Mid-Module Assignment 2: Blog post

This is the second assessment for this module and is used to examine how you explore the challenges and opportunities of regulating and policing cyberspace. This accounts for 20% of your final module mark. Word count 500 words.

Assignment Brief

You have been asked to contribute to an international organisation’s monthly Newsletter. This organisation concerns itself with problems regarding investigation and apprehension of cyberspace criminality. The aim of the Newsletter is to draw awareness and influence policy.

The theme of this month’s Newsletter is ‘Investigating Cybercrime: Problems and Solutions'. You are required to write a blog that focuses on cyber-identify theft in your country (or any other country).

Instructions

To guide your writing, take the following points into consideration, with the applicable grading criteria highlighted for your information (see the Module Resources page for the full grid):

Briefly explain the crime at the start of the blog (Knowledge and Understanding weighted at 30%, Use of relevant sources weighted at 10%), and then, assess only one of the following limitations:

How international regulations might prevent a national effective investigative outcome? (you can focus on human rights legislation (see week 4). For example, how the EU General Data Protection Regulation might have affected the investigative process in your chosen country.

OR

How international and/or national investigative tools and practice might limit an effective national/international investigative outcome.

This can relate to a scenario where the cybercrime affects only your chosen country, or when the cybercrime is committed internationally/transnationally.

If available, in either option you have chosen, identify the costs of this crime and the extent of this affecting effective investigation. (Criticality weighted at 30%, Use of relevant sources weighted at 10%)

Presentation and Structure of your work (weighted at 10%), as well as Academic Integrity (weighted at 10%), includes spelling, style, evidence of proofreading, correct use (and format) of citations and references.

在博客開頭簡要解釋犯罪行為（知識和理解權重為 30%，相關資源的使用權重為 10%），然後僅評估以下限制之一：

國際法規如何阻止國家有效的調查結果？ （您可以關注人權立法（見第 4 週）。例如，歐盟通用數據保護條例可能如何影響您選擇的國家/地區的調查過程。

或

國際和/或國家調查工具和實踐如何限制有效的國家/國際調查結果。這可能與網絡犯罪僅影響您選擇的國家或網絡犯罪發生在國際/跨國的情況有關。

如果可用，在您選擇的任一選項中，確定此犯罪的成本以及影響有效調查的程度。 （重要性權重為 30%，相關資源的使用權重為 10%）

作品的展示和結構（權重為 10%）以及學術誠信（權重為 10%），包括拼寫、風格、校對證據、引文和參考文獻的正確使用（和格式）。

<https://ncsi.ega.ee/country/cn/>

<https://www.cisa.gov/uscert/china>

<https://blog.alixpartners.com/post/102hlnj/what-are-we-facing-when-performing-mobile-forensics-in-china>

Forensic Analysis of Pirated Chinese Shanzhai Mobile Phones

<https://link.springer.com/chapter/10.1007/978-3-642-33962-2_9>

<https://www.unodc.org/documents/Cybercrime/English.pdf>

Mobile evidence

<https://www.unodc.org/e4j/en/cybercrime/module-6/key-issues/handling-of-digital-evidence.html>

<https://techwireasia.com/2019/04/access-to-mobile-and-cloud-data-is-key-to-solving-crimes-faster/>

<https://www.southuniversity.edu/news-and-blogs/2016/08/fighting-crime-with-mobile-technology-137309>

<https://www.unodc.org/e4j/en/cybercrime/module-5/key-issues/obstacles-to-cybercrime-investigations.html>

<https://www.ithome.com.tw/news/143991>

<https://blog.pagefreezer.com/legal-lessons-learned-5-times-digital-evidence-was-denied-in-court>

<https://link.springer.com/article/10.1007/s10609-021-09430-4>

Global leading forensics tool provider “Cellebrite” has exited the China market

Mainstream mobile forensics software fails to stay up to date with Chinese mobile applications

Different Chinese phone manufacturers produce various models of mobile phones

more and more Shanzhai phones are being used by criminals. However, there has been little published research related to Shanzhai phone forensics.

