Emerging risks in industry 4.0: innovative approaches for safety and security
Rome, 25 November 2019

Cyber-physical security threats to Occupational Safety and Health (OSH) in Industry 4.0

Dr. George Loukas
htttp://isec.group
University of Greenwich

Definition:

A cyber-physical attack is a security breach in cyberspace that adversely affects physical space

Why is OSH affected by cyber?

Machines

Computerised

Networked

People

Social engineering

Insider threat

Human error

The 1st order impact on employees

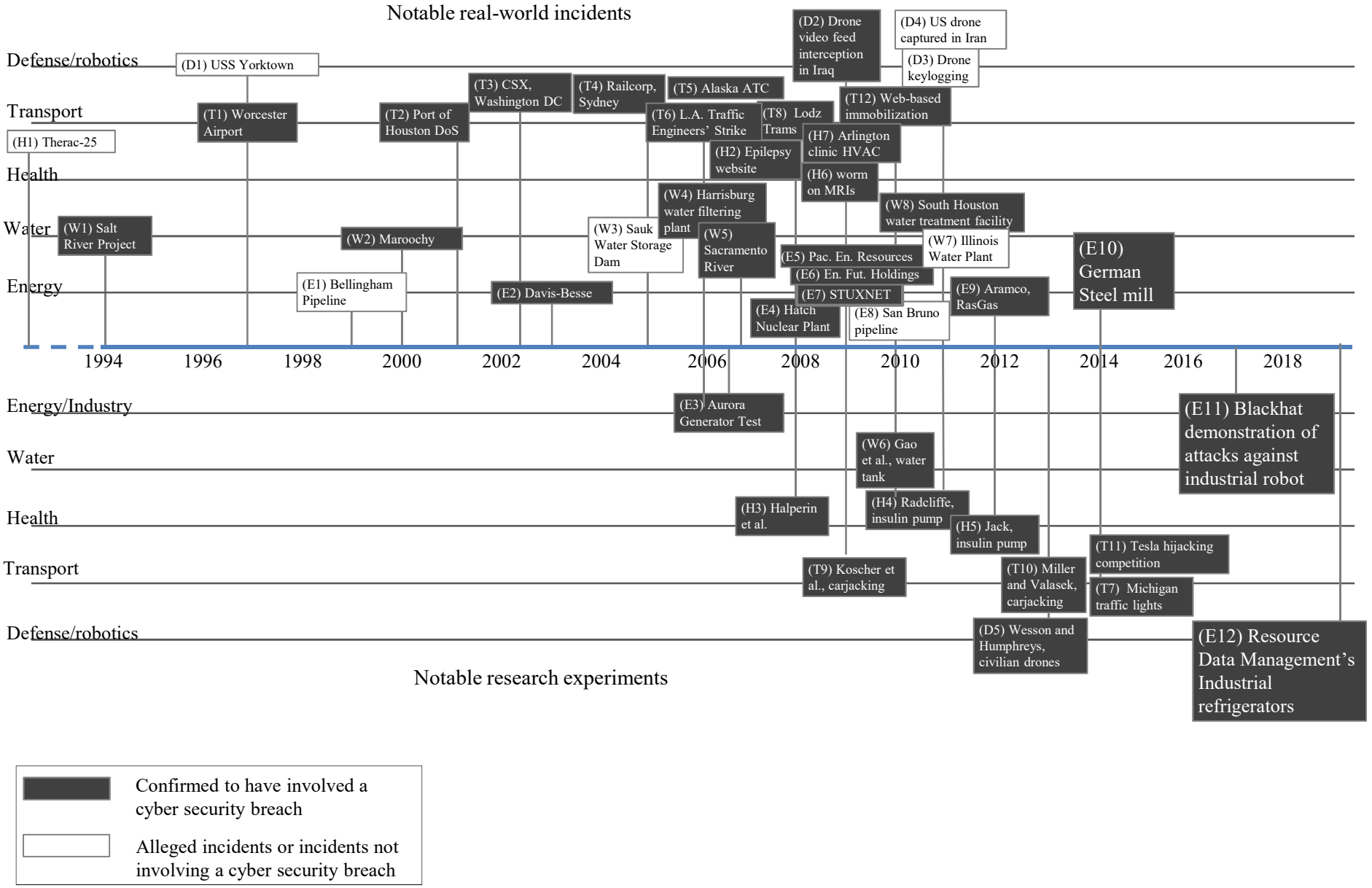
- Physical injury

When a machine's actuation is manipulated or its safety mechanism is disrupted

- Physical privacy

When a sensor (e.g., a camera) is compromised and leaked online

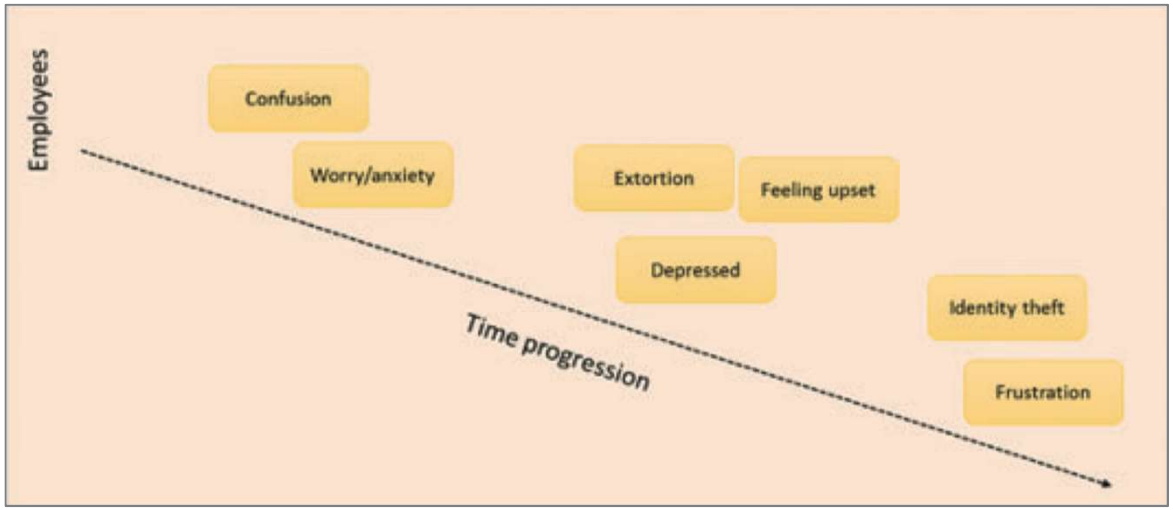
History of security breaches with impact on safety



The 2nd order impact on employees

Examples:

- Reluctance to trust intelligent machines after one misbehaves
- Feeling embarrassed/ashamed because of the information disclosed or for having been deceived by an attacker



Agrafiotis, I., Nurse, J.R., Goldsmith, M., Creese, S. and Upton, D., 2018. A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. Journal of Cybersecurity, 4(1).

