Contribution ID: **183** Type: **Presentation**

Regulate, Respond and Rectify: Reviewing the Governance and Technologies Behind Cyber Crime Attribution

Tuesday 14 October 2025 17:17 (11 minutes)

Core Idea

As part of the United Nation's Sustainable Development Goals, justice and apprehension of criminal activity is imperative for fostering healthy communities. Given the rise of cyber criminality, developing strong crime attribution practices and legal infrastructures is more important than ever. Notably, the cyber threat landscape is being revolutionised by emerging technologies such as AI and Blockchain. These technologies are forever changing the way crime is performed, and how it's intercepted. However, over-arching issues in law enforcement's legal structure is inhibiting effective countermeasures against them, and online crime as a whole.

This paper investigates the current state of cyber crime attribution. It reviews the technologies used in digital forensic efforts, and their influence on the legal frameworks underlying law enforcement. By relating this to case studies in scams and cryptocurrency crime response, it delivers impactful insights into the current shortcomings of global cyber crime mitigation. Finally, we provide an up-to-date analysis of recent events, forums and workshops in internet governance, which provides indication of the future directions in cyber crime mitigation, from both a legal and technical perspective.

Ultimately, these insights are distilled into three over-arching issues that impinge upon the successful deployment of crime prevention technologies. From these, we offer insight into the strategies being devised to mitigate these issues, and provide actionable future recommendations to achieve more effective technical and legal interventions to cyber crime.

Context of Presentation

This presentation directly addresses cyber crime attribution from an inter-disciplinary standpoint of how technology is influencing internet governance. It amalgamates information from academic literature, press releases, workshops and conferences. As such, it provides a holistic perspective of the digital forensic processes. It focuses on the technologies utilised by both law enforcement and cyber criminals, and how these are reshaping the legal infrastructures behind criminal takedowns.

AI and Blockchain are of particular importance, due to their revolutionising effect on modern life. Blockchain's pseudonymity, transparency, security and immutability make it ideal for ethical data storage in forensic efforts. Additionally, many experts have identified AI as a solution to digital forensics' longstanding crisis with non-uniform, heterogeneous data from various sources.

At the same time, these technologies have become a double-edged sword. Criminals have been leveraging them for their own purposes. Since 2018, cryptocurrency crime has increased by 524%. The entirety of crypto crime from that year was the equivalent to the amount lost in 2024 from scams alone. AI is also making crime more accessible than ever, with Generative AI being frequently used to facilitate wide-scale scams and extortion.

Due to the inherent slowness of internet governance, criminals are far out-stripping law enforcement with the adoption of these technologies. This is further magnifying the rise in cyber crime, and compounding digital forensics' data volume crisis. In realising this shortcoming, internet governance entities such as auDA, the UN, ICANN and the IGF are moving towards international standardisation and scaling of laws. Their proceedings, which are being accentuated in 2025, are focused on addressing these gaps in AI and blockchain regulation.

Due to the recency of these events, they are yet to become widely discussed in academic literature. To the best of our knowledge, this is the first work which systematically reviews the new developments in internet governance, and their effects on cyber crime.

Audience to whom it is relevant

This presentation is of direct interest to a range of professionals. Fundamentally, it analyses the adoption of new technologies on a global scale. As such, it's of direct interest to technical experts in the fields of AI and Blockchain. Additionally, this paper's commentary on internet governance is of interest to experts from a legal background. People from cyber security and law enforcement will similarly benefit. Finally, the multi-disciplinary nature of international governance models means that experts from these backgrounds and many more can help deliver an impact.

The audience in this presentation will benefit in several ways. Notably, they will gain insights into the current state of online crime due to the emergence of AI and blockchain. They will learn how it's being used to facilitate cyber criminality, particularly in scams and fraud. Furthermore, it provides insight into how these technologies are being used by law enforcement against criminals. In refocusing these topics to a legal perspective, the audience will be able to see these problems from a different lens. They'll be educated on the ISO standards, data safety and privacy protocols behind forensic efforts. These will prove instructional when discussing the issues with global technological adoption. Finally, this will help inform their judgements on the key topics for the UN's internet governance forums in 2025, and how these technologies are shaping them. In total, the audience will receive a high-level view of how emerging technologies are revolutionising the landscape of cyber crime attribution, both on a technical and legal front.

Primary author: GAUL, David (University of Queensland)

Co-authors: Prof. KO, Ryan (University of Queensland); Prof. MUTHUKKUMARASAMY, Vallipuram (Griffith University)

Presenter: GAUL, David (University of Queensland)

Session Classification: Presentations Session 6: The Transformative Role of Data in SDGs and Disaster Resilience

Track Classification: SciDataCon2025 Specific Themes: The Transformative Role of Data in Sustainable Development Goals and Disaster Resilience