Trustworthy AI requires solid Cybersecurity

At the third annual ENISA-Europol Internet of Things (IoT) Security Conference, it was Artificial Intelligence (AI) that was the newcomer on the scene. The rise of AI technologies requires a new dialogue and awareness of the related cybersecurity challenges.

Published on October 25, 2019



Tagged with

* [Cyber Threat Analysis](https://www.enisa.europa.eu/search?Subject%3Alist=Cyber%20Threat%20Analysis)
* [cybersecurity](https://www.enisa.europa.eu/search?Subject%3Alist=cybersecurity)
* [5G](https://www.enisa.europa.eu/search?Subject%3Alist=5G)
* [Cyber Threat Agents](https://www.enisa.europa.eu/search?Subject%3Alist=Cyber%20Threat%20Agents)
* [Cyber Attacks](https://www.enisa.europa.eu/search?Subject%3Alist=Cyber%20Attacks)

ENISA, the European Union Agency for Cybersecurity and Europol, the EU Agency for Law Enforcement Cooperation, co-organised successfully their third annual IoT Security Conference on the 24th and 25th of October in Athens looking at the evolution of IoT security and how to implement adequate security measures.

Beyond technical aspects, the adoption of IoT and emergence of AI has raised many new legal, policy and regulatory challenges, broad and complex in scope. In order to address these challenges, cooperation across different sectors and among different stakeholders is essential.

It is for these reasons that Europol and ENISA are jointly organising such an event, to facilitate a discussion among all interested parties on ways to address the security challenges of IoT and AI and to combat the criminal abuse of such technologies, ultimately making cyberspace a safer place for all.

 ENISA’s Head of Core Operations, **Steve Purser**, stated:

“The annual IoT Security Conference keeps up with the trends of new opportunities and challenges of emerging technologies. This 3rdedition focuses on the impact of IoT and AI technologies. As these technologies are being deployed across various sectors, cybersecurity is a primary condition for trustworthy IoT and AI. ENISA is prepared to support technical aspects as well as policy with regards to ethics and a coordinated strategy on AI and liability. I welcome the collaboration with Europol and I am confident that such joint efforts contribute significantly to ensuring a safer and secure connected future for all.*”*

**Steven Wilson**, Head of Europol's European Cybercrime Centre, said*:*

"The importance of the Internet of Things and Artificial Intelligence has become undeniable, as these technologies have the potential to help us respond to societal challenges while making our lives more efficient. Both the public and private sector are devoting significant efforts to maximise the opportunities of these developments. Europol focuses on how IoT and AI can enhance law enforcement capability with respect to fighting and investigating crimes, while reflecting and identifying how criminals can and will abuse their potential. Through our joint work with ENISA at the IoT Security Conference, we can proactively respond and ensure that we anticipate the next criminal move while simultaneously protecting citizens across the EU, and ensuring that the benefits of these technologies prevail."

**IoT Security Attacks**

Over the last few years, prominent examples of IoT attacks have made media headlines such as the hacking of pacemakers and smart toys for kids. Even artificial intelligence algorithms have been manipulated, leading to erroneous decision-making such as spoofing of traffic lights and false image recognition. With IoT technologies, the digital and the physical worlds are no longer kept apart from one another. Cars, medical devices, factories and energy plants are all becoming increasingly interconnected, creating new types of threats against critical infrastructure.

**Europol's and ENISA's efforts on IoT security**

ENISA has a strong record in IoT security, publishing many reports on the subject, identifying security threats and risks and providing recommendations to strengthen its security, such as the Baseline Security Recommendations for IoT.

On the other hand, Europol has been researching the many advantages of the Internet of Things for law enforcement as a tool to fight crime. Data from connected devices at a crime scene can provide crucial evidence to an investigation but such data require the same safeguards and security standards to ensure the privacy and safety of citizens. It has also successfully supported operations targeting the criminal abuse of IoT devices such as ‘Operation PowerOff’.

**Working towards a more secure and safe future of AI**

The conference pointed out that one of the biggest challenges brought about by AI is the question of trust. Future AI deployments need to be secured appropriately, for instance by establishing a platform to promote collaboration on the cybersecurity aspects of AI in the EU.

ENISA can help build understanding on AI building blocks and their interplay, engage stakeholders in dialogues for AI cybersecurity and encourage collaboration and establish synergies, as well as raise awareness on AI cybersecurity.

Equally law enforcement needs to be in a position to address the criminal abuse of AI as well as adversarial AI for instance in the form of data poisoning or the manipulation of algorithms.

There is a close relationship between AI and data governance. For machine learning algorithms to be effective, it is essential to have relevant training data and to control this learning process to avoid any bias.

**Conclusions and actionable suggestions**

* Security should not be an afterthought when designing systems and products, IoT and Artificial Intelligence are no exception;
* The inclusion of law enforcement enables a response beyond defence and incident response by being able to investigate and prosecute the criminals abusing connected devices;
* Building on the cooperation in IoT security, law enforcement and the cybersecurity community need to work closely together to address the criminal abuse and security of AI;
* There is a need to discuss digital forensics in regard to Artificial Intelligence and IoT and the importance of data and privacy protection, considering the amount and different categories of data collected by these algorithms and the possibility to manipulate them;
* Whereas horizontal guidelines to ensure IoT and AI security are much needed, it is also important to look into sectorial implementations such as autonomous cars, industrial automation, automation of cybersecurity operations, to name a few. ENISA will be soon publishing guidelines on securing the software development process for IoT, as well as on cybersecurity of autonomous vehicles.
* IoT and AI are part of a wider interlinked emerging technologies ecosystem that also comprises 5G and Cloud computing; the interplay between all these elements needs to be considered when addressing cybersecurity.