ENISA's categorisation of vulnerable assets in industry 4.0

Industrial Internet of Things (IIoT) end devices

Robotics

Servers, systems

Industrial Control Systems (ICS)

Information

Algorithms

Cloud

Mobile devices

Smart robotics

Let's map some of these against impact on human

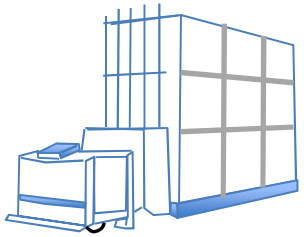
ENISA (2018). Good Practices for Security of Internet of Things in the context of Smart Manufacturing.

	Impact on System	Impact on human
IIoT end devices	**Sensor confidentiality**	**Physical privacy**

Examples:

Biometrics in building access control systems

Cameras on vision-guided Autonomous Guided Vehicles



	Impact on System	Impact on human
IIoT end devices	Sensor confidentiality	Physical privacy
Robotics	**Actuation modification**	**Physical injury**

Death at Volkswagen plant in Germany in 2015 was caused by human error:

A young external contractor was setting up a stationary robot when it grabbed and crushed him against a metal plate.

https://www.theguardian.com/world/2015/jul/02/robot-kills-worker-at-volkswagen-plant-in-germany

	Impact on System	Impact on human
IIoT end devices	Sensor confidentiality	Physical privacy
Robotics	**Actuation modification**	**Physical injury**

