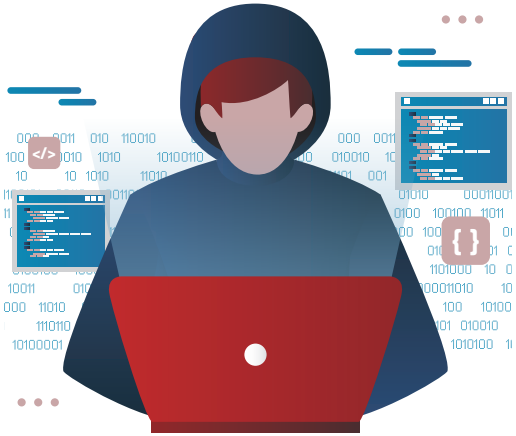
科技罪行
Technology Crime

近年來，香港特別行政區的複雜電腦網絡罪行急劇增加。這些罪行利用日新月異的科技，對市民造成重大傷害和金錢損失，亦對公共安全構成嚴重威脅。此外，與使用數碼證據相關的法律問題也越趨複雜。為應對這些挑戰，分科五除了繼續致力打擊複雜的高科技罪行，特別是涉及加密貨幣、加密貨幣交易平台、暗網、元宇宙等的案件，還在訂立相關法例和提出法律改革建議方面作出貢獻。該分科亦在本地和國際層面，積極加強與執法機構、網絡安全專家及法證專家的合作，以加強防止和偵查罪案的工作。

In recent years, the Hong Kong Special Administrative Region has seen a sharp increase in sophisticated cybercrime that exploits evolving technologies, resulting in substantial harm and financial loss to citizens and posing serious threats to public safety and security. Legal issues relating to the use of digital evidence are also getting more complicated. To address these challenges, Sub-division V continued its commitment to combatting complex high-tech crimes, particularly cases involving cryptocurrencies, cryptocurrency trading platforms, the dark web, the Metaverse and the like. Contributions were made in the drafting of relevant legislation and in making law reform recommendations. Efforts have also been stepped up to strengthen cooperation with law enforcement agencies, cyber experts and forensic experts, locally and internationally, to enhance crime prevention and detection.



制定《保護關鍵基礎設施（電腦系統）條例》（第 653 章）
Enactment of the Protection of Critical Infrastructures (Computer Systems) Ordinance (Cap. 653)

《保護關鍵基礎設施（電腦系統）條例》（第 653 章）於 2025 年 3 月制定，並於 2026 年 1 月 1 日生效，成為香港特區首部全面保障重要數碼系統免受網絡攻擊的網絡安全法律。分科五在該條例的立法過程中提供支援，就該條例所訂刑事罪行和相關事宜提供實質的法律指引。該條例訂立規管框架，旨在提升香港特區關鍵基礎設施電腦系統的安全及復原能力，以及對能源、資訊科技、銀行、運輸、醫療和電訊等界別的指定營運者施加法定責任，規定這些營運者須採取適當措施保護其電腦系統。主要責任包括關於組織架構規定、預防措施（例如安全管理計劃和風險評估），以及事故通報及應對的責任。該條例使香港特區與全球趨勢一致，以可強制執行的規則取代自願性標準，由新設的專員辦公室負責監督指定工作和執行情況。

Enacted in March 2025 and brought into operation on 1 January 2026, the Protection of Critical Infrastructures (Computer Systems) Ordinance (Cap. 653) marks the HKSAR's first comprehensive cybersecurity law to safeguard essential digital systems against cyberattacks. Sub-division V supported the legislative process of the Ordinance and provided substantive legal advice on the criminal offences and related matters under the Ordinance. It establishes a regulatory framework to enhance the security and resilience of the HKSAR's critical infrastructure computer systems, and imposes statutory obligations on designated operators in sectors like energy, IT, banking, transport, healthcare, and telecoms to adopt appropriate measures to protect their computer systems. Key obligations include organizational requirements, preventive measures such as security management plans and risk assessments, and incident reporting and response obligations. It aligns the HKSAR with global trends, shifting from voluntary standards to enforceable rules, with the new Commissioner's Office overseeing designations and enforcement.

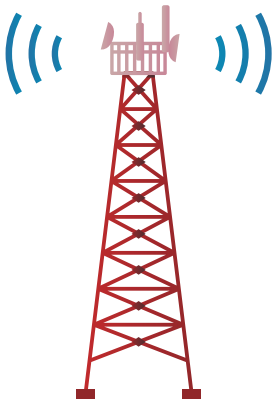
香港法律改革委員會電腦網絡罪行小組委員會
Cybercrime Sub-committee of the Law Reform Commission of Hong Kong

香港法律改革委員會(法改會)在2025年繼續進行相關工作，並在2026年1月9日發表報告書，建議引入全新針對電腦網絡罪行的特定法例，以處理五類依賴電腦網絡的罪行，即非法取覽、截取、干擾數據或系統，以及提供或管有用作干犯該等罪行的工具。這是法改會繼在2022年發出諮詢文件後，就其電腦網絡罪行研究首度發表的報告書。該報告書指出《刑事罪行條例》(第200章)及《電訊條例》(第106章)所訂的現有罪行已不合時宜。電腦網絡罪行小組委員會參考了澳洲、加拿大、英國、中國內地、新西蘭、新加坡及美國的法例後，提出有關建議。分科五的一名代表擔任該小組委員會的成員，積極參與小組委員會的工作。

Following continued effort in 2025, on 9 January 2026, the Law Reform Commission of Hong Kong ("LRC") released a report recommending new bespoke legislation on cybercrime to address five cyber-dependent crimes, namely illegal access, interception, interference with data or systems, and making available or possessing tools for such crimes. The report, the first in the LRC's cybercrime study following a 2022 consultation paper, notes that current offences in the Crimes Ordinance (Cap. 200) and the Telecommunications Ordinance (Cap. 106) are outdated. The Cybercrime Sub-committee reviewed laws in Australia, Canada, the UK, the Chinese Mainland, New Zealand, Singapore, and the US in making the recommendations. A representative of Sub-division V actively participated in the Sub-committee as a member.

