Hôpitaux Universitaires
SAINT-LOUIS
LARIBOISIÈRE
FERNAND-WIDAL

Technological Disasters: Why Do Cyber Attacks Cause Disasters?

Dr Jennifer Truchot

Emergency Department

Lariboisière Teaching Hospital

Antoine Feghali

PoTECH CONSULTING

tony@potech-consulting.com

ASSISTANCE PUBLIQUE HÔPITAUX DE PARIS

université PARIS DIDEROT PARIS 7

Introduction

- Cyber risk: growing global threat.
- Digitisation:
  - revolutionising business models
  - transforming daily lives
- Making the global economy more vulnerable to cyber-attacks.
- Cost estimated to 450 billion a year

Protection

- In 2016:
  - 2 billion personal records were stolen
  - 100 million Americans had their medical records stolen
- However, only:
  - 53 percent of the companies prepared to deal with an attack
  - 30 percent were rated "expert" in their overall cyber readiness.

Sources of vulnerability

- Within the software development community
  - Code is never released error free *(Chelf, 2009)*
  - Industry average number of bugs for every 1,000 lines of code range from 15 to 50 bugs, *(McConnell, 2004)*
- These bugs:
  - Lead to vulnerabilities through which malicious actors can obtain the ability to bypass safeguards
  - Misuse systems outside the intended purpose

Exemple 1:

- May of 2017:
  - a widespread ransomware (WannaCry) infested Windows operating system users worlwide
  - Exploiting a security flaw (known and addressed by many through Windows updates)
- Virus made its way into unprotected computers
- Ransom all the data (erase all data on an infected computer)
- This ransomware attack alone resulted in a total global loss of approximately USD4 billion.

Health care consequences

Over 2 dozens Hospitals and Medical Care Institutes in England were hit

Staff were forced to revert to pen and paper

Doctors were forced to turn away patients

People were advised to seek medical care only in emergencies

Exemple 2

- June 2017, Petya
- Infected networks in multiple countries—
  - The US pharmaceutical company Merck, Danish shipping company Maersk, and Russian oil giant Rosnoft
  - The ransomware hit Ukrainian infrastructure, disrupting utilities like power companies, airports, public transit, and the central bank

Exemple 3: Attack On Organs

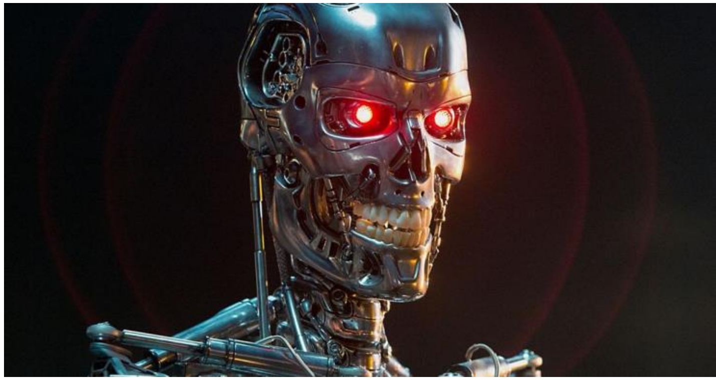
- **Pacemaker Hijacking:**

→ Barnaby Jack, the director of embedded device security for computer security firm IOActive, developed a software allowing him to send an electric shock to anyone wearing a pacemaker within a 50-foot radius

→ University of South Alabama researchers were able to speed up or slow down the heart rate

→ FDA: “the vulnerabilities found in pacemakers can be easily exploited and cause life-threatening injuries even death”

