立法會
Legislative Council

立法會CB(2)930/2024(04)文件

檔號：CB2/PL/SE

保安事務委員會

2024年7月2日的會議

關於加強保護關鍵基礎設施網絡安全的背景資料簡介

目的

本文件就政府當局為關鍵基礎設施營運者的網絡安全責任立法的相關事宜提供背景資料，並概述議員曾就此課題進行的討論。

背景

2. 網絡安全是國家主席習近平提出的**總體國家安全觀下的20個安全重點領域之一**。政府當局表示，網絡安全是指通過採取必要措施，防範對網絡的攻擊、侵入、干擾、破壞和非法使用以及意外事故，從而確保網絡處於穩定可靠的運行狀態，以及保障網絡數據的完整性、保密性、可用性的能力。內地已於2016年訂立《中華人民共和國網絡安全法》。

保障香港網絡安全

3. 網絡安全風險無處不在，有見及此，政府當局一直致力提升公私營機構的能力，保障它們的系統，並提升網絡系統和數據的安全，以抵禦網絡攻擊。然而，網絡安全事故的數目連年上升，在2023年6月至2024年5月期間，香港網絡安全事故協調中心[1]共接獲9 017宗網絡保安事故通報。在政府資訊系統及數

---

1 香港生產力促進局轄下的香港網絡安全事故協調中心實行中央統籌，收集本地企業及互聯網用戶就電腦及網絡安全事故提交的資料，並協助作出應變。該協調中心亦收集和發布有關資訊保安的信息，並就防範相關威脅的措施提供意見。

據方面，政府當局已就數據保安風險管理採取多重保安措施和工作機制，涵蓋數據保護、審計及風險評估、事故處理及應變、教育培訓等方面。政府當局於2000年4月成立資訊保安管理委員會，核心成員包括政府資訊科技總監辦公室("資科辦")及保安局的代表，以監督整個政府內部的資訊科技保安。[2]

保障香港關鍵基礎設施安全

4. 香港警務處("警方")於2011年成立重要基礎設施保安協調中心，負責保障關鍵基礎設施的實體安全。該協調中心旨在透過公私營機構合作，增強香港關鍵基礎設施的自我保護能力。與此同時，為保障政府部門、銀行及金融、運輸業、通訊及公用事業等界別的關鍵基礎設施免受網絡罪行[3]所害，警方的網絡安全及科技罪案調查科轄下的網絡安全中心會適時進行網絡威脅的審計及分析，以防止及偵查針對關鍵基礎設施的網絡攻擊。重要基礎設施保安協調中心和網絡安全中心均為本港的關鍵基礎設施提供24小時支援。

議員的意見及關注

保護香港的重要設施和基礎設施

5. 議員提及針對海外重要基建設施的網絡攻擊，並要求政府當局闡述**警方為確保關鍵基礎設施的安全而進行的工作**，特別是警方進行有關演習的目標及參與演習的部門。政府當局表示，警方的網絡安全及科技罪案調查科一直透過與不同界別的關鍵基礎設施營運者密切合作，提升其面對網絡安全事故及網絡攻擊的應變能力。當局所進行的工作包括與關鍵基礎設施營運者舉行網絡安全演習，以加強警方與關鍵基礎設施營運者在網絡安全領域的合作，以及分享有關網絡威脅的資訊與相關

---

2 委員會定期舉行會議，以：(a)檢視和批核政府資訊科技保安相關規例、政策和指引的修訂；(b)界定與資訊科技保安有關的具體角色和職責；及(c)透過資訊科技保安工作小組(即委員會的執行機構)，就執行資訊科技保安相關規例、政策和指引，向各政策局/政府部門提供指引和協助。

3 根據警方資料，現行法例下與網絡世界行為有關的部分罪行包括：(a)《電訊條例》(第106章)第27A條禁止藉電訊而在未獲授權下取用電腦資料；及(b)《刑事罪行條例》(第200章)第60及161條分別禁止摧毀或損壞財產，以及有犯罪或不誠實意圖而取用電腦。

預防和應變行動，以提升各關鍵基礎設施營運者對網絡攻擊的防備意識和整體防禦能力。

6. 議員要求**政府當局闡釋，就訂定關鍵基礎設施營運者的網絡安全責任的立法建議所進行的前期工作**，包括參考其他地方的相關法例(例如內地的《關鍵信息基礎設施安全保護條例》)、將對關鍵基礎設施營運者的董事會施加的責任，以及業界對立法建議的框架有何意見。議員亦詢問當局會否設立專責部門，執行與保護關鍵基礎設施網絡安全相關的職責。