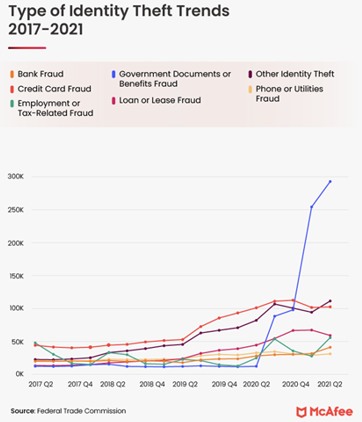
Another is that there is almost no official documentation about the phones, especially regarding flash memory, file systems and other details about how the phones store data.

As with other smartphones, internal flash memory is the major data storage component in Shanzhai phones, but extracting evidence from the flash memory of Shanzhai phones is very challenging because of the variety of phones and the absence of documentation.

Asia & Pacific

Cyber identity theft is the illegal act of obtaining another person's personal information without that person's knowledge or consent with the goal to commit fraud. Identity thieves utilize personal information to masquerade as data subjects and commit fraud, such as accessing bank accounts, getting credit cards, or making transactions to benefit financially immediately. Use social networking accounts to harass and ruin someone's online reputation, commit fraud or deceit, or hide the identities of evildoers (Infosec, 2022).

Identity theft in the U.S. is increasing, according to fraud reports from the 2017 Q1 to the 2021 Q1. Over 500,000 recorded cases of identity theft were reported in the 2021 Q1, a dramatic increase from over 100,000 in the 2017 Q1. Bank fraud, government document fraud, loan or lease fraud, employment or tax-related fraud, and phone or utility fraud were the most often reported types of identity theft in 2021 (McAfee, 2022).



Identity theft could occur in these ways (Terranova Security, 2022):

1. Social engineering using email or phone messages, listening in on private conversations, or retrieving papers out of mailboxes or rubbish bins.
2. Malware that infects a network and installs spyware or keyloggers to collect credentials and other sensitive data
3. Cybercriminals explore social networking sites for personal data, using this data to interact with victims and become familiar with their information to elicit a response.
4. Using a variety of methods to hack systems and databases. from malware or phoney wi-fi access points that provide access to personal data, and fraudulent websites used to steal passwords.

The increasing of identity theft occurs on mobile devices, making it difficult for mobile investigative practices and technologies to produce reliable results for international investigations. Mobile forensics, a novel subset of digital forensics, has gained popularity recently. Since mobile forensics may support the immediate and efficient provision of digital evidence or pertinent data in litigation or investigation-related settings.

For investigative practices in China, some news reported the security forces might confiscate electronic devices without prior notice from the suspects to investigate or modify the electronic records (Shibani, 2021).

The world's leading manufacturer of forensics tools, Cellebrite, left the China market in 2020. Cellebrite presents that only going after clients who they consider would act ethically and not in a way that is at odds with human rights or privacy. Due in part to worries about data security and human rights, Cellebrite highlighted the withdrawal from Bangladesh, Belarus, China, Hong Kong, Macau, Russia, and Venezuela (Cellebrite, 2020).

On the other hand, investigating each model of mobile phone produced by numerous Chinese phone manufacturers is difficult. Furthermore, forensic analysis is made more challenging by the rise in the usage of pirated Chinese "Shanzhai" (knockoff) mobile phones by criminals. Like other smartphones, internal flash storage serves as the primary data storage component in imitation phones. However, there is nearly no official documentation for the phones, particularly with reference to flash memory, file systems, and other information about the way the phones store data. There has also been minimal published study on counterfeit phone forensics, retrieving evidence from the flash storage of knockoff phones is particularly difficult (Junbin et al., 2012).

<https://www.infosec.gov.hk/en/knowledge-centre/identity-theft>

<https://www.mcafee.com/blogs/tips-tricks/a-guide-to-identity-theft-statistics-for-2022/>

<https://terranovasecurity.com/what-is-identity-theft/>

Cellebrite (October 7, 2020) https://cellebrite.com/en/cellebrite-facts/

<https://link.springer.com/chapter/10.1007/978-3-642-33962-2_9>

Shibani Mahtani January 12, 2021 https://www.washingtonpost.com/world/asia\_pacific/hong-kong-national-security-law-internet/2021/01/12/01738064-53b6-11eb-acc5-92d2819a1ccb\_story.html