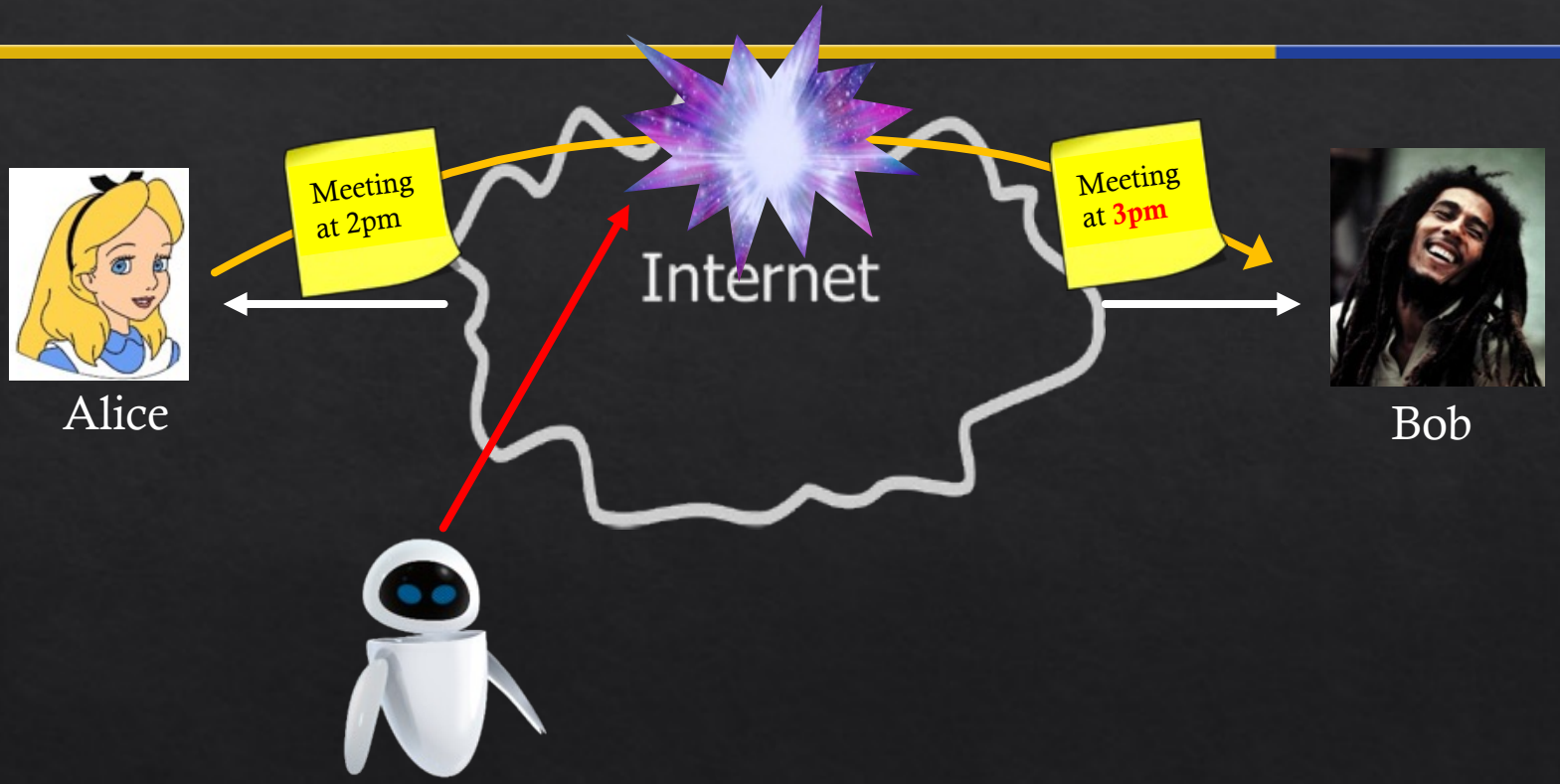


Confidentiality: the information is only accessible by authorised entities.

How to achieve…

- Confidentiality?