7. 政府當局表示，為推展上述立法工作，已研究內地、澳門、新加坡、英國、澳洲及美國的相關規管架構。經與業界交換意見後，有關行業普遍支持立法建議，而不少關鍵基礎設施的主要營運者亦已施行防範管理體系，以防範其基礎設施遭受網絡攻擊。視乎立法建議的最後定案，當局建議成立專責辦公室進行條例的實施工作，並會就辦公室所需的人手和配置，適時按政府既定程序作出安排，以便在法例獲通過後執行與保護關鍵基礎設施網絡安全相關的工作。

防禦網絡攻擊和應對網絡安全事故

8. 議員對近期針對公營機構的網絡攻擊導致資料外泄深表關注，並要求**政府當局闡釋這些事件的根本原因**。他們進一步詢問，有多少個政策局/部門(“局/部門”)及公營機構的系統(例如網站、應用程式及主機)曾遭勒索軟件攻擊，包括沒有向公眾公布的攻擊，以及這些遭受攻擊的系統是否已納入持續保安評估及改善計劃。

9. 政府當局表示，當局沒有備存公營機構遭受網絡攻擊的統計數字。同時，根據政府的資訊保安事故應變機制，所有局/部門須在發生資訊保安事故時向資科辦通報；而在2023年，資科辦透過其政府電腦保安事故協調中心，處理了9宗與政府裝置有關的已呈報保安事故，其中首3類已呈報事故為遺失載有機密數據的流動裝置或可移除媒體(佔所呈報事故的23%)，以及勒索軟件和資訊系統或數據資產受損害(兩者均佔所呈報事故的22%)。[4]

---

[4] 政府的資訊保安事故統計數字登載於政府的公共資料入門網站“資料一線通”，供公眾查閱，而相關數字由資科辦每月更新

10. 議員關注**政府和公營機構在網絡安全領域的管治架構**，包括**資科辦在公營機構的網絡安全領域可否發揮作用**、由資科辦制訂及定期更新的**《政府資訊科技保安政策及指引》("《政策及指引》")是否適用於公營機構**，以及會否參考新加坡的相關管治架構，成立公共機構數據安全檢討委員會及數據局。

11. 政府當局表示，當局已提出多重的評估、監察、風險管理及應變制度，以確保局/部門資訊系統的安全。各局/部門均須採用風險為本的原則，持續為其資訊系統識別保安風險。相關規定包括定期進行獨立的資訊保安風險評估，以及檢視現行的保安措施，以確保相關措施與時並進，有效應對最新網絡風險。同時，資科辦制訂及定期更新的《政策及指引》，雖然僅供各局/部門遵從，但資科辦已把《政策及指引》上載至其網站供其他機構參考。[5] 公營機構可制訂和採取最為切合其營運模式的電腦系統、資訊科技管治政策和網絡安全防禦措施，並按實際情況和最新科技發展，提升其資訊科技基礎設備。

12. 議員提及警方擔當的重要角色，並詢問警方制訂的應變計劃有何更新，以**應對日益增加的網絡攻擊等情況**。政府當局表示，為應對新型網絡攻擊，警方已提出一系列相關措施，包括加強公私營合作及定期舉辦網絡安全演習，從而防止透過互聯網作出危害國家及散播恐怖主義的不法行為。此外，資科辦轄下的政府電腦保安事故協調中心與網罪科自2017年起合辦跨部門網絡安全演習，旨在提升各局/部門對網絡攻擊的防備意識和整體應變能力。上述演習最近一次在2024年4月25日舉行，有來自70個局/部門超過250名政府人員參與。

相關文件

13. 相關文件一覽表載於**附錄**，該等文件已登載於立法會網站。

立法會秘書處
議會事務部2
2024年6月28日

---

[5] 《政策及指引》可於以下網址閱覽：https://www.ogcio.gov.hk/tc/our_work/information_cyber_security/government/。

附錄

加強保護關鍵基礎設施網絡安全
相關文件一覽表

委員會	會議日期	文件
保安事務委員會	2022年2月8日	議程第III項：保安局局長就行政長官2021年施政報告作出簡報 會議紀要
	2022年10月31日	議程第IV項：保安局局長就行政長官2022年施政報告作出簡報 會議紀要
財務委員會	2023年4月12日	政府當局就審核2023-2024年度開支預算對立法會議員初步書面問題的答覆（答覆編號：SB011及SB065)
保安事務委員會	2023年11月13日	議程第III項：保安局局長就行政長官2023年施政報告作出簡報 會議紀要
財務委員會	2024年4月18日	政府當局就審核2024-2025年度開支預算對立法會議員初步書面問題的答覆（答覆編號：SB019及SB062)

立法會會議	文件
2023年10月18日	第17項質詢：提升網絡安全
2023年11月22日	第11項質詢：政府部門和其他公營機構的網絡安全
2024年5月29日	第18項質詢：政府部門和其他公營機構的網絡安全

立法會秘書處
議會事務部2
2024年6月28日