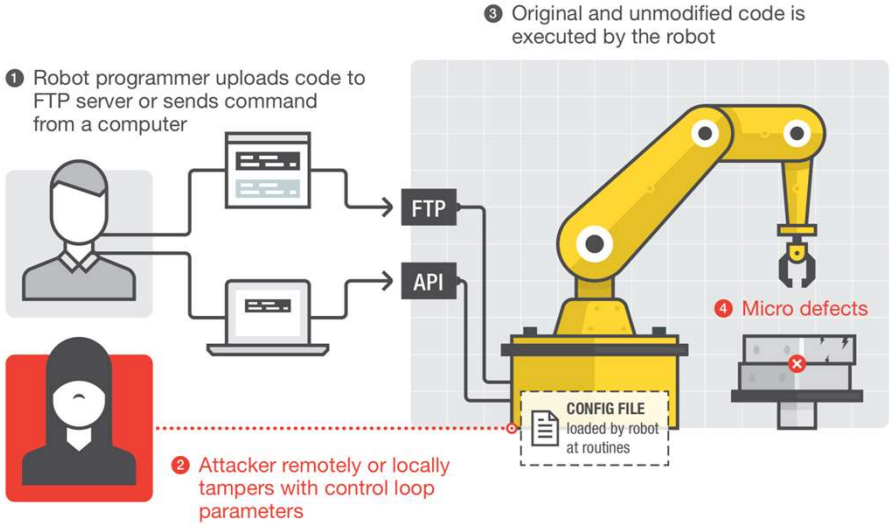
However, the same can be caused by a cyber attack

Example:

https://robosec.org

A joint research project between Politecnico di Milano and Trend Micro'

1. Altering the Control-Loop Parameters
2. Closed-Loop Control Detuning
3. Open-Loop Control Parameters Tampering
4. Robot Arm and Workpiece Configuration Tampering
5. Safety Limits Tampering



	Impact on System	Impact on human
IIoT end devices	Sensor confidentiality	Physical privacy
Robotics	Actuation modification	Physical injury
Servers, systems	**Actuation prevention**	**Physical injury**

Example:

*A worm disabled the safety display at **Davis-Besse** nuclear power plant.*

	Impact on System	Impact on human
IIoT end devices	Sensor confidentiality	Physical privacy
Robotics	Actuation modification	Physical injury
Servers, systems	Actuation modification	Physical injury
ICS systems	**Actuation prevention**	**Physical injury**

Examples:

Bellingham, Washington, pipeline ruptured because of slow-down of the SCADA system controlling it. When pressure started building up (due to unrelated damage), the SCADA system was unable to detect the buildup. It led to 3 deaths.

A natural gas pipeline explosion in San Bruno, California, that led to 8 deaths and 60 injured was partly attributed to unavailable SCADA pressure readings.

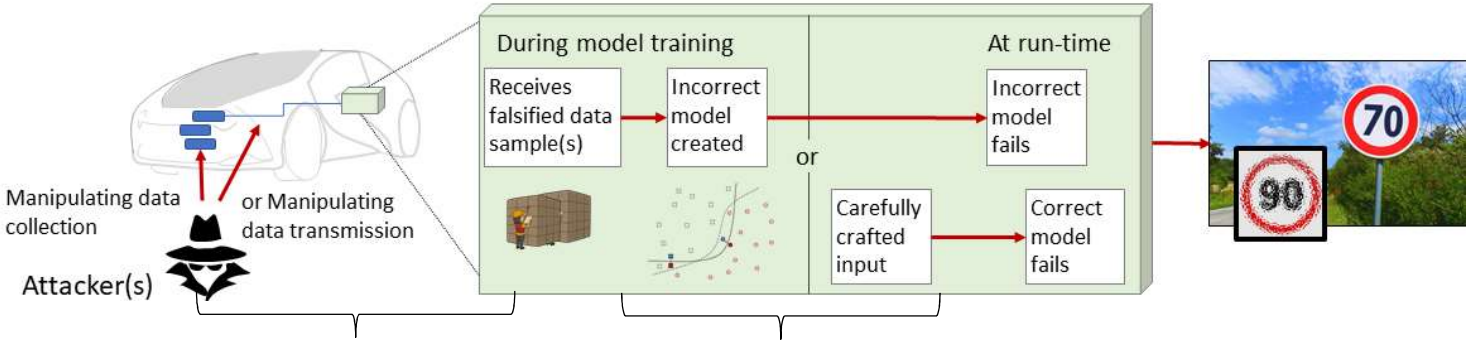
	Impact on System	Impact on human
IIoT end devices	Sensor confidentiality	Physical privacy
Robotics	Actuation modification	Physical injury
Servers, systems	Actuation modification	Physical injury
ICS systems	Sensor confidentiality	Physical privacy
Information	**Unauthorized actuation**	