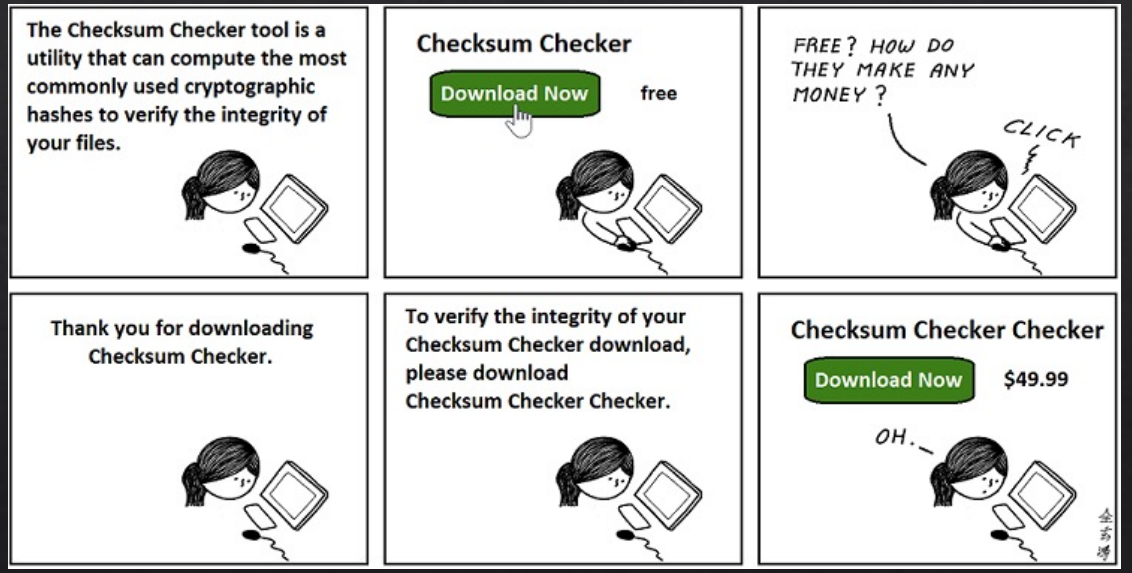
Integrity



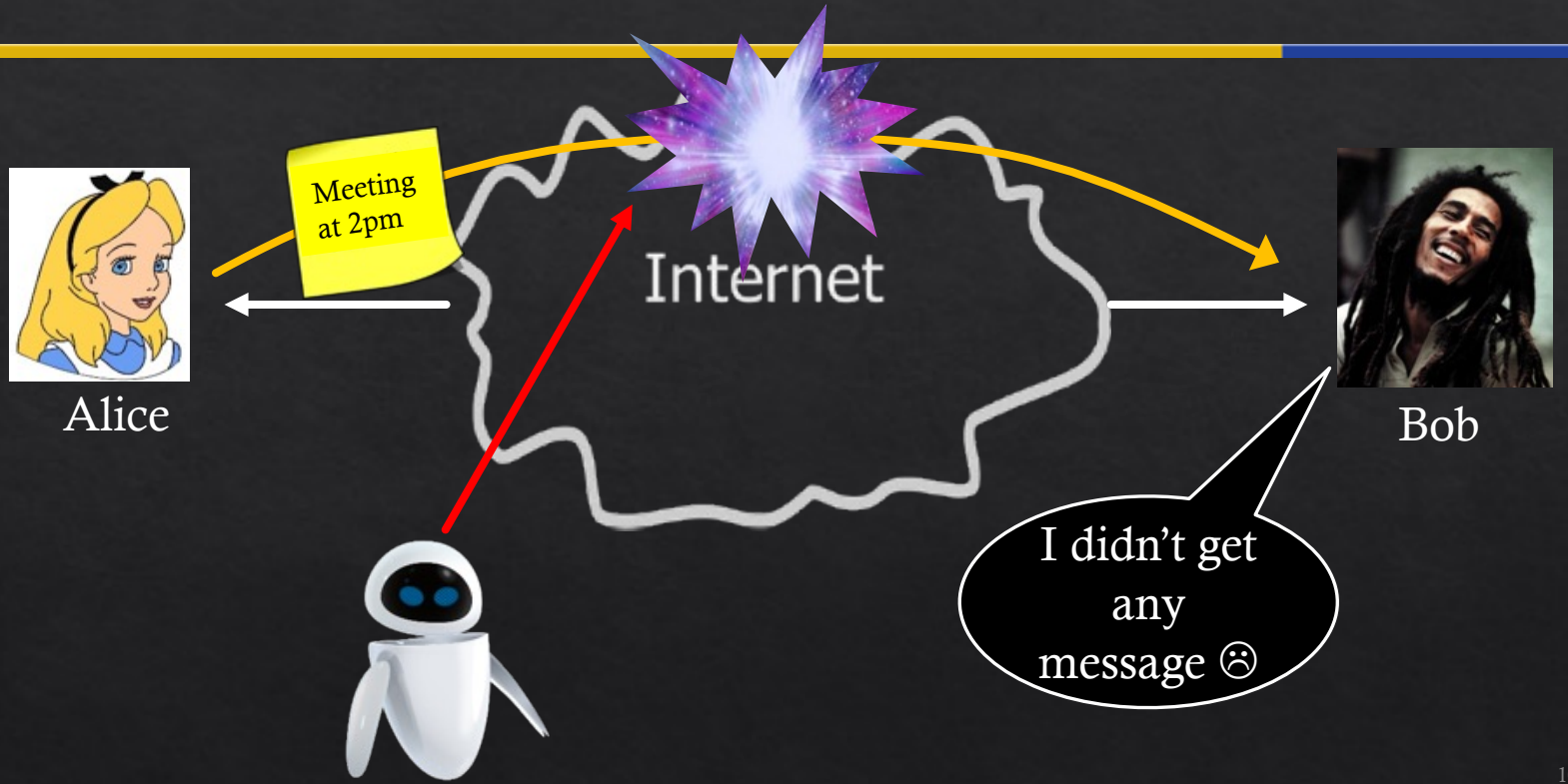
Integrity: the information can only be changed by authorised entities.

How to achieve…

- Integrity?



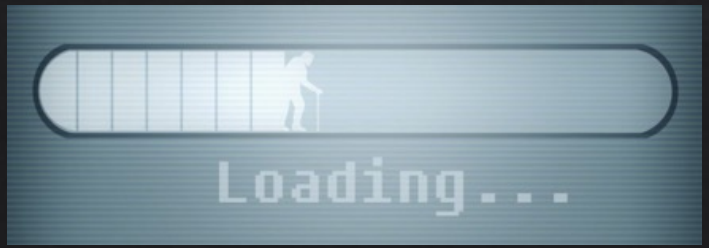
Availability



Availability: the information must be accessible when needed.

How to achieve…

- Availability?



