Mid-Module Assignment 1 Presentation Transcript

EncroChat Hacking Case Study: Australia

By: Xue Ling Teh

[Opening Slide]

Speaker: Good day, thank you for joining my talk today. My name is Xue Ling, and I will be presenting on the EncroChat hacking case study, with a primary focus in Australia.

[Slide 2: Introduction]

Speaker: As reported in Eurojust (2020), a joint investigation team (JIT) led by the police, including French and Dutch law enforcement and judicial authorities were successful in the targeted infiltration of EncroChat, an encrypted communication app that was marketed as having guaranteed anonymity. In this presentation, we will dive into the different aspects of the EncroChat case study and its implications in Australia.

[Slide 3: Table of contents]

Speaker: Here are the five main sections we will explore. The first section introduces the use of EncroChat as part of criminal investigations in Australia, specifically in online scams. Next, we will look into how technology is used in cybercrime, such as the ways police work with technology in dealing with cybercrime or the use of technology such as EncroChat by cybercriminals to commit cybercrime. After that, we will dive into the gains and challenges observed by Australia's law enforcement in using evidence from hacking EncroChat, followed by jurisprudence in court, debates and narratives concerning the

legalities of the EncroChat evidence. Lastly, we will look at public opinion and perception regarding this case and wrap up with the conclusion.

[Slide 4: EncroChat Criminal Investigation]

Speaker:

[Slide 5: Technology Usage in Cybercrime]

Speaker:

[Slide 6: Gains & Challenges]

Speaker:

[Slide 7: Jury trials]

Speaker:

[Slide 8: Public opinion]

Speaker: There is divided public opinion among netizens on the authorities' strategy of hacking EncroChat whereas some had mixed reviews from both sides. One side commended the strategy in capturing organised cybercriminals. On the other hand, there were those who disapproved the disclosure of the details of the investigation, such as the forensic techniques used. Additionally, there was the issue of a breach in regular users' privacy.

[Slide 9: Conclusion]

Speaker: In conclusion, co-regulation is a recommendation to address international cybercrime that is across multiple nations and jurisdictions. It is imperative when

conducting ethical investigations to consider the cultural perspectives of jurisdictions and the handling of digital evidence.

Speaker: Thank you for your time and attention.

[Slide 10: References]

Speaker: Here is the list of references used.

References

Eurojust. (2020) Dismantling of an encrypted network sends shockwaves through organised crime groups across Europe. Available from: https://www.eurojust.europa.eu/news/dismantling-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe [Accessed 14 December 2023].

Eurojust. (2020) 7.2 encrochat: Dismantling of an encrypted network used by criminal groups. Available from: https://www.eurojust.europa.eu/ar2020/7-casework-crime-type/72-encrochat-dismantling-encrypted-network-used-criminal-groups [Accessed 15 December 2023].

Henschke, A., Reed, A., Robbins, S. & Miller, S. (2021) *Counter-Terrorism, Ethics and Technology: Emerging Challenges at the Frontiers of Counter-Terrorism*. Springer Nature.

Levi, M. & Smith, R.G. (2022) Fraud and pandemics. *Journal of Financial Crime* 29(2): 413-432.

SlidesMania. (2023) Free google slides themes and PowerPoint templates. Available from: https://slidesmania.com/ [Accessed 13 December 2023].