EU CHECK

THREATS IN THE TECHNOLOGICAL FUTURE

CONVERGENCE 2023, Brussels, Belgium

1 December 2023

Jarno Salonen (VTT) & Koen Teuwen (TU/e)

Background

EU CHECK

Ongoing “arms race” of cyber threats and defences against them.

Most visions (e.g. Forbes, WEF, Microsoft) focus on short or intermediate time span. Long-term visions are “safe”:

- *A world with no privacy* - BBC Future 2017: “10 grand challenges we’ll face by 2050”
- *Less about confidentiality…more about integrity and provenance* - WE Forum 2023: “7 trends that could shape the future of cybersecurity in 2030”
- *Credit card thief knows your PIN* - Kaspersky - Secure Futures Magazine 2023: “How will cybersecurity change by 2050?”

Aim: What are the technological trends in the eyes of a young generation of academics with a digital security interest?

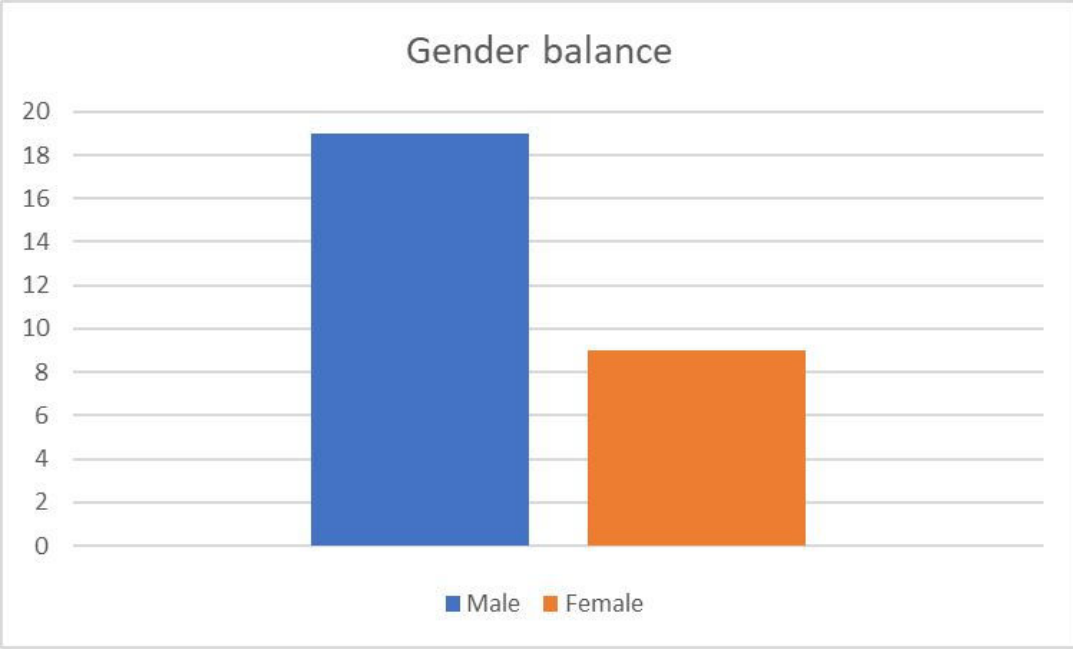
RQ1 What assets are perceived to be most critical in the future?