Examples

- In University (in class exercise)
- In Business
- In Government

In University

- Confidentiality
- Integrity
- Availability

In Business

Confidentiality	• Project data is undisclosed to the public • Customer details are encrypted and stored securely
Integrity	• An employee cannot modify his/her own salary • Annual summary data is not improperly modified
Availability	• Paychecks are received on time as stipulated by law • Internal network is accessible from the Internet

In Government

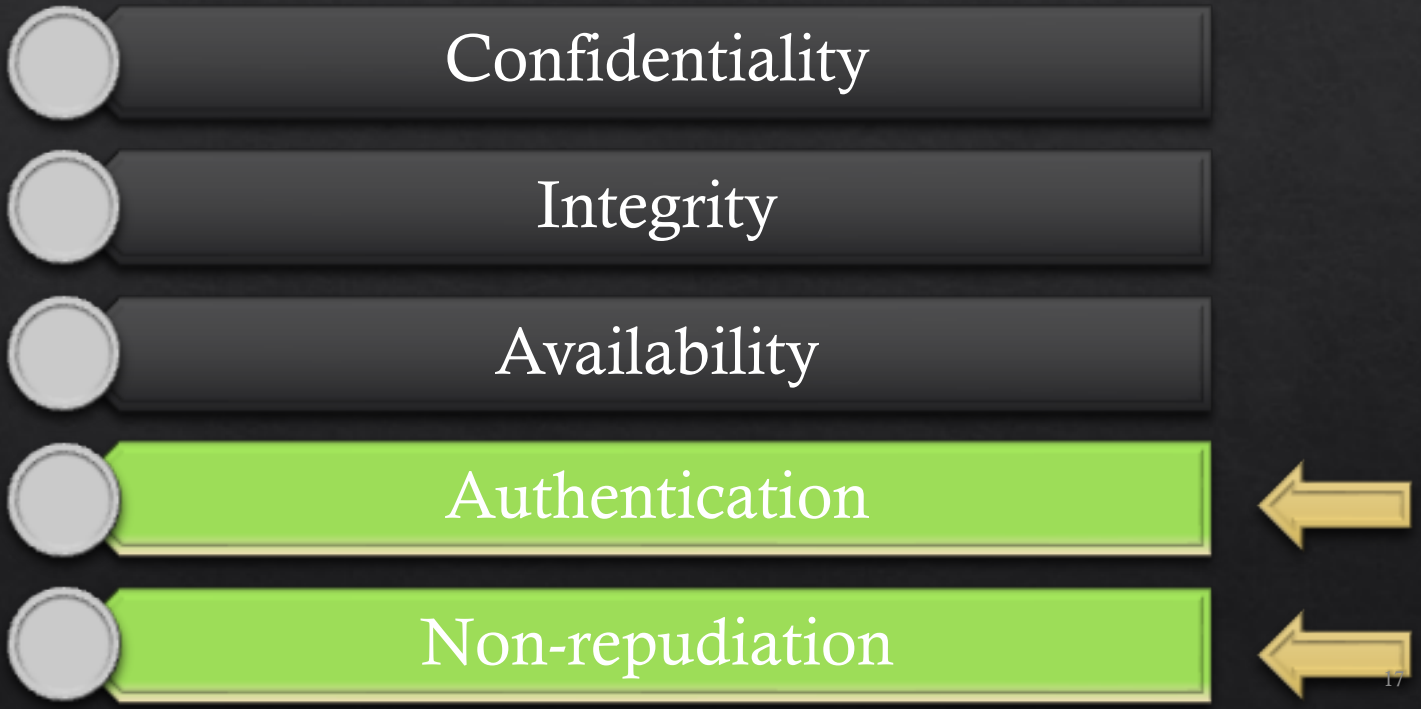
Confidentiality	• Passport details are kept safe from public access • Tax return details are not improperly disclosed to others
Integrity	• Passport details should not be modified by unauthorised persons • Tax return should be made to the correct bank account
Availability	• Passport details are checked in real time when travelling • Tax return should be made within 20 working days

Security Objectives summary

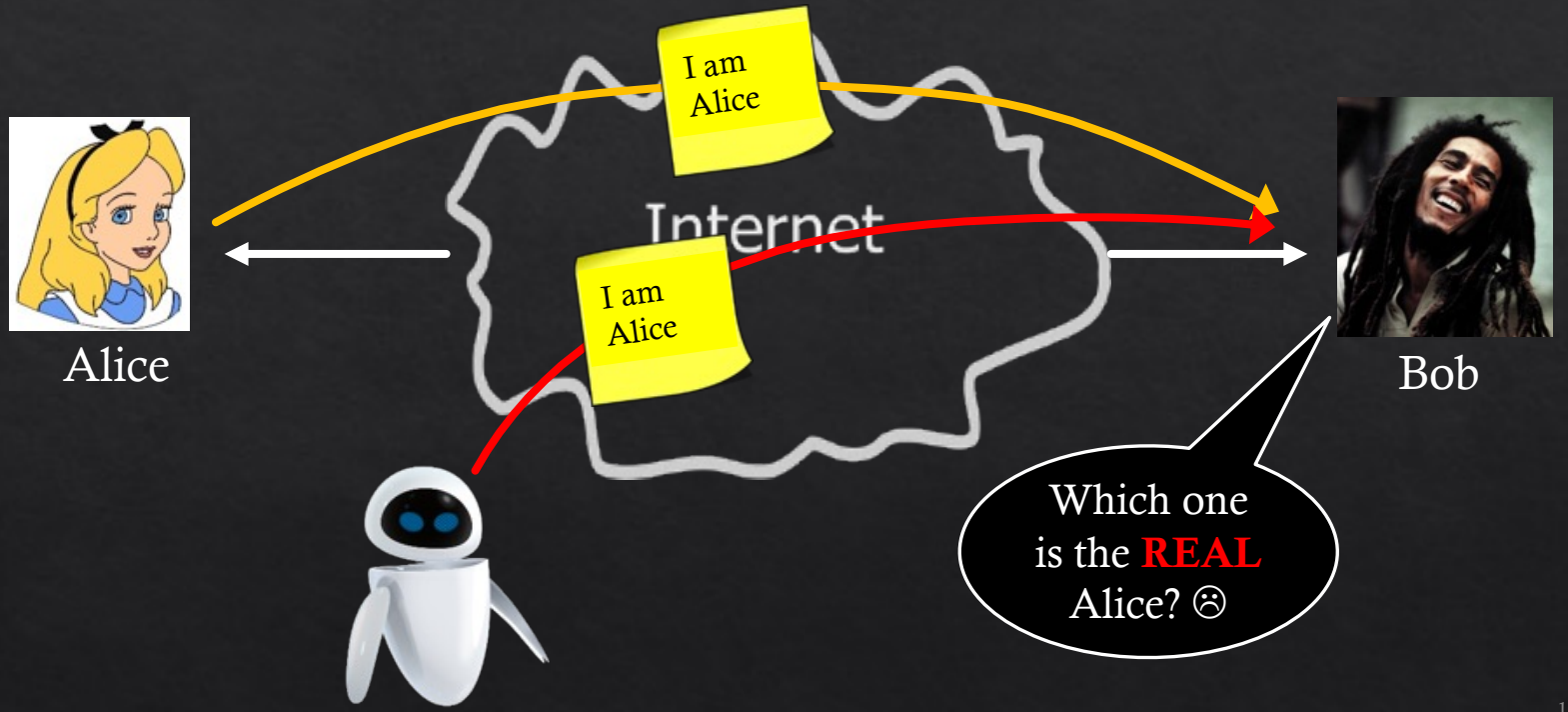
- **C**onfidentiality
  - To prevent, detect and deter improper disclosure of information
- **I**ntegrity
  - To prevent, detect and deter improper modification of information
- **A**vailability
  - To prevent, detect and deter improper denial of access to services

