為全運會及立法會選舉護航

網安攻防演練對戰60小時

為提升政府部門和公共機構識別和應對網絡攻擊的技術、經驗及整體防禦能力，數字政策辦公室昨日（10日）起舉行為期三天的「香港網絡安全攻防演練—以攻築防2025」，也為即將舉行的第十五屆全國運動會及立法會換屆選舉作好網安準備。攻防演練為期三日兩夜，共60小時，將於10月12日（星期日）晚上11時完結。

大公報記者 陳劍

▲數字政策辦公室昨日起舉行為期三天的「香港網絡安全攻防演練——以攻築防2025」。

創新科技及工業局局長孫東在活動開幕典禮上致辭表示，安全穩定的網絡環境是社會、經濟發展的重要保障，更是建設智慧城市及發展數字經濟的先決條件。他強調，隨着數字化時代的發展，當局更要加強網絡安全防範意識，以應對層出不窮的網絡挑戰和威脅。

孫東：知己知彼 方能掌控全局

孫東表示，數字政策辦公室去年舉辦首屆「香港網絡安全攻防演練」，通過「實兵」、「實網」、「實戰」方式，全方位對參與政府部門和公共機構的安全防護能力進行深度檢驗並提供反饋，達至以攻築防的效果，全面提升香港網絡安全防護及韌性。今年數字辦再接再厲，整體演練規模進一步擴大，涵蓋更多的公共服務，也正好為即將舉行的第十五屆全國運動會及立法會換屆選舉做好網絡安全的準備。

孫東將攻防演練比喻為兵法實戰，唯有知己之漏洞，知彼之攻勢，方能掌控全局，確保安全無虞。他說，期望藉着這次演練，能讓各部門和公共機構時刻警惕網絡安全對公共事業帶來的憂患，同時把握這次機會進行深度檢驗，堵塞潛在網安漏洞，防患未然。

孫東感謝數字辦及這次攻防演練的協辦單位，強調「網絡安全為人民，網絡安全靠人民」，維護網絡安全需要全社會的共同努力。

廣東網信辦派頂尖隊伍參加

今年的攻防演練繼續獲各方積極響應，參與的政府部門和公共機構大幅增加，負責防守的「藍隊」共有34隊，包括25個政府部門及九間公共機構；而負責攻擊的「紅隊」亦大幅增加至15隊，當中包括多支經驗豐富的網絡安全機構、專上學院，以及由廣東省網信辦推薦的三支頂尖攻擊隊伍，充分體現粵港兩地在網絡安全和資訊保安教育上交流合作。

除了紅藍兩隊外，數字辦還邀請多家具豐富攻防演練經驗的網安機構，包括香港網絡安全專業協會的多個成員，提供技術支援和專家意見，確保演練順利進行。此外，有60多個政府部門及公共機構以觀察員身份參與演練。數字辦表示，希望透過實戰，提升各單位抵禦實際網絡攻擊的水平，同時進一步完善應急指揮機制及增強應變能力。

活動由數字政策辦公室統籌主辦，香港警務處網絡安全及科技罪案調查科、香港互聯網註冊管理有限公司、數碼港及香港資訊科技學院協辦，邀請不同政府部門和公共機構參與。

▲孫東（左五）表示，安全穩定的網絡環境是社會、經濟發展的重要保障。

AI「換臉」製假證開戶借貸 警拘22人

【大公報訊】記者秦英偉報道：警方揭發有詐騙集團成功利用人工智能（AI）技術，將報失的身份證「改頭換臉」，多次騙過網上銀行驗證，成功開戶及申請借貸和信用卡，然後將犯罪得益轉賬至傀儡戶口。由2024年10月至2025年9月期間，這些傀儡戶口曾經清洗的黑錢合共超過港幣1.9億元。警方表示行動仍在進行，正繼續追查相關傀儡戶口資金流向；警方亦已將案情通知監管部門及金融機構，建議提升保安措施，並呼籲市民保護好個人資料。

傀儡戶口洗黑錢1.9億

港島總區刑事部於前日及昨日（10月9及10日）展開「銀殿」行動，瓦解一個本地詐騙集團，拘捕16男6女（19歲至76歲），包括主腦、骨幹及傀儡戶口持有人，他們報稱的職業為無業、家庭主婦、學生、退休人士等，其中部分人有三合會背景。