Exemple 4: Attack On Remote Surgeries



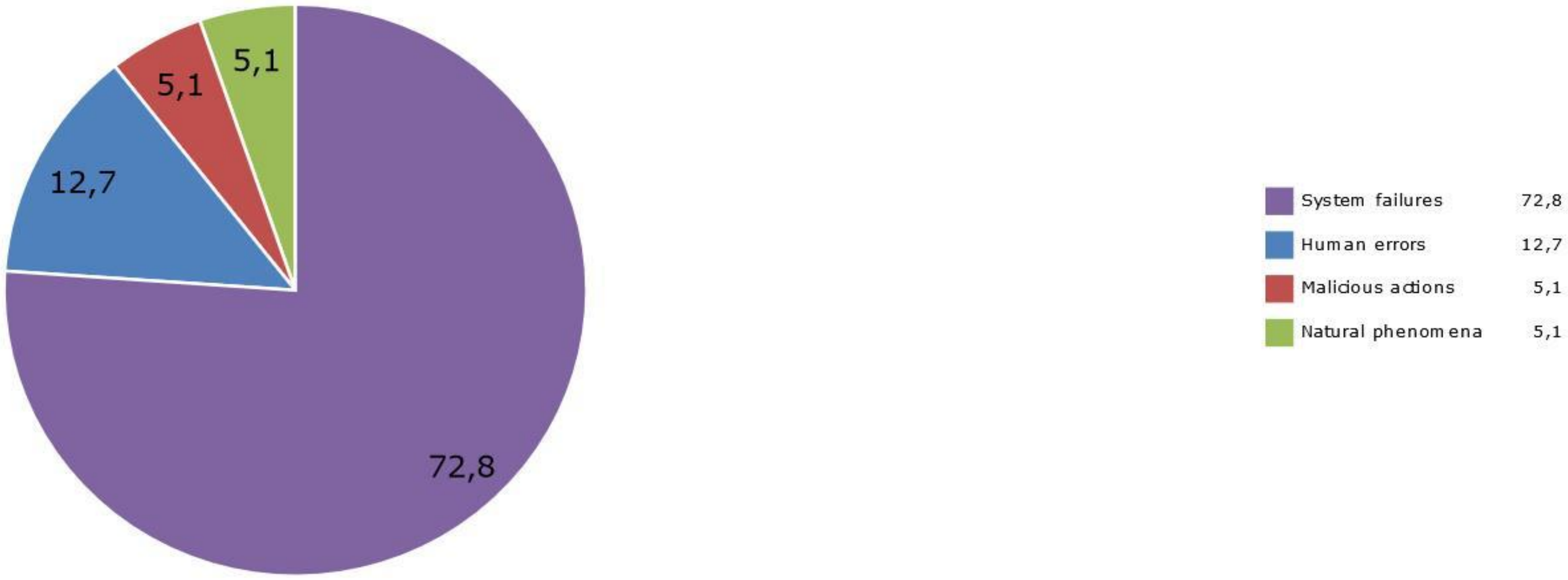
- **Robot Hijacking:**

→ Security Researchers hijacked a robot during surgery and launched a DoS attack

→ It became impossible for the surgeon to remotely operate

→ By sending maliciously crafted packets, the reset function was forbidden, thus making the robot impotent

Exemple 5: Communication incidents report



- **Only 2,5 % in 2015**
- **most impact in terms of average duration and user hours lost**

Impact on emergency medicine

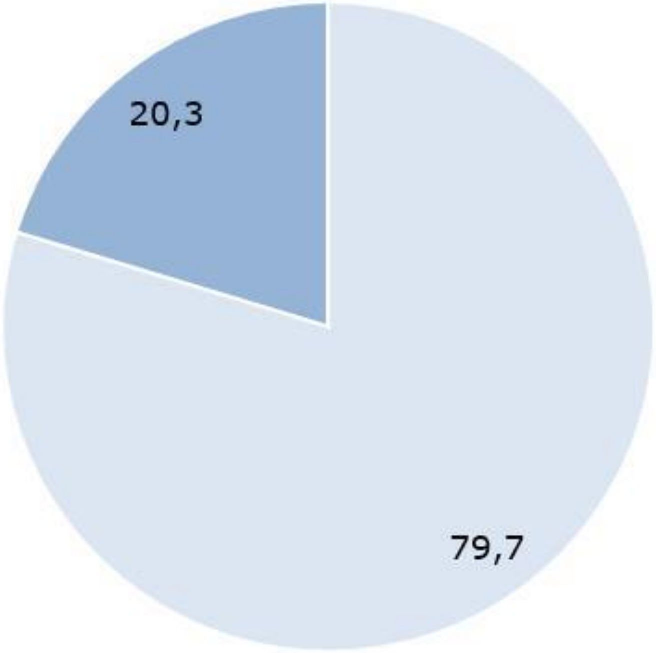
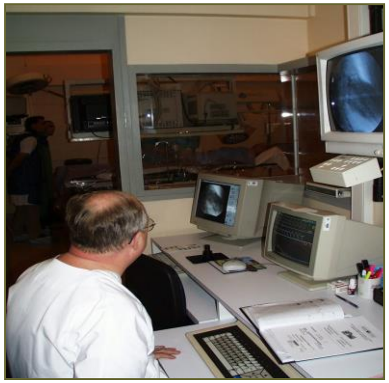


Figure 9: Impact on emergency calls.