Example:

*Automatic shutdown of the **Hatch Nuclear Plant** was triggered by wrong water level data*

	Impact on System	Impact on human
IIoT end devices	Sensor confidentiality	Physical privacy
Robotics	Actuation modification	Physical injury
Servers, systems	Actuation modification	Physical injury
ICS systems	Sensor confidentiality	Physical privacy
Information	Actuation modification	Physical injury
Algorithms	**Actuation modification**	**Physical injury**

Adversarial machine learning



Poisoning attack

Evasion attack

	Impact on System	Impact on human
IIoT end devices	Sensor confidentiality	Physical privacy
Robotics	Actuation modification	Physical injury
Servers, systems	Actuation modification	Physical injury
ICS systems	Sensor confidentiality	Physical privacy
Information	Actuation modification	Physical injury
Algorithms	Actuation modification	Physical injury
Smart robotics	**Actuation modification**	**Physical injury**

Detailed instructions on how to hack collaborative robotics systems are available online.

https://ioactive.com/exploiting-industrial-collaborative-robots/

Point no1:

The landscape of threats is exceptionally diverse

Technical defences against industry 4.0 threats

- Very advanced defences are currently being developed

Examples from isec.group/projects:

C4IIoT: Cybersecurity 4.0 - Protecting the Industrial Internet of Things
C4IIoT will build and demonstrate a novel and unified Industrial IoT cyber security framework for malicious and anomalous behaviour anticipation, detection, mitigation and end-user informing. The role of the my group is to equip the framework with the ability to decide dynamically where to process the security-relevant data it collects in a manner that takes into account the performance, energy and security of the system.

UK MoD/dstl "Safeguarding Autonomous Vehicles from Cyber Attacks"
We developed cyber-physical intrusion detection systems for robots to self-detect attacks against them. Both cloud-based remote and onboard.

- Individual industry 4.0 systems' vulnerabilities are being ethically disclosed to manufacturers, but patches are not always developed

Point no2:

Technical defences are still immature

The role of employees

- **Social engineering**

84-91% of all attacks start with a phishing email opened by a human user
(2016 Enterprise Phishing Susceptibility and Resiliency Report https://www.nuix.com/black-report/black-report-2018)

- Insider threat

75% of all attacks involving data are committed by an insider
(https://securityintelligence.com/news/insider-threats-account-for-nearly-75-percent-of-security-breach-incidents/)

- Human error

Many attacks are facilitated by human error
(failing to apply a software update, using easy password, …)

- Human sensors

Employees are usually the ones who **detect a security breach**
But often inform nobody and try to fix the problem themselves.

The typical attack path – for industry 4.0 targets

<u>Research target</u>

Preliminary research and reconnaissance

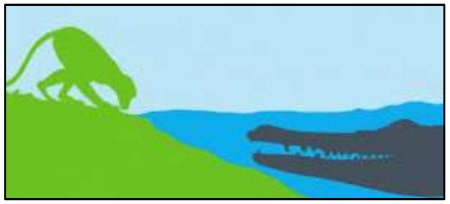
Vulnerability discovery

<u>Deceive user</u>

Spear-phishing

or

watering hole



<u>Enter business network</u>

Infect computer on business network for remote connection

Scan for entry point in control network (e.g., hole in firewall, VPN, …)

<u>Enter control network</u>

Gain access on device in control network (e.g., a workstation, data server, printer, …)