警方發現，該詐騙集團在2024年9月至2025年4月期間，多次利用AI技術修改報失身份證，包括以人工智能換臉技術，換走已報失身份證上的圖像，再上載騙徒自拍照片，企圖攻破網上銀行或支付工具的驗證程序。

遞交23次申請 19次成功

該詐騙集團總共向7間銀行及儲值支付工具，遞交合共23次網上開戶申請，其中19次成功通過身份驗證程序並開設戶口。集團隨即利用這些戶口申請借貸及信用卡，將犯罪得益轉賬至18個傀儡戶口。

警方亦發現這些戶口同時涉及最少14宗本地詐騙案，案件類別包括電話騙案、投資騙案及網上購物騙案等，損失金額共達港幣168萬元，個別案件騙款由港幣1600元至港幣76萬元不等。

警方提醒市民必須時刻提高警覺，保護好個人資料，亦不要向第三者透露個人資料，以免被不法分子有機可乘。根據香港法例第455章《有組織及嚴重罪行條例》，清洗黑錢罪最高可被判處罰款500萬元及監禁14年。警方亦會與律政司就適當案件向法庭申請加刑，並積極研究就清洗黑錢罪行加快檢控程序。

◀有詐騙集團成功利用AI技術，將報失的身份證「改頭換臉」，多次騙過網上銀行驗證，成功開戶及申請借貸和信用卡，並將犯罪得益轉賬至傀儡戶口。圖為警方檢獲的證物。

警方虛擬資產情報工作組 助打擊科技金融犯罪

◀警務處昨日成立「虛擬資產情報工作組」。大公文匯全媒體記者麥鈞傑攝

【大公報訊】記者李清報道：本港今年首8個月共錄得1463宗虛擬資產相關案件，其中15宗針對Web3業界機構的黑客入侵案件導致約9.9億元損失。香港警務處昨日成立「虛擬資產情報工作組」（VAIT），並舉辦「Web3情報與執法高峰論壇」，匯聚金融監管機構、執法部門、學術界及逾60間金融與虛擬資產服務機構的代表，共同探討合作策略。

周一鳴：強化公私營協作

「虛擬資產情報工作組」由警務處牽頭，聯合執法部門（警務處及海關）、金融監管機構（金管局及證監會）及持牌虛擬資產服務提供者，構建公私營協作平台，旨在促進跨部門情報共享與行動協作，提升對相關罪行及網絡安全威脅的偵測與防範能力。

警務處處長周一鳴在開幕致辭中指出，今年首8個月共錄得1463宗虛擬資產相關案件，包括騙案、網上勒索、盜用電腦、洗黑錢及盜竊等。其中，15宗針對Web3業界機構的黑客入侵案件，導致約9.9億港元損失，受害機構涵蓋交易所、投資機構及去中心化項目。

周一鳴強調，Web3技術帶來機遇的同時，也帶來了前所未有的執法挑戰。警隊必須主動應對，確保創新科技不被罪犯濫用。在「智慧警察」策略方針下，警務處自主研發一站式虛擬資產分析工具「Crypto Trace系統」，利用區塊鏈技術追蹤透過虛擬資產洗黑錢的犯罪收益，該系統更在日內瓦國際發明展上獲獎。

提升網安威脅防範能力

除技術工具外，警務處亦注重專業團隊建設與跨界協作。網絡安全及科技罪案調查科已設立「虛擬資產調查專隊」，由懂技術、通警務的專業人員統籌案件調查，並與本地及海外數字資產服務提供者建立緊密合作關係。自2022年起，警務處成立「科技罪案警證顧問小組」，重點探討Web3生態及區塊鏈技術對警證的影響。周一鳴表示，VAIT將透過情報互通與協作機制，強化公私營協作網絡，提升對虛擬資產罪行及網絡安全威脅的應對能力。