- These objectives may have different interpretations in different contexts.

But wait, there's more!



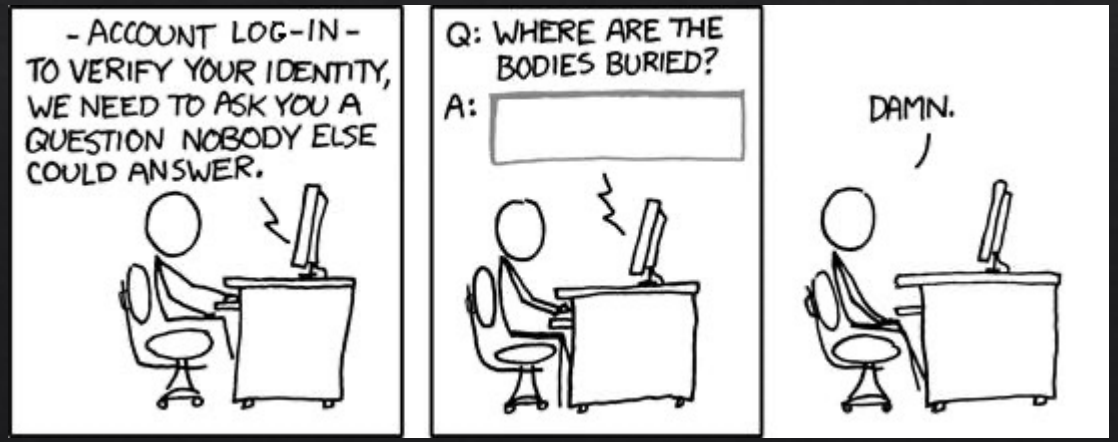
Authentication



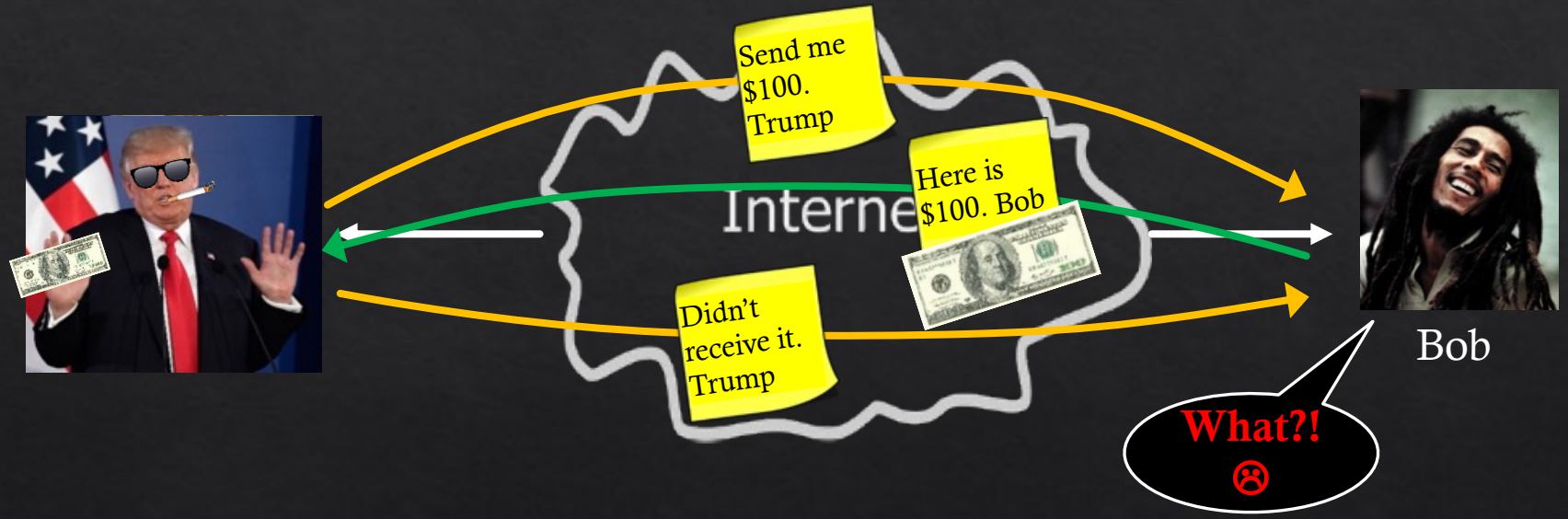
Authentication: the entity you are communicating with is who he/she claims.

How to achieve…

- Authentication?



Non-repudiation



Non-repudiation: entities cannot disclaim their actions.

How to achieve…

- Non-repudiation?

"Now we will follow this audit trail and catch him"

Defense overview

- There are many actions against cyberattacks.