Gain access on HMI or specific PLC/RTU

Issue commands, change credentials, change firmware

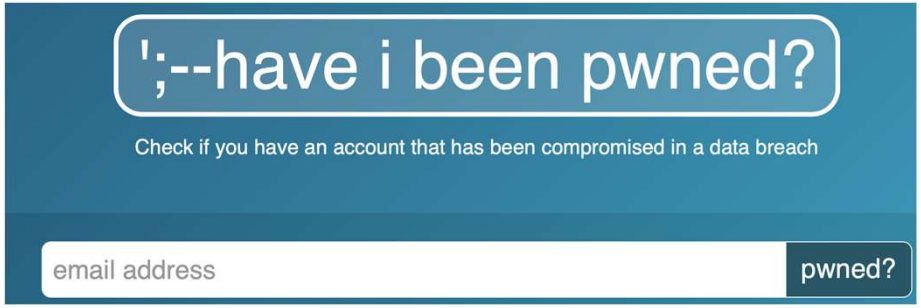
Cyber-physical Hygiene

- Disciplined approach to security of machines, computers, mobile devices and the network itself (e.g, the business's WiFi)
  (especially authentication and updates)

- Security awareness training of employees
  (+ employees need to know who to speak to)

- Recognise the importance of each employee's passwords

Check here, for example: https://haveibeenpwned.com



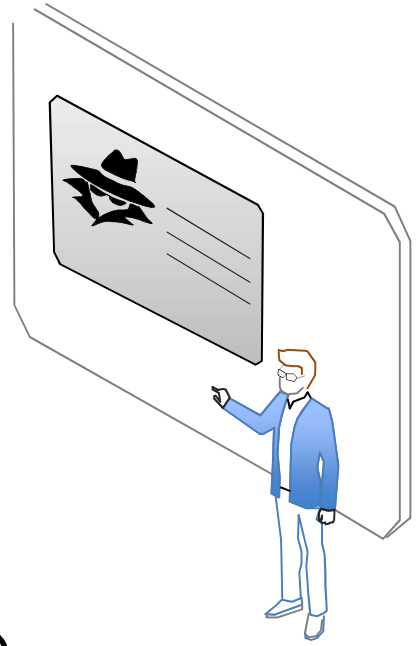
"The employees in my organisation still fall for cyber deception despite training"

There are some obvious reasons

Wasn't designed well

They didn't take it seriously

Wasn't tailored to them



But it is not just that.

Fear appeals don't work

Takes effort to be vigilant

Lack of consistency

Awareness is not training

Low priority to the individual

"Not my job"

Old habits die hard

Security fatigue

Almost no practice

No real reward

Risk perception

No monitoring

Rules learned are complex

Based only on **known** deception-based threats, but attackers adapt

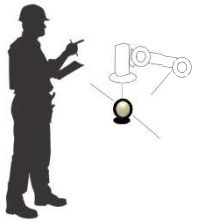
Maria Bada, Angela Sasse, Jason Nurse (2018) Cyber Security Awareness Campaigns: Why do they fail to change behaviour?

The real reason is:

It is hard

"What makes it hard?"