保安局副局長卓孝業強調，安全、合規與科技創新並非二選一，需透過監管、業界與執法三方協同，結合監管清晰度、業界自主與執法效能，保障投資者與市場誠信。

在「高管對話」環節，VAIT主席、網絡安全及科技罪案調查科總警司林焯豪表示，要恆常化情報交流機制，增強安全預警，強化止付能力，在預防和教育兩方面下功夫。海關副關長（管制及執法）胡偉軍提示要增強危機意識。證監會中介機構部執行董事葉志衡表示，要增強學習能力，才能在打擊犯罪層面與時俱進。金管局助理總裁（法規及打擊清洗黑錢）陳景宏說，目前對虛擬資產交易平台的發牌較為謹慎，牌照持有人需做身份認證程序。他另外提示，反洗錢在全球都是新興發展的事物，國際標準不是標準答案，要不斷增進香港標準，進而積極影響國際機制。

醫院及口岸爆炸案 三被告罪成月底判刑

【大公報訊】記者程進報道：2020年明愛醫院及羅湖口岸爆炸案，以及計劃在將軍澳引爆一個「墓碑」形炸彈案，八名涉案男女被捕，否認全部控罪。其中三人被裁定串謀導致爆炸罪罪成，昨日在高等法院求情，法官陳仲衡將案押後至本月27日判刑，其間3名被告須繼續還押。

由2男7女組成的陪審團早前以8比1裁定三名被告何卓為、李嘉濱和張家俊在反恐條例下，屬於交替控罪的串謀導致爆炸罪罪成，而串謀犯對訂明標的之爆炸罪罪名不成立。

控方陳詞指出，他清楚知道其住所內的爆炸品，是用作威脅特區政府關閉與內地的邊境，認為可用作考慮被告是否對社會有潛在危險，並可視為加刑因素。辯方求情時指，由10多份親友撰寫的求情信，反映出被告平時的操行，與心理專家報告不同，但法官陳仲衡則表示，雖然欠缺悔意非加刑因素，但這關乎到重犯機會及對社會有否潛在危險。

本案涉及2020年1月27日的明愛醫院急症室廁所爆炸案、同年2月2日羅湖港鐵站月台爆炸案，Telegram頻道「九十二籤」事後承認責任。控方亦指控各被告策劃於同年3月8日在將軍澳尚德邨停車場外，引爆一個「墓碑」形的炸彈。

黑暴期間毒打便衣警 四人被索償19.7萬

【大公報訊】記者陳劍報道：有便衣警員在2019年10月於將軍澳黑暴中被「私了」，涉案四人劉文全、吳婉菁、黃竣賢認罪，雷藝佳則於審訊後被裁定罪成，分別被判囚及入教導所。律政司司長前日（9日）入稟區域法院，指按警務處處長指示，就一名政府僱員因公受傷的僱員補償款項，向4人索償逾19.7萬元，以及有關利息及訟費等賠償。

原告人為律政司司長，4名被告分別為劉文全、吳婉菁、雷藝佳及黃竣賢。

入稟狀指，本案由原告律政司司長代表政府，按警務處處長的指示，根據《官方法律程序條例》等條例，向4名被告申索一名政府僱員因公受傷的僱員補償款項，共計197509.42元，以及有關利息及訟費等賠償。

翻查資料，2019年10月13日，在將軍澳有便衣警被暴徒「私了」。該便衣警當日三度被暴徒包圍，其間曾被不明的尖銳硬物猛烈襲擊，造成其面部及四肢等多處受傷，以及鼻骨骨折等。4名被告其後就非法禁錮、傷人及暴動等罪，被判囚及入教導所。

網絡安全無死角

透視鏡 蔡樹文

「香港網絡安全攻防演練——以攻築防2025」昨日舉行開幕典禮。今年整體演練規模較去年進一步擴大，涵蓋更多的公共服務。

全運會及立法會選舉，是今年底香港的大事。樹欲靜而風不息，每每有重要活動舉行時，總會有個別躲在暗角的不法分子，唯恐天下不亂，趁機製造事端，擴大所謂的影響力。

與境內不法分子比較，境外網絡不法分子來自各地，會用更多不同手法策劃陰謀，常見是透過竊取網上資料，癱瘓政府及公共服務網絡運作，製造惡性事件，達到不可告人目的。特區政府擴大網絡安全攻防演練，是為應付可能發生的網絡違法行為作充分準備。

網絡戰是一場攻防戰，在進攻與防守之間，關鍵在於做好各種緊急應變預案。別以為黑客只會進攻電腦網絡，環顧外國經驗，電力供應系統、公共交通系統都會成為黑客攻擊對象，一旦電力系統及公共交通系統被黑客入侵，對民生造成的影響難以估計。