社評雙語道

港立網絡罪行專法 可升數碼安全

原文

摘錄自1月10日香港《文匯報》：香港法律改革委員會昨日發表《依賴電腦網絡的罪行及司法管轄權事宜》報告書，建議引入一項全新針對電腦網絡罪行的特定法例，涵蓋五類依賴電腦網絡的罪行，最高可判處終身監禁。報告書的建議不僅是對現行散落於《刑事罪行條例》等條文的系統性革新，更是香港主動應對數碼時代犯罪挑戰、保障社會治安的重要法律進程，是維護網絡空間清朗、保障市民及企業機構利益、維護國家安全的重要舉措。

特區政府應盡快展開研究跟進落實，並應就人工智能罪行進行前瞻性研究和推動立法，為香港的長治久安與數碼發展築牢法治屏障。

電腦網絡犯罪在香港時有發生，如在2023年8月，有勒索軟件組織對數碼港的電腦系統進行黑客入侵及勒索，大量個人資料外洩，其後在暗網被公開，當中包括銀行賬戶資料、身份證號碼及職員證資料。

然而，本港一直沒有專屬法例處理，檢控只可使用《刑事罪行條例》的「刑事毀壞」「不誠實使用電腦」等。在資訊科技日新月異的今天，傳統法律框架在應對黑客入侵、數據竊取、勒索軟件攻擊等新型犯罪時往往力不從心。

法改會的立法建議展現了香港法律體系與時俱進，有助形成更安全可靠的電腦網絡環境。報告書明確劃分的五類罪行，構建了一個層次分明、覆蓋全面的追究罪責法律體系。

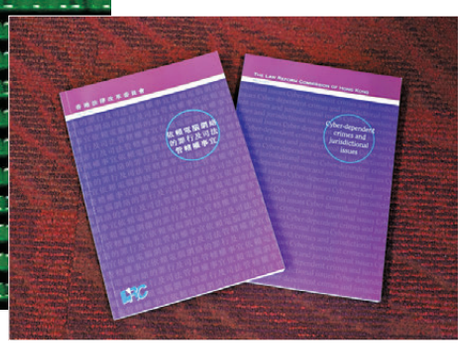
例如，提出將「純粹未獲授權取覽」行為入罪，並設立「意圖進行其他犯罪」的加重罪行，讓執法機關在黑客攻擊的早期階段即可介入，防止後續更嚴重的罪行發生，體現了「預防為先」的治理思維。

立法建議具備強烈的現實針對性與保護效能。在數碼時代，公眾個人隱私、企業商業秘密乃至機構關鍵基礎設施的良好順暢運行，均繫於網絡空間的安全性。報告書建議將非法截取數據罪的保護範圍擴展至「所有通訊」及「元數據」，並引入域外司法管轄權條款，確保只要犯罪行為或結果涉及香港，或受害人身處香港，香港法庭即有權審理。

這意味着，無論是本地機構遭遇跨境數據竊取，還是市民在社交媒體的通訊遭境外不法分子截取，都能得到香港法律的強力保護。這極大增強了法律對潛在犯罪者的威懾力，也為受害者提供了更堅實的支援途徑。

尤為重要的是，立法建議也與維護國家安全的大局要求高度契合。報告書明確指出，干擾關鍵資訊基礎設施（如機場控制塔、鐵路信號系統）的行為，最高可處終身監禁，而且此類罪行可能同時觸犯香港國安法及《維護國家安全條例》中關於破壞活動的條款。

◀電腦網絡犯罪在香港時有發生，然而本港一直沒有專屬法例處理。 資料圖片



▼《依賴電腦網絡的罪行及司法管轄權事宜》報告書，建議引入針對電腦網絡罪行的特定法例。 資料圖片

這將在網絡安全領域織密國家安全的防護網，使任何意圖透過網絡攻擊癱瘓社會運作、危害公共安全的行為，都將面臨法律的嚴厲懲處。

報告書在建議從嚴治罪的同時，亦為合法使用與犯罪行為定下明確界線，避免「一刀切」對科技創新與正常業務運作造成誤傷。立法建議為「白帽黑客」等網絡安全從業員設定了在合規前提下進行安全測試的免責辯護，亦為教育科研、互聯網服務提供者設定了合理的責任豁免空間。這種既嚴格打擊惡意犯罪，又保護合法專業活動的立法思路，有利於營造一個既安全又充滿活力的數碼生態環境，促進香港國際創新科技中心的建設。

