Cybersecurity regulation in the age of AI: from dilemmas to practical solutions

With the rise of AI-powered cybersecurity tools and techniques, there is a growing concern that malicious actors could use these tools to carry out more potent cyber-attacks. As AI increasingly integrates into our daily lives there is a need to ensure that AI technologies are developed and used safely.

Cyber robustness, which refers to the ability of AI systems to withstand cyber-attacks and maintain their functionality in the face of malicious activity, is one of the key principles for trustworthy AI developed by the OECD.

The overlap between AI and cybersecurity raises a number of challenges, some of which could be addressed through effective regulation. Thus, in order to ensure that AI systems are cyber robust, it is important to establish clear standards and balanced regulations. The question faced by cybersecurity regulators across the globe is what such standards and regulations should include.

Moreover, it is inevitable that effective cybersecurity of AI systems should require a multi stakeholder approach involving collaboration between governments, industries, academia, and civil societies. It seems appropriate, therefore, to examine what such an approach might look like in the context of AI robustness regulation.

The round table will attempt to tackle these challenges to propose a regulatory and technology expert from governments, standards organizations and civil society, to address the following questions:

1. What are the key issues that need to be addressed in legal frameworks and technical standards for AI development and use?

2.How can cybersecurity regulation help promote an ecosystem in which AI systems are cyber resilient and maintain their functionality in the face of cyber-attacks?

3 Given that AI systems are based extensively on commercial and personal data, what are the standards and regulations that need to be in place to ensure data protection, privacy, and transparency in AI systems?

4. What are the guidelines and regulations that need to be in place to prevent the misuse of AI-powered tools and techniques to ensure accountability of use?

5. How can a multi-stakeholder approach be used to ensure effective regulation of AI in cybersecurity? What role does regulation have in enabling this approach?

In this session we hope to contribute to global discussions on AI robustness regulation by practical suggestions for cybersecurity.

Daria Tsafrir, Adv
Legal Advisor
INCD
dariat@cyber.gov.il