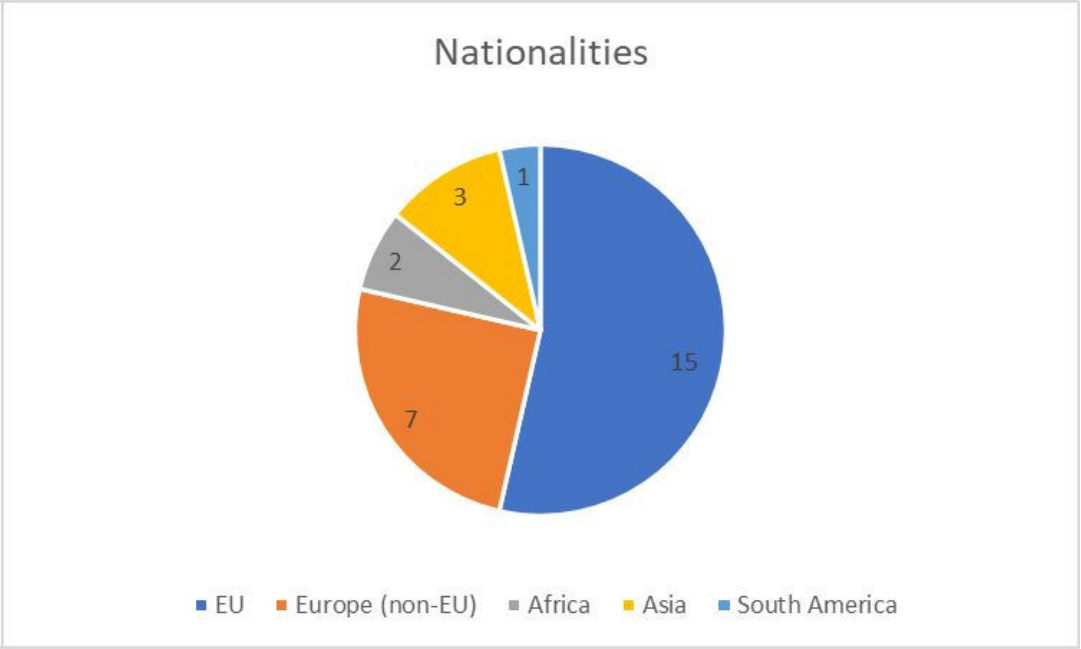
RQ2 What digital threats are perceived to pose a risk to these critical assets?

Information collection

EU CHECK

FOSAD 2023 workshop in Bertinoro, Italy 28.8.-1.9.2023 with 28 participants (International School on Foundations of Security Analysis and Design)





Information collection (2)

EU CHECK

We asked the workshop participants to respond to three questions (in groups)

1. What does the digital/technological future look like in 2050?

2. What are the top-3 assets that need to be protected?

3. For each asset from the previous session, please identify three (digital) threats that need to be contained or mitigated

Results overview

EU CHECK

Diverse results within and across groups:

- Pessimistic vs. optimistic
- Physical assets vs. intangible assets
- Specific assets vs. broad assets
- Threats vs. threat vectors vs. impacts

Critical infrastructure (1)

EU CHECK

Increasing interdependency and automation:

- Internet
- Electricity
- Water

Critical infrastructure (2)

EU CHECK

Availability:

- Denial of Service (Dos) attacks
- Supply chain attacks

Confidentiality:

- Mass surveillance

Insider threats, Advanced Persistent Threat (APT) groups

Data (1)

EU CHECK

Variety of interpretations:

- Public data
- Personal data
- Confidential data

Important for automation

Data (2)

EU CHECK

Confidentiality/Privacy:

- Phishing attacks

Correctness:

- Spreading of misinformation

Availability:

- DoS through overloading

Environment

EU CHECK

Ecosystems and natural resources

Availability:

- Overexploitation

Integrity:

- Attacks on Operational Technology (OT)

Life & miscellaneous

EU CHECK

Mental wellbeing and human rights

Threatened by:

- Artificial Intelligence (AI)
- Surveillance
- Monopolies and algorithms

Discussion & conclusion

EU CHECK

Not based on past observed events, but experience of young academics

Critical infrastructure, data, and the environment

Availability at risk

Step towards security by design

Future work:

- Finalising the article and submitting it to a conference/journal
- Conducting a survey to a wider target group (e.g. Youth4Cyber)

Funny fact: Lack of skilled professionals is no longer an issue in 2050

Thanks!

EU CHECK

Source: https://sites.google.com/uniurb.it/fosad/home/fosad-2023