Reduced context

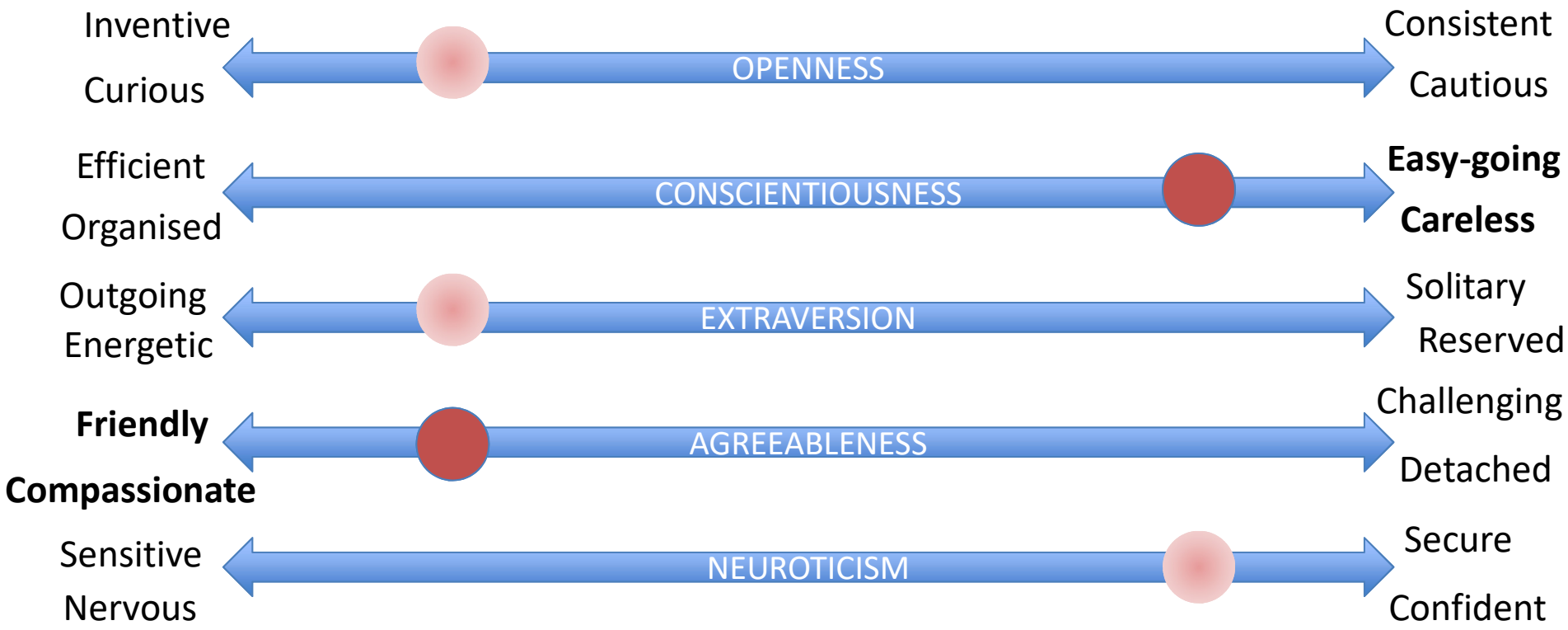


Cyberspace communication channels carry less information than face-to-face interactions.

Cues that we normally use to orient ourselves in face-to-face interaction **are unavailable** or **easily forged** in cyberspace.

Vrij, A. (2000). *Detecting lies and deceit: the psychology of lying and the implications for professional practice*. Chichester, UK: Wiley.

Even personality matters



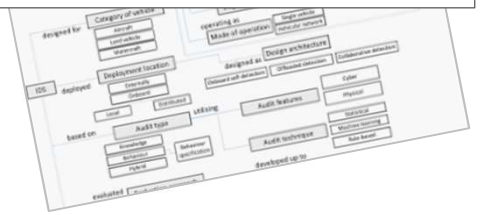
Halevi et al. (2015) Spear-Phishing in the Wild: A Real-World Study of Personality, Phishing Self-Efficacy and Vulnerability to Spear-Phishing Attacks
Parsons, K., Butavicius, M., Delfabbro, P. and Lillie, M., 2019. Predicting susceptibility to social influence in phishing emails. *International Journal of Human-Computer Studies*, *128*, pp.17-26.

Final point:

Human defences can fill some of the gap until technical defences mature, but the risk will always be there

Example roadmap for future research in OSH and cyber security

A taxonomy of cyber threats with OSH impact



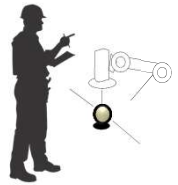
A formal cyber risk model that takes into account OSH impact

$$\max_{z} \sum_{i=0} A_i R_i \left\{ \prod_{\sigma=1} \quad \right. \quad j=0$$

$$\text{s.t.} \sum_{\sigma=1}^{|\mathcal{U}|} \sum_{\lambda=0}^{|\mathcal{L}|} F(\delta_{\sigma,\lambda})\, z_{\sigma,\lambda} \leq B,$$

$$\sum_{\lambda=0}^{|\mathcal{L}|} z_{\sigma,\lambda} = 1, z_{\sigma,\lambda} \in \{0,1\}, \forall \sigma = 1,2,\ldots,|\mathcal{S}|.$$

Apply model and taxonomy on real use-case, such as collaborative manufacturing



Training users how to recognize cyber-physical misbehaviour

Early warning mechanisms for cyber-physical safety breaches

Automated protection against cyber-physical safety breaches

Thank you

isec.group

g.loukas@gre.ac.uk