Enacting Bespoke Cybercrime Legislation to Enhance Hong Kong's Digital and Technological Security

譯文

The Law Reform Commission of Hong Kong yesterday published a report on Cyber-Dependent Crime and Jurisdictional Issues, recommending the introduction of a new piece of bespoke legislation on cybercrime to cover five types of cyber-dependent crimes, with the maximum penalty being life imprisonment. The recommendations in the report are not merely a systematic overhaul of existing provisions currently scattered across ordinances like the Crimes Ordinance; they represent a significant legal step forward for Hong Kong to proactively address the challenges of crime in the digital age and safeguard public order. This initiative is crucial for maintaining a clean cyberspace, protecting the interests of citizens and corporate entities, and preserving national security. The Government should expedite research and follow up on the implementation of these proposals, while also conducting forward-looking research and promoting legislation concerning artificial intelligence crimes, thereby fortifying the rule of law as a bulwark for Hong Kong's long-term stability and digital development.

Cybercrime incidents occur from time to time in Hong Kong. For example, in August 2023, a ransomware group hacked and extorted the computer systems of Cyberport, resulting in a massive data breach where large quantities of personal data—including bank account details, ID numbers, and staff ID information—were subsequently published on the dark web. However, Hong Kong has long lacked dedicated legislation to deal with such incidents; prosecutions can only rely on offences such as "criminal damage" and "access to a computer with dishonest intent" under the Crimes Ordinance. In a world where information technology evolves rapidly, the traditional legal framework is often inadequate for tackling new forms of crime such as hacking, data theft, and ransomware attacks.

The Commission's legislative recommendations demonstrate that Hong Kong's legal system is keeping pace with the times, helping to create a safer and more reliable cyber environment. The five clearly defined categories of offences in the report form a structured and comprehensive legal framework for determining criminal liability. For instance, the report recommends that "unauthorised access to programme or data without lawful authority should be a summary offence" and that "an aggravated form of the offence arises if the unauthorised access is accompanied by an intent to carry out further criminal activity." This allows law-enforcement agencies to intervene at early stages of hacking activities to prevent more serious offences from occurring, reflecting a "prevention-first" governance mindset.

The legislative recommendations possess a strong practical relevance and protective efficacy. In the digital age, the protection of personal privacy, corporate commercial secrets, and even the smooth operation of critical institutional infrastructure all depend on the security of cyberspace. The report recommends extending the scope of protection for the offence of unlawful interception of data to cover "all communications" and "metadata," and introduces provisions for extraterritorial jurisdiction. This ensures that Hong Kong courts have the power to hear cases as long as the criminal act or consequence involves Hong Kong, or the victim is located within Hong Kong. This means that whether a local institution encounters cross-border data theft, or a resident's social media communications are intercepted by offenders abroad, they can rely on the robust protection of Hong Kong law. This greatly enhances the deterrent effect on potential criminals and provides more solid support channels for victims.

Crucially, the proposed legislation also aligns with the overarching requirements for safeguarding national security. The report explicitly states that acts of interfering with critical information infrastructure—such as airport control towers or railway signalling systems—could carry a maximum penalty of life imprisonment. Furthermore, such acts may simultaneously contravene provisions on sabotage in both the Hong Kong National Security Law and the Safeguarding National Security Ordinance. This would strengthen the national security protection network within the realm of cybersecurity, ensuring that any attempt to paralyse social operations or endanger public safety through cyberattacks faces severe legal consequences.

While recommending stringent measures against offences, the report also draws clear boundaries between lawful activities and criminal conduct, preventing "one-size-fits-all" outcomes that could inadvertently hinder technological innovation or normal business operations. The report recommends providing a defence of exemption for cybersecurity professionals such as "white-hat hackers", allowing them to conduct security testing under compliant conditions. Reasonable liability exemptions are also proposed for educational and research institutions, as well as internet service providers. This legislative approach—strictly combating malicious crime while protecting legitimate professional activities—helps foster a digital ecosystem that is both secure and vibrant, supporting Hong Kong's development as an international innovation and technology centre.