下文載述該分科在2025年處理的一些值得關注的案件。
Some notable cases handled by the Sub-division in 2025 are highlighted below.

1



香港特別行政區 訴 蘇華諺 [2025] ESCC 452案是本港首宗涉及偽基站的案件。2025年2月，安裝在一輛GoGoVan貨車上的偽基站發出懷疑詐騙短訊。該短訊具有以"#"號開頭的發送人名稱，內含釣魚網站連結。操作人(即被告)於2025年2月17日被捕，當時他正利用手提電話操控該偽基站，向附近的手提電話發送虛假的"#ALIPAY"訊息。被告承認"串謀詐騙"罪及"無牌管有或使用無線電通訊器具"罪，於2025年12月9日被判處監禁合共15個月。裁判官在判刑時指出，本案是本港首宗涉及偽基站的案件，並指出利用科技進行詐騙，犯案容易，無須面對面接觸，受害人難以察覺或追討損失。此類案件的嚴重程度不低於街頭騙案或電話詐騙，必須判處嚴厲和具阻嚇性的刑罰。

HKSAR v So Wai-yin [2025] ESCC 452 was the first local case involving a pseudo base station ("PBS"). In February 2025, suspected fraudulent SMS messages with "#" sender IDs linked to phishing sites were sent via a PBS mounted in a GoGoVan. The defendant operator was arrested on 17 February 2025 with a mobile phone controlling the PBS, which broadcast fake "#ALIPAY" messages to nearby mobile phones. The defendant pleaded guilty to "conspiracy to defraud" and "unlicensed possession or use of radiocommunication apparatus". On 9 December 2025, he was sentenced to a total of 15 months' imprisonment. In sentencing, the magistrate remarked that this was the first local case involving a PBS, and that technology-based frauds are easy to perpetrate, involve no face-to-face contact, and make detection or recovery of losses difficult. Their seriousness is no less than that of street scams or telephone frauds. A severe and deterrent sentence was warranted.

2

在***香港特別行政區 訴 繆招興及另二人*** [2025] HKDC 680 案中，三名被告使用電話卡及電話數據機發送釣魚短訊，冒充某合法速遞公司，誘騙受害人提供信用卡資料支付虛假的手續費。被盜取的信用卡憑證其後被用於進行未經授權的購物交易。三名被告犯案時年僅 17 至 18 歲，共同被控一項 " 串謀詐騙 " 罪，全部認罪並罪名成立。法庭指第一被告及第二被告如非犯案時年少和各自具有可獲減刑的酌情因素，適用的量刑起點應分別為監禁三年及三年半。第三被告在串謀中擔當較重要的角色，被判處監禁兩年四個月。

In ***HKSAR v Mio Chiu-hing and 2 others*** [2025] HKDC 680, the three defendants used SIM cards and a modem pool to send phishing SMS messages mimicking a legitimate courier company. Victims were tricked into providing credit card details to pay a fake handling fee. The stolen credentials were then exploited to make unauthorised purchases. The defendants, aged only between 17 and 18 at the time of the offence, were jointly charged with and convicted of one count of "conspiracy to defraud" upon their guilty pleas. The Court remarked that the respective proper starting point for D1 and D2 would have been three years' and three and a half years' imprisonment but for their young age and individual mitigating circumstances. D3, who played a more serious role in the conspiracy, was sentenced to two years and four months' imprisonment.

3

香港特別行政區 訴 楊尚樺 [2025] HKCA 735 是一宗就一項 " 煽惑他人有意圖而傷人 " 的定罪提出的上訴許可申請。申請人於網上討論區帖文下發表回應 (屬公開性質)，煽惑讀者襲擊及殺害警務人員，經審訊後罪成，被判處監禁 13 個月。申請人辯稱原審法官把某些材料接納為證據是錯誤的。這些材料包括申請人的其他帖文、顯示申請人手提電話屏幕正在瀏覽該網上討論區的照片，以及顯示申請人對該討論區具有認知及熟悉程度的錄影會面片段。上訴法庭認為這些材料與案中爭議點有關聯，裁定把它們接納為證據實屬恰當。上訴法庭亦裁定該則回應確構成非法煽惑，遂拒絕就定罪批出上訴許可。

HKSAR v Yeung Sheung-wa [2025] HKCA 735 was an application for leave to appeal against a conviction of "incitement to wound with intent". The applicant, who was convicted after trial and sentenced to 13 months' imprisonment, made a single comment on a publicly accessible online forum inciting readers to attack and kill police officers. The applicant argued that the trial judge erred in admitting into evidence his other posts, photographs of his mobile phone showing the online forum, and parts of the applicant's video-recorded interviews in which he demonstrated his knowledge and familiarity with the said forum. Finding that these materials were relevant to the issues in dispute, the Court of Appeal held that they were properly admitted into evidence, and that the comment amounted to unlawful incitement. Leave to appeal against conviction was refused.