The intersection of climate change and cybersecurity:

environmental hazards' impacts on cybersecurity infrastructure, sustainable ICT and comprehensive risk management of cyber and climate-related risks

Piret Pernik

Strategy Researcher

CCDCOE

Piret.Pernik@ccdcoe.org

CCDCOE

1. Comparison of economic costs

- → The two-year Russian war in Ukraine is estimated to have caused C02 emissions at cost $32 billion.
- → Two cyberattacks that caused the greatest economic losses, NotPetya and Wannacry, cost 14 billion euros.
- → Cybercrime in the US costs $12.5 billion in 2023 (FBI)
- → The 2021 flooding in Germany and Belgium cost €44 billion
- → The 2022 drought in Europe cost €40 billion
- → In 2022, all climate events in Europe amounted to €52.3 billion

CCDCOE

2. Climate change-related environmental hazards to cyber-physical systems

- → NATO report: cyberattacks against environmental data, the manipulation of environmental data, instrumentalizing climate change to spread disinformation and propaganda, sow distrust, and undermine democratically elected governments
- → Direct risks
- → Indirect risks

3. Carbon footprint of the ICT sector

- **Data centres' current consumption**
- In 2022, data centres and networks consumed 1% of energy-related global GHG emissions (0.6% of total GHG emissions)
- The ICT sectors' carbon footprint is estimated between 1.5-4% of global GHG emissions; the EU digital Strategy (2020): more than 2% of global GHG emissions
- However, in 2018 EU28 data centres' share was only 0.4-0.6% of total EU28 GHG emissions
- **Projected increase of GHG emissions**
- In the US, the compound annual growth rate in data centers' power demand will be 15% until 2030 (Goldman Sachs);
- in the EU a 28% increase of electricity demand from the 2018 level is expected by 2023 which is from 2.7% of total EU electricity demand in 2018 to 3.21%by 2023 (European Commission)

3. (cont.) Carbon footprint of the ICT sector

→ **AI**

→ Unsubstantiated popular claim: AI consumes 2% of total GHG emissions (airline industry)

→ One researcher predicts that AI servers could use 0.5% of global electric generation by 2027

→ Fine-tuned AI models consume less than generic ones (difficult to estimate an average consumption)

→ Microsoft's indirect emissions increased by 30.9%, in 2023; and direct and indirect emissions were up 29.1% from the 2020 baseline; Google had 13% increase due to data centres and supply chain (chips)

→ The IEA anticipates that by 2026, the AI industry's total energy consumption will be at least ten times its demand in 2023; Gen Mark Milley: a third of US military robotic in 10-15 years

3. (cont.) Carbon footprint of the ICT sector

→ **Sustainable ICT/cybersecurity sector**

→ Currently proven AI-enabled use cases could reduce emissions by 5% to 10% by 2030 (Boston Consulting Group 2021)

→ AI has the potential to reduce global GHG emissions by 4% in agriculture, energy, transport, and water (Microsoft/PwC)

→ Companies reported reductions from AI apps between 11.3-14.3%; executives believe that AI could reduce overall GHG emissions by 15.9% in the next three to five years (Capgemini survey)

→ If the entire ICT sector 0.6-4% of GHG emissions, cybersecurity part could be 10-15% of that (10-15% of the total IT budget spent on cybersecurity in average)

4. International sustainability initiatives

→ The UN

→ Private sector commitments

→ The EU

→ NATO

CCDCOE

5. Integrating cyber risks and risks from extreme weather events: comprehensive risk management

→ Little awareness in the cybersecurity community about the impact of climate change, extreme weather events on cybersecurity. The cybersecurity community is less focused on the physical damage

→ Climate-related environmental hazards are currently not integrated into EU cybersecurity policies, strategies, risk assessment and management, incidence reports (CI/KR regulations address largely superficially)

→ The ENISA cyberthreat report (2024): environmental disruption ranks at the 10th place among 21 top threats (survey)

6. Conclusion

→ Improve monitoring and adaptability to address both types of risks
  - Better transparency and evidence based data about GHG emissions of large data centres' and foundation AI models
  - Provide quantitative and qualitative data, and comparative studies on the impacts of climate change on cybersecurity infrastructure, networks, and devices,
  - Provide specific guidance for assessing climate-related risks and fostering resilience to them within the cybersecurity sector

→ Climate change-related risks should be managed in a standardized way across EU member states due to cross-sector and cross-border interdependencies. Integrate environmental hazards into cyber/digital CI/KR risk management processes and frameworks, utilizing the mentioned concepts and approaches.

→ Cross-fertilization across both domains could be useful (resilience, business continuity, mission assurance, risk based approach) relevant to both types of risks

6. (cont.) Conclusion

→ Develop policies and processes to choose cybersecurity solutions with the highest PUE and lowest GHG emissions, reduce e-waste and cooling water consumption, develop and implement AI applications for increasing PUE, and monitor and assess the progress towards net zero GHG emissions

→ Issue specific guidance on integrating climate-related risks into cybersecurity policies, strategies, risk management frameworks and incident response plans