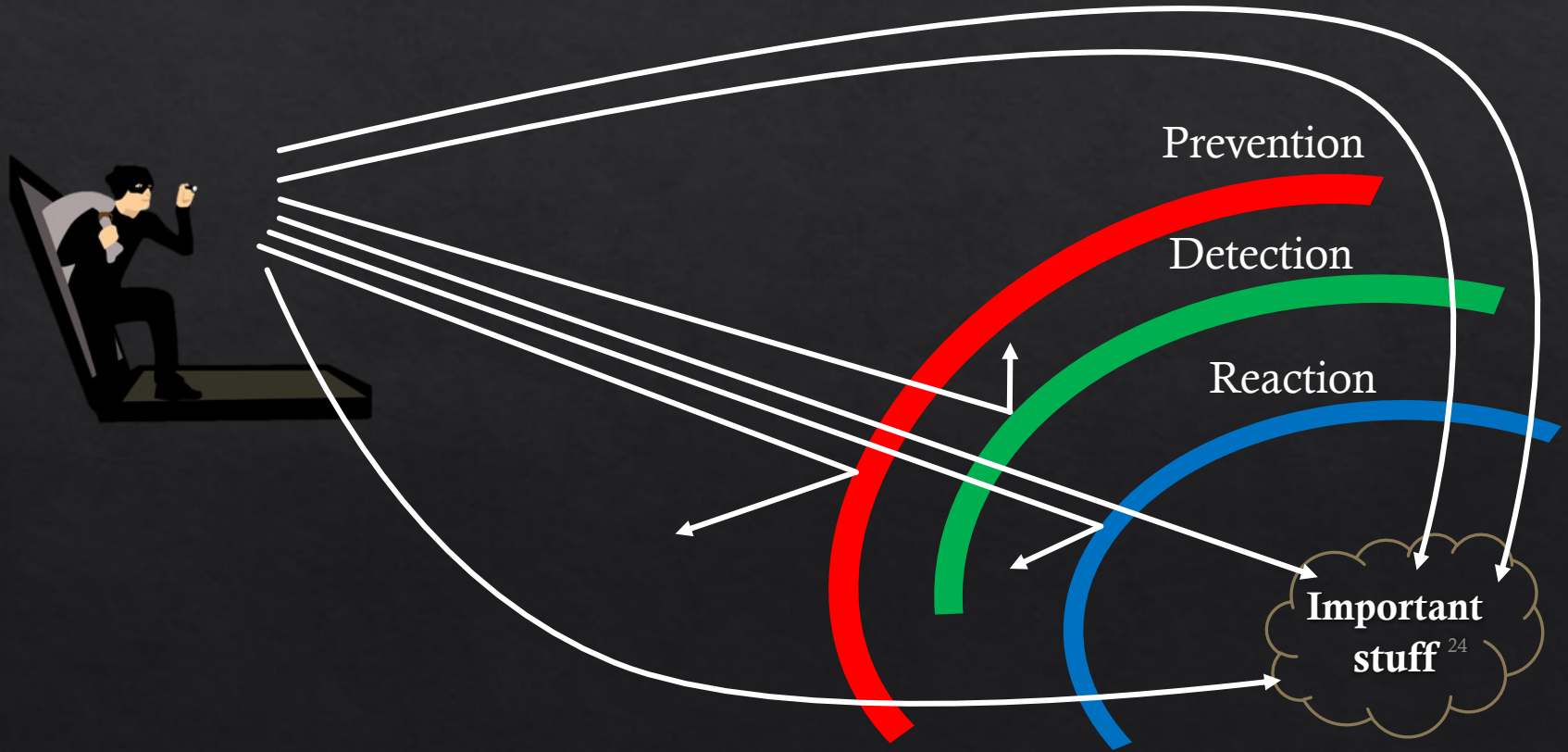
Defense overview

- Three types in general.

Prevention	Such as:
Detection	Such as:
Reaction	Such as:

Security Evaluation Standard: ISO/IEC 18045:2008

Defense overview

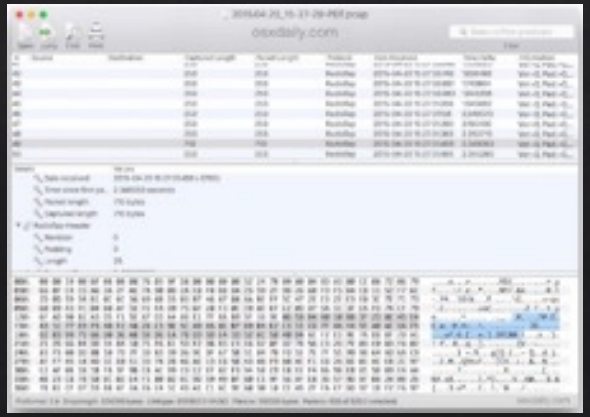


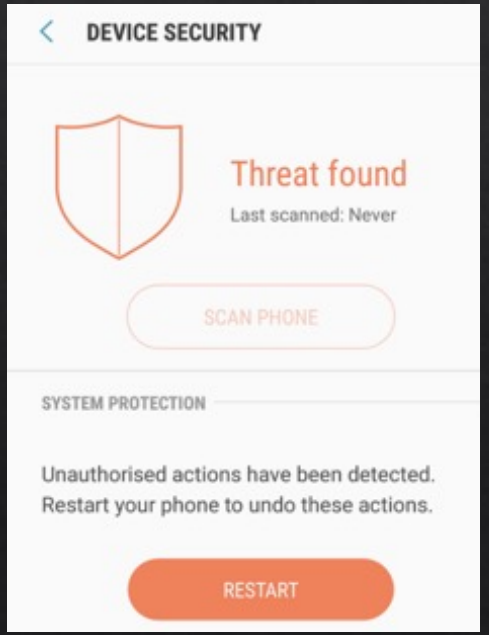
Prevention examples

- Prevention aims to protect your assets from attacks
  - Using encryptions for secure communication
  - Authentication of legitimate users in the system
  - User information is kept confidential