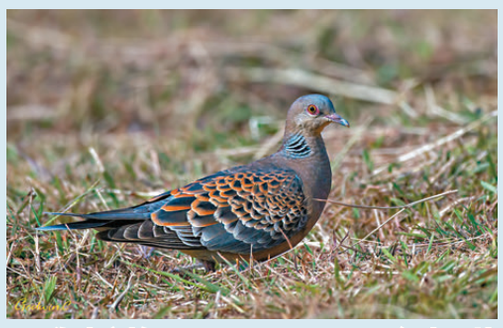
●Tiffany

《詩》中鳥寄情長 鳩鳧雁訴離合

恒大清思

承接去年年末筆者所分享的《詩經》「鳥意象」一文，今天在此欄再與大家一起續賞「《詩》中鳥」的魅力。《詩三百》不乏以鳥類詠唱愛情的作品，除了上篇文章曾提及的「鳩」及「鵲」外，尚有其他詩篇同以鳥類比興愛情的悲歡離合。

率先登場的依然是「鳩」，然而今次所指有別於上文，此處之「鳩」實乃「山斑鳩」。《衛風．氓》謂「桑之未落，其葉沃若。于嗟鳩兮，無食桑葚。于嗟女兮，無與士耽。士之耽兮，猶可說也。女之耽兮，不可說也。」作者對自己被拋棄的命運感懷身世，藉詩歌忠告天下女子勿沉溺於愛情而不能自拔，故以「桑樹」繁茂之時喻女子的青春，而「鳩」食「葚果」則比作女子青春被負心漢浪費。據考證，「山斑鳩」果真喜棲於桑，並食其葚果，因此本詩以「鳩」起興，正合詩旨。



●圖為山斑鳩。 網上圖片

●圖為綠頭鴨。 網上圖片

不過，愛情之所以能成為古今中外永恒歌詠之題材，或許在於其甜蜜一面仍然令人無限憧憬。《邶風．匏有苦葉》一詩的作者便於水岸邊向意中人詠唱詩歌，表達急不及待欲與其成親的心意。

詩中提到「雝雝鳴雁，旭日始旦。士如歸妻，迨冰未泮。」開端以「雁」鳴起興，與「旭日」初升形成和樂景致，繼而呼喚情人趁冬冰未融解前娶作者過門。據悉古時適婚男女多於秋冬季節或開春堅冰未融化之前舉行嫁娶儀式，有說與正值農閒時節相關，正如《荀子》有言「霜降逆女，冰泮殺內」，《孔子家語》亦云「霜降而婦功成，嫁娶者行焉。冰泮而農桑起，婚禮而殺於此。」推而論之，寒冬春暖交替之際，正逢候鳥「雁」醒覺遷徙回航之時，便明詩中作者以「雁」起興之由。

「弋鳧與雁」反映家庭和睦

「雁」也曾出現於另一首洋溢新婚幸福的詩篇當中。《鄭風．女曰雞鳴》詩中「將翱將翔，弋鳧與雁」一句，借用形容鳥飛的「翱翔」動作，比喻丈夫出外遊逛，不忘途中打獵捕捉「鳧」和「雁」回家，反映家庭和睦的一面。

「鳧」即今人所謂「野鴨」，當中以「綠頭鴨」最為常見。研究者表示，「綠頭鴨」乃我國早期的「家鴨」，早於戰國時期已被古人馴化養殖，同時亦為狩獵對象，很可能便是詩中所言之「鳧」。

可惜即使有情人終成眷屬，世事又豈能盡如人意？《邶風．雄雉》詩中的思婦便以「雄雉」單飛起興，比興丈夫離家遠行、久久不還之嘆。該詩首二章云「雄雉于飛，泄泄其羽。我之懷矣，自詒伊阻」「雄雉于飛，下上其音。展矣君子，實勞我心」，其所展現的「賦比興」手法可謂質樸自然、渾然天成，讓人真切地感受到思婦內心之纏綿悱惻。