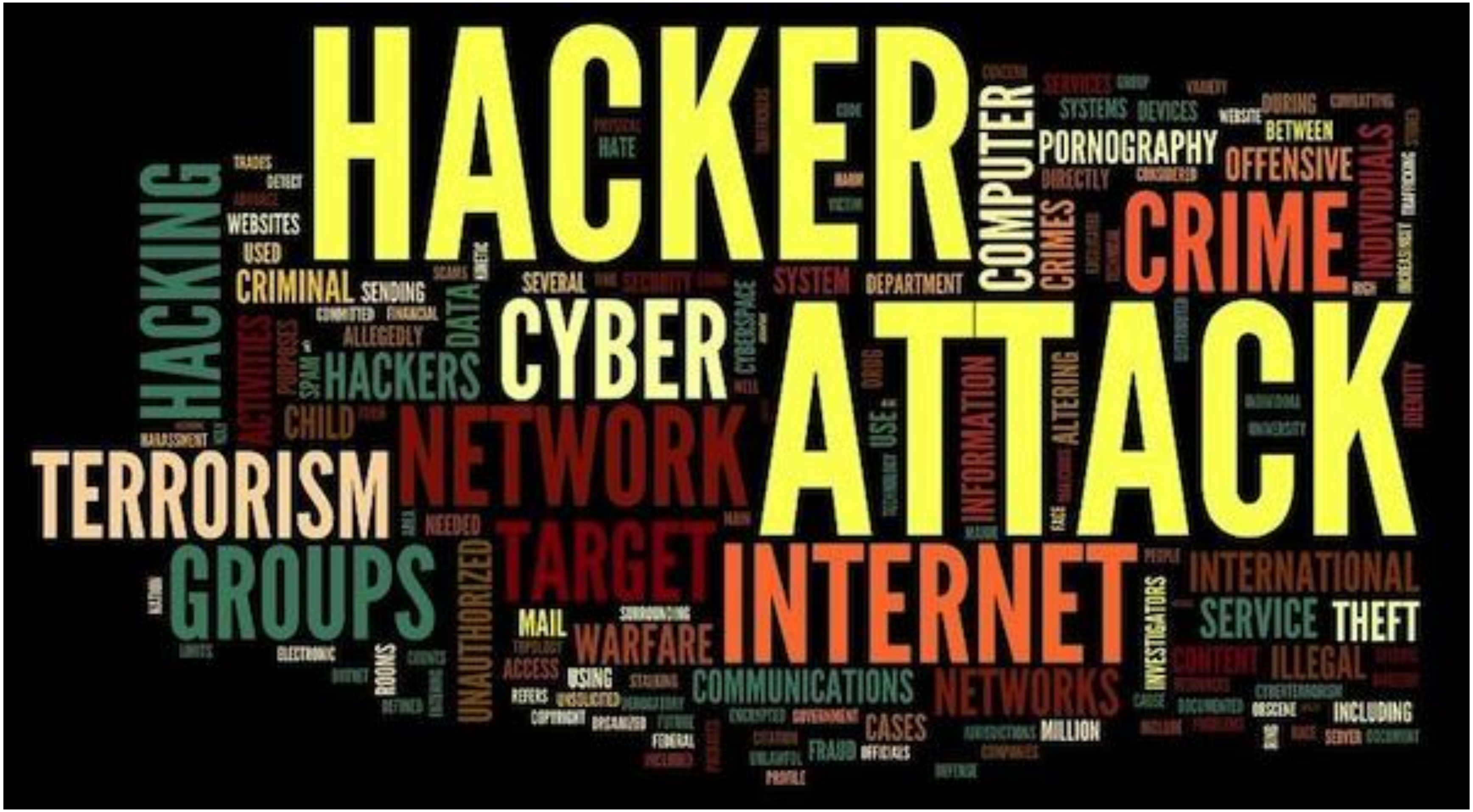
Possible threats

- 2017 Nuclear Threat Initiative (NTI) report:
- A cyber attack against a nuclear facility
  - theft of nuclear materials
  - an act of sabotage leading to a catastrophic radiation release.
- Most states are not effectively prepared to deal with this threat
- many countries, though they are looking at and developing nuclear technology, lack the capacity to make sure that it's safe.
- 20/ 47 countries: lack basic requirements to protect nuclear facilities from cyber attacks

