Press release 2

NOTIONES held its 2nd annual conference

Second annual conference of NOTIONES convened on 12 of May 2023, in Paris. The aim of the 2nd NOTIONES conference was to address the pressing challenges confronting Law Enforcement agencies, focusing on emerging issues such as generative AI, cybercrime with a particular emphasis on cryptocurrency, and the proliferation of disinformation. These topics were aligned with the ongoing work in Working Groups 3 and 4. The conference, themed "Generative AI and Other Related Challenges for LEAs," provided valuable insights into tackling emerging threats in the security landscape, and saw participation from 44 individuals, including representatives from 11 different organizations.

Keynote speeches by Paolo Venturoni from EOS, Livia Di Bernardini from APRE, and Eva Škruba from EACTDA set the stage for discussions on AI in the security ecosystem, emerging innovation monitoring for LEAs, and operationalizing technological solutions in cybercrime combat.

Cybercrime challenges: Prof. Shlomo Shpiro from Bar Ilan University led discussions on the use of emerging technologies by terrorists, followed by presentations on tools for tracing cryptocurrencies and disrupting illicit money flows by industry experts.

Disinformation Solutions: Michal Choras from Bydgoszcz University Of Science And Technology addressed challenges in disinformation detection, complemented by presentations on AI validation for misinformation and projects like FERMI and vera.ai.

Revolutionizing Security: European Organisation for Security Unveils AI Solutions to Tackle Emerging Threats

In a keynote speech, Paolo Venturoni, CEO of the European Organisation for Security (EOS), revealed advancements in utilizing artificial intelligence to address evolving security challenges. The presentation emphasized the critical role of AI in navigating the complexities of the modern security landscape, particularly in combating state-sponsored and hybrid threats.

Venturoni highlighted the rise of generative AI and its potential to deceive, making it increasingly challenging to discern between genuine and fabricated content. However, advancements in technology enable the detection of hybrid threats, as tools used in such attacks leave traceable trails that can be identified and tracked. The presentation underscored the vulnerability of critical infrastructure, such as airports and train stations, to cyber attacks, including "Spoofing attacks" facilitated by generative AI. Despite these vulnerabilities, AI-based systems offer a promising avenue for enhancing security by adapting to evolving threats in real-time.

Machine learning technologies emerged as a key tool in addressing hybrid threats by monitoring criminal transactions and detecting changes in criminal behavior. The presentation emphasized the importance of exploring opportunities to utilize AI in cryptocurrency monitoring to combat financial crimes effectively.

Venturoni discussed the implications of EU regulations on emerging technologies, expressing concerns about potential drawbacks for the security industry. Excessive regulatory burdens, particularly related to regulatory sandboxes, may hinder the adoption of innovative AI tools by Law Enforcement Agencies (LEAs).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021853.

The presentation highlighted challenges faced by start-ups in the AI industry, with many considering relocation outside the EU or discontinuing AI projects due to regulatory concerns. The EU's regulatory framework, particularly Article 14 (Human oversight) of the Artificial Intelligence Act, was scrutinized for its potential impact on AI development.

Highlighting the interconnected nature of security threats, Venturoni emphasized the importance of directing investment towards civil security technologies to complement defense capabilities. Collaboration on a global scale is essential to address state-sponsored security threats effectively.

Paolo Venturoni concluded the keynote speech by stressing the need for a balanced approach to AI regulation, one that promotes innovation while safeguarding security and fundamental rights.

Key innovations presented:

Developing AI tools for LEAs. TRACE Project (GA No101022004)

The TRACE project, led by Thomas Havranek from CIN Consult GmbH, made a significant stride in combating financial crimes with the introduction of its AI tool. TRACE aims to empower LEAs with advanced technologies to identify and track illicit money trails, including those involving cryptocurrencies and Non-Fungible Tokens (NFTs). By leveraging advanced AI tools, LEAs will be equipped to better investigate and address illicit money flows while enhancing information sharing among EU agencies and ensuring compliance with legal and ethical standards.

During the presentation, the TRACE project showcased several case studies demonstrating the diverse range of illicit activities it addresses. From terrorism financing to cyber extortion and money laundering via NFTs and online gambling, the TRACE tool is designed to tackle complex financial crimes effectively. TRACE seeks to contribute to policy development by advocating for the harmonization of evidence collection procedures, streamlining data for AI systems, and regulating emerging digital assets like NFTs. Additionally, the project aims to improve investigation tools and systems, including enhancing the analysis of digital media and hidden service directories.

The highlight of the presentation was the unveiling of the TRACE tool, equipped with state-of-the-art features to handle vast amounts of data efficiently. Utilizing optical character recognition (OCR) technology and a full-text search engine, the tool enables swift data analysis. The integration of a Crowd Knowledge Graph enhances insights, while dynamic visualization capabilities aid in data exploration and comprehension.

Fake news risk mitigation FERMI project (GA No 101073980)

The FERMI project took center stage at the Conference presenting strategies to tackle the growing threat of disinformation. With a focus on supporting LEAs, FERMI showcased its holistic approach to mitigating the risks associated with fake news.

The presentation provided insights into the historical context of disinformation, highlighting the evolution of tactics in the digital age.

Focused on advancing investigations and assessing threats, the FERMI platform equips LEAs with powerful tools to combat disinformation. By analyzing social media data, the platform identifies key actors in disinformation campaigns and assesses the likelihood of offline crimes. Additionally, it provides insights to facilitate information exchange among LEAs.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021853.

The FERMI project is committed to enhancing community resilience and decision-making processes. Through community resilience assessments and situation analysis tools, LEAs will be empowered to respond effectively to disinformation campaigns. The project also aims to refine its analysis on propagators of fake news, particularly focusing on left-right extremism.

In an open discussion, participants addressed challenges in distinguishing between human-operated accounts and automated bots, emphasizing the importance of ethical considerations in assessing information authenticity. Concerns about potential biases were also acknowledged, with a commitment to prioritize threats originating from regions posing a significant risk to democracy and European values.

VERA.AI Project (GA No 101070093)

Vera.ai is a pioneering European-funded project aimed at developing AI and network science-based methods to assist verification professionals in combatting disinformation. With a focus on innovation and collaboration, Vera.ai strives to stay at the forefront of technological advancements in content verification.

Vera.ai unveiled user-facing tools including the InVID-WeVerify Verification plugin, Truly Media, and the Database of Known Fakes. These tools have garnered widespread adoption among media professionals and human rights activists across Europe and beyond. Notably, the "Fact-checker in the loop" AI design approach simplifies fact-checking processes, minimizing technical complexities and errors. The project showcased promising results, such as achieving high accuracy in identifying frequency-based artifacts in images downloaded from Twitter. Additionally, the project conducted a Person-of-Interest (PoI) analysis to detect deepfakes in videos, exemplifying the efficacy of AI in combatting disinformation.

Vera.ai is committed to further empowering professionals by enhancing web-based assistants, introducing chatbots to explain AI tool outputs, and facilitating low-overhead flagging of errors. The project actively collects images to enhance fake detection effectiveness, demonstrating a proactive approach towards combating misinformation.

The NOTIONES project will continue to assess and test innovations to ensure they meet the needs of panEuropean practitioners in security and intelligence area.

NOTIONES is an EU-funded project dedicated to enhancing security and intelligence practices through the adoption of innovative technologies. By facilitating collaboration between stakeholders and leveraging emerging solutions, NOTIONES aims to strengthen the capabilities of Law Enforcement Agencies (LEAs) in addressing contemporary security challenges. Discover more about NOTIONES on: Website | LinkedIn | X Twitter

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021853.