Detection examples

- To discover the damage to you asset (what, how, when, who, where).
  - Unauthorised access attempts in the log
  - Packet tracing
  - Intrusion detection systems





Reaction examples

- To enhance security and mitigate attacks.
  - Deploy two-factor authentication
  - Revoke malicious membership/access
  - Enforce deterrence

Defense Mechanisms

- Defense mechanisms includes
  - Firewall
  - Vulnerability scanning and patching
  - IDS and IPS
  - Security Protocols
  - IPSec and VPN
  - Sandboxing
  - Moving Target Defense
  - *etc…*

Risk control/management

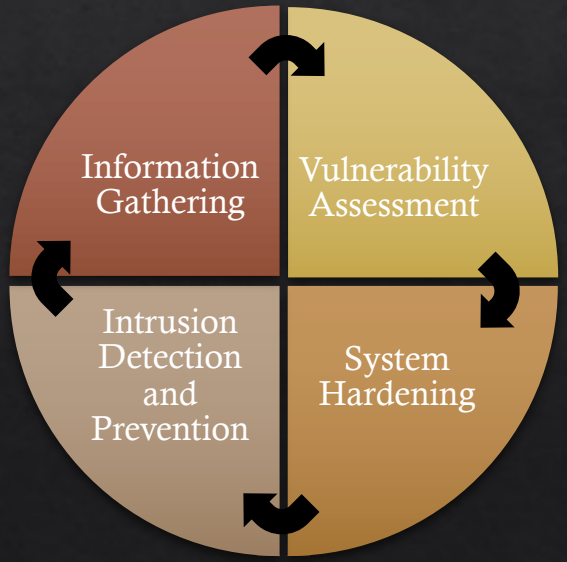
- Risk: **unwanted** outcome by a potential **threat**.
- Falls under ISO/IEC 27005:2011

ISMS: Information Security Management System

Source: International Organization for Standardization - https://www.iso.org/news/2011/02/Ref1595.html

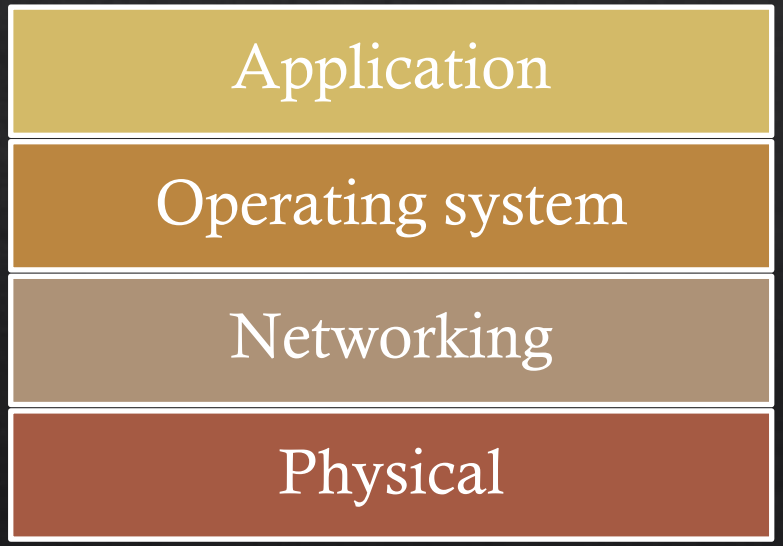
Risk control/management

- How to carry out ?



Risk control/management

- Also think about the layers



Security Policy

- A set of procedures and tasks to ensure the security objectives of an organisation
  - Specifies **what** are the assets, and may specify **how** it is done
- To produce the policy, you need to know
  - Assets to be protected
    - E.g., hardware, software, data and information, *anything else*?
  - Vulnerabilities
  - Threats
  - Mitigations

Security Policy

- Understanding security requirements are critical step towards formulating the security policy
- Example, passwords
  - Length
  - Specification of conditions (e.g., uppercase, special chars)
  - Frequency of change
  - Location of the user
  - Client software specification (e.g., not on mobile)

Security Management

- Risk control and security policy development is a part of security management.
- Security management requires security measurements
  - Quantitative and qualitative
  - Risk, impact, probability, return on security investment etc.
- But measurement is a difficult task. Why?

Security Management

- Security management has a defined standard
  - ISO/IEC 27001:2013
- It specifies tasks associated with establishing, implementing, maintaining and continually improving an information security management system.
- 14 clauses of security controls are defined in this ISO.

Security Management

- A.5: Information security policies
- A.6: How information security is organised
- A.7: Human resources security - controls that are applied before, during, or after employment.
- A.8: Asset management
- A.9: Access controls and managing user access
- A.10: Cryptographic technology
- A.11: Physical security of the organisation's sites and equipment
- A.12: Operational security
- A.13: Secure communications and data transfer
- A.14: Secure acquisition, development, and support of information systems
- A.15: Security for suppliers and third parties
- A.16: Incident management
- A.17: Business continuity/disaster recovery (to the extent that it affects information security)
- A.18: Compliance - with internal requirements, such as policies, and with external requirements, such as laws.