Economic consequences

- Economic losses from cyber events:
- = those caused by major hurricanes.
- Major issue in the insurance business
- How well is your hospital covered ?

Cyber terrorism



Risks and Responsibilities

- We must understand, evaluate, mitigate and in some cases accept the risk
- How to define responsibilities in case of breach
  - Is it the responsibility of all stakeholders ?
- Today the impact of hacking is not only financial, but social and in some cases life threatening

Personal Responsibility (some tips)

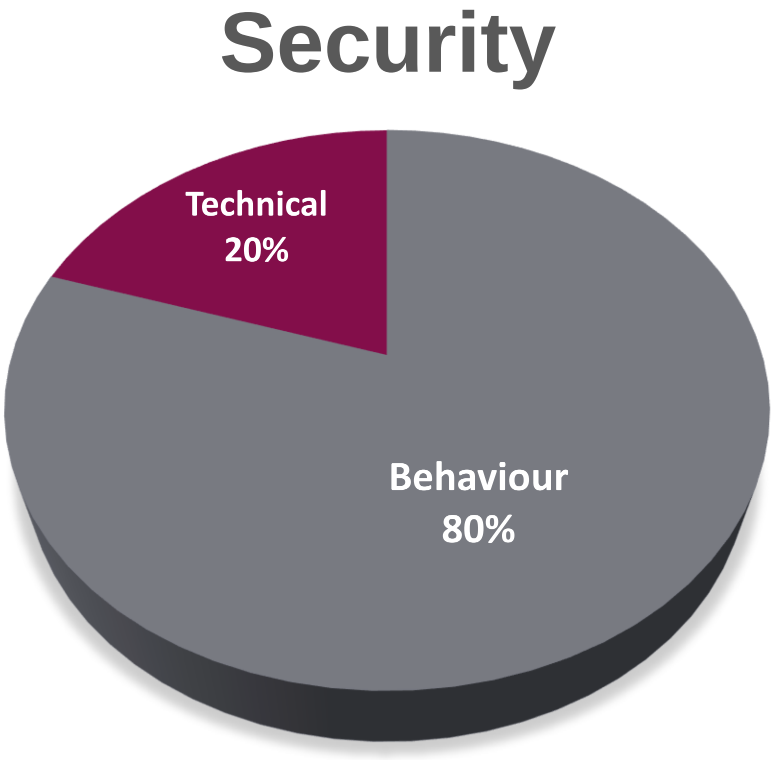
- Don’t use weak passwords
- Lock your device when not in use
- Secure your devices
  - Update/patch system and applications
  - Install applications only from trusted sources
  - Use anti-malware software
  - Don’t open attachments (from mail or chat) unless sure of the content
  - Don’t access untrusted websites
  - Don’t connect everything all the time
- Abide by the enterprise policy and procedures

Security tips: Social networking

- Once you publish something it’s very hard to take it back and sometimes impossible
- Limit the amount of personal information you post
- Be cautious with third-party applications
- Check privacy policies
- Don’t believe anything you read online
- Beware impersonation

Also: Stalking Bieber in Montclair / The 100 Best Screenwriters Ever per other screenwriters / Elizabeth Warren Gets Hillary-ed
TECH & DESIGN
NEW YORK
October 2–15, 2017
SPACE-BENDING HOUSES
BY WENDY GOODMAN
Facebook and Us
BY MAX READ
Plus
Preet Bharara's New Megaphone
By Andrew Rice
The Museum of Ice Cream's Walt Disney
By Anna Wiener
Silicon Valley's A Cappella Wars
By Jessica Pressler
And
Uber's Cavalry
NYMAG.COM
$6.99 USA/CANADA

The user is the first line of defense



Information security is as simple as **ABC**

Always **B**e **C**areful

Questions ?