●歐亦修博士
香港恒生大學中文系講師
香港恒生大學 THE HANG SENG UNIVERSITY OF HONG KONG

溯英文詞源 探文化交流痕跡

貼地英文

當一個強權取得另一方領土時，新統治者必然將其語言定為官方及主導語言，原有語言最終難免被取代或逐漸式微。其結果通常不外乎三種可能：**一是**原有語言在歷史中被抹去；**二是**兩種語言並存，經歷有限度的交融；**三是**兩種語言高度結合，形成一種新的語言。

以英格蘭為首、說英語的白人，從東岸十三殖民地到美國建國後數十年間，與原住民（Native Americans）的融合相當有限。原住民即昔日所謂的「紅印第安人」（Red Indians），同時也包括阿拉斯加的愛斯基摩人（Eskimos）和夏威夷的土著毛利人（Kanaka Maoli）。

如上一學年所述，部分原住民以山河特徵命名的地名，因白人沿用已成習慣，便直接以羅馬字母拼寫保留，例如 Mississippi（密西西比河）、Michigan（密歇根湖）、Ohio（俄亥俄河）和 Massachusetts（麻薩諸塞州）等——密西西比意為「大河」，密歇根指「大湖」，俄亥俄是「好水」，麻薩諸塞則為「大藍山」，這些名稱本身皆富有意境。

此外，許多歐洲人須向原住民請教的新事物，其名稱也直接取自原住民語言，如：raccoon（浣熊）、moose（駝鹿）、coyote（土狼）、pecan（山核桃）、tomahawk（戰斧）、canoe（獨木舟）、tobacco（煙草）、cigar（雪茄）、igloo（冰屋）、husky（哈士奇）和 avocado（牛油果）。也有一些詞彙是通過其他歐洲語言轉介進入英語，例如 tomato 經由西班牙語中轉，而原住民的「莫卡辛鞋」（moccasin）則是法國人比英國人更早接觸並引入。

現代白人某程度上「追認」了原住民的地位，將一些產品冠以原住民相關的名稱，例如自由軟件組織 Apache（阿帕奇），以及汽車 Jeep Grand Cherokee（吉普大切諾基）等。然而，白人過去對原住民的蔑視，如今欲加補償，卻不免令人感到「太少、也太遲」（too little, too late）。

化敵為友語言和

在七年戰爭期間，美國尚未立國，仍聽命於倫敦，曾與法國為敵；然而到了獨立戰爭時，法國卻成為盟友。其後拿破崙因急需資金，而美國正想向西部擴張，雙方各有所需，美國便從法國手中買下了整個路易斯安那地區。

在此和諧氛圍下，法語與英語得以相互交流。路易斯安那州法裔移民後代卡津人（Cajun）所使用的區域性語言「卡津英語」（Cajun English），在全美範圍內的影響，可能連許多美國說英語者亦不自覺。

例如 lieutenant（中尉）一詞，便是由法國傳入英語世界的軍階名稱，其英式與美式發音分別為 /lɛfˈtɛnənt/ 與/luːˈtɛnənt/——簡單來說，英式讀音首音似"left"，而美式讀音則接近粵語的「廖」。這類詞彙同樣來自法語，但英國的 lieutenant 可能源於諾曼法語（Norman French），而美國接觸的已是現代法語。隨着美國文化仰望的對象從英國轉向法國，更多詞彙由此渠道引入英語，除軍階外，還有如 rendezvous（約會）、sovereignty（主權）、fraternity（博愛）、laissez-faire（自由放任）、passport（護照）等。

美國立國百餘年後，加州為紀念獨立戰爭期間曾援助美軍的法國將軍拉法葉（Lafayette），將一座城市命名為拉法葉。如今緬因州雖禁止在學校教授法語，但與其接壤的加拿大新不倫瑞克省（New Brunswick）居民卻多操法語——語言交流本身，實不應帶有歧視。

●康源 專業英語導師

單詞卡

raccoon	浣熊	tobacco	煙草
moose	駝鹿	cigar	雪茄
coyote	土狼	igloo	冰屋
dock	碼頭	rendezvous	約會
pecan	山核桃	sovereignty	主權
tomahawk	戰斧	fraternity	博愛
canoe	獨木舟	laissez-faire	自由放任