Security Management

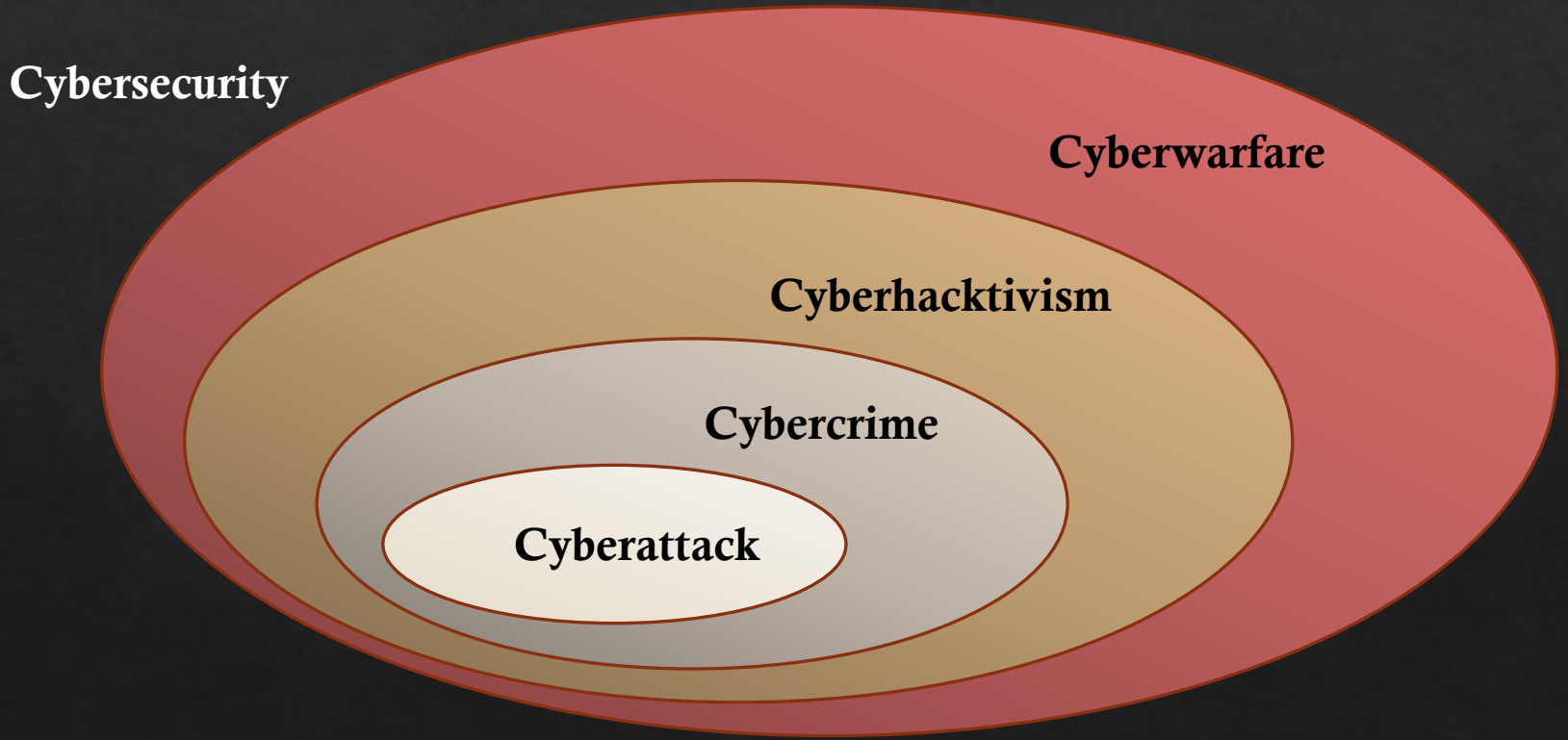
- There are other security standards too
  - U.S. Federal Government information security standards
    - E.g., NIST SP 800-53
  - U.S. Department of Defense information security standards
    - E.g., DoD Instruction 8500.2

- And other international standards.
  - Q: Which one should you follow?

Cyber-something

- Cybersecurity is not only about security mechanisms and methodologies.
- A broader aspect of the cyberspace safety must be considered.
- A lot of cyber-something nowadays, let's have a look at a few of interest.

Cyber-something



Cybersecurity

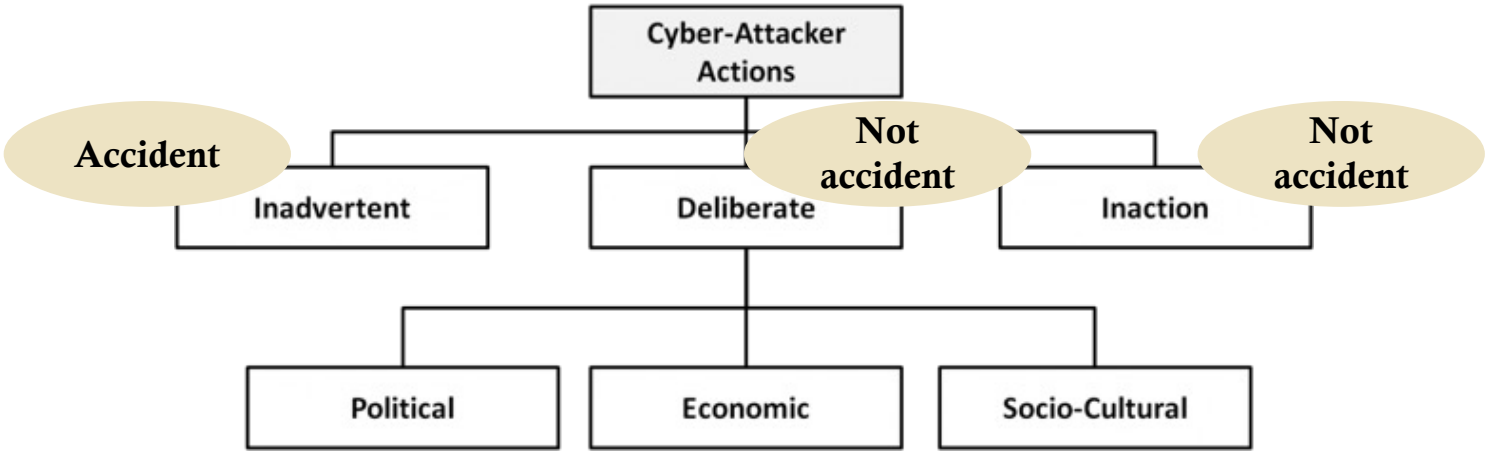
"The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are **protected** from and/or defended against **damage**, **unauthorized use** or **modification**, or **exploitation**." – CNSSI, NIST, DHS and White House

Cyberattack

- Cyberattack is an act of malicious activities in the cyberspace that causes harm to legitimate entities.
  - i.e., violating the CIA

- There are various entities that conduct cyberattacks.
  - Script kiddies
  - Black/White Hat Hackers
  - Hacktivists
  - Organised criminals
  - Nation States

Cyberattack



Source: Han, C. and Dongre, R. "Q&A: What Motivates cyber-attackers?", in Technology Innovation Management Review

Cybercrime

- Activities in the cyberspace that violates the laws and regulations.
- Cybercrimes not only affect financially, but also socially, psychologically and physically.
- There are laws and regulations to punish cybercrimes.
  - See the cybercrime details from the Australian Government Attorney-General's Department
  - https://www.ag.gov.au/CrimeAndCorruption/Cybercrime/Pages/default.aspx
- Still a global issue.

https://www.acorn.gov.au/learn-about-cybercrime

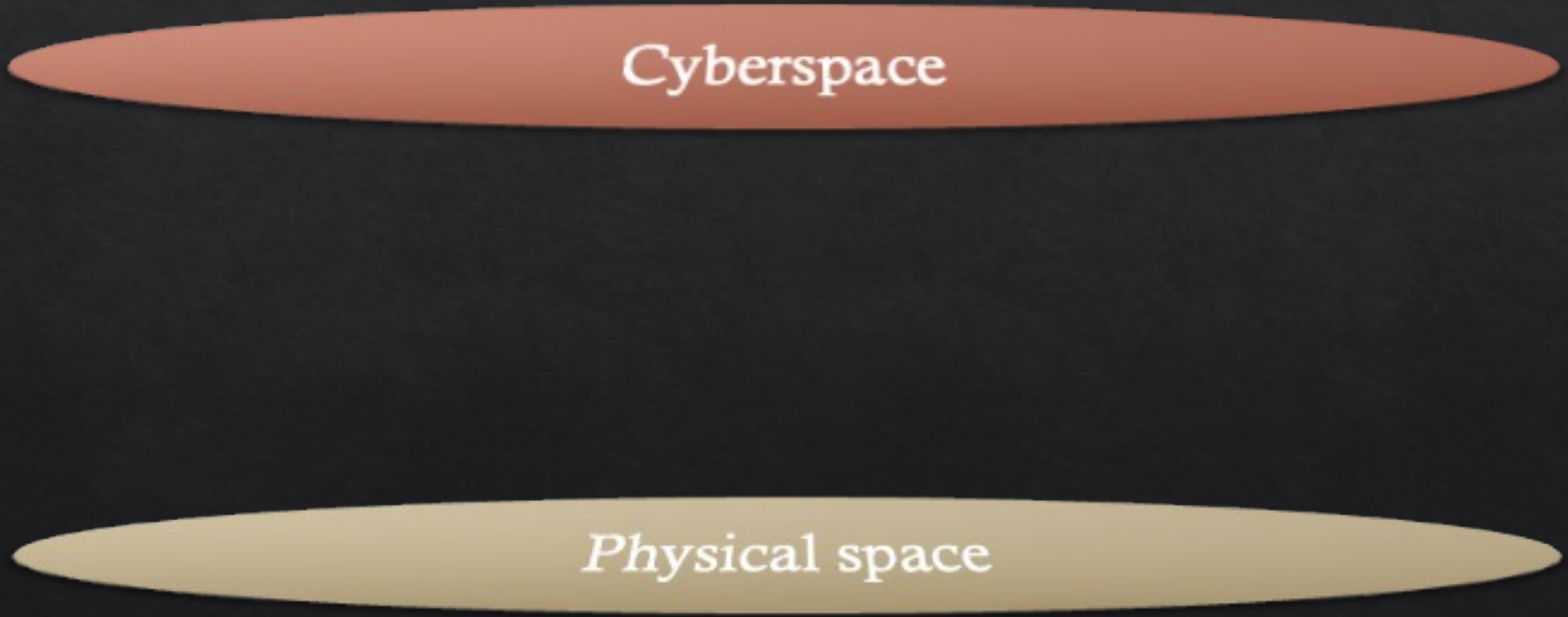
Cyberhacktivism

- May have other intentions than cybercriminals
  - i.e., not just personal gains
  - E.g., Panama papers in 2015
- Hacktivists pursue:
  - Political issues
  - Free speech
  - Prove a point

Cyberwarfare

- It's a war!
  - Involving both attack and defense, but in the cyberspace
- Involves orchestrated cyberattacks, hacktivism, as well as spies, espionage, sabotage, propaganda and deterrence.
- No widely accepted rules
  - Hence the arguments

Importance of cyber



Question

- Tik Tok collected your private data.
  - What type of cyberattack is this?
  - Is this a cybercrime? If yes, what type?
  - Could it be an unintentional Hacktivism?
  - Other thoughts?

Additional Items

- A glossary of cybersecurity terms
  - https://niccs.us-cert.gov/glossary
- List of ISO standards (like, all of them)
  - http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

Pre-reading materials

- Crypto stuff pre-reading/watching:
  - Youtube video (9 mins): https://youtu.be/fNC3jCCGJ0o
  - The Basics of Cryptography (6 mins): https://towardsdatascience.com/the-basics-of-cryptography-80c7906ba2f7
  - Basic Principles (4 mins): https://www.thegeekstuff.com/2012/07/cryptography-basics
  - Intro to public key cryptography (3 mins):
    - https://www.globalsign.com/en/ssl-information-center/what-is-public-key-cryptography/
  - Intro to RSA (15 mins):
    - http://www.dragonwins.com/domains/getteched/crypto/rsa.htm
    - Don't have to read thoroughly, just get the idea…