

加快立法保障關鍵基建網絡安全

梁熙 立法會議員

本港的網絡平台存在不少安全漏洞，越來越多企業成為黑客攻擊勒索的目標，如去年 8 月、9 月數碼港和消委會先後遭黑客以勒索軟件惡意入侵，警方統計去年本港錄得 37 宗涉企業系統被黑客入侵案件。有關事件敲響警號，如果入侵的是香港重要關鍵設施，後果將會不堪設想。特區政府早前向立法會保安事務委員會提交討論文件，建議訂立《保障關鍵基礎設施（電腦系統）條例草案》，訂明關鍵基礎設施的營運者承擔保護「關鍵電腦系統」的法定安全責任，需要採取適當措施加強其電腦系統的保安能力等。相關公眾諮詢本月 1 日完成，共收到 53 份意見書，有 47 份來自業界。除了一份來自英國人權組織表示不同意之外，其餘的意見書都是表示支持。

根據警方數據，今年上半年已錄得 30 宗黑客入侵及 26 宗軟件勒索，按年升一倍及近三倍，反映本港網絡安全情況堪憂。香港互聯網註冊管理有限公司表示，有近四成四的網站使用了不安全的第三方服務鏈接，讓黑客有可乘之機。因此，如何促使相關機構加大網絡安全的投入，防止黑客入侵，是特區政府是次諮詢的一個重點，有關立法望可促使關鍵基礎設施的經營者盡力採取措施，防範黑客透過

入侵影響社會運作。能源、水電、金融服務、電訊業等，都是維持社會有效運作的關鍵基建，屬於是次諮詢條例的規管範圍。

雖然社會普遍支持立法保障關鍵基建，但有外國團體認為，有關條例會讓當局進一步掌握相關機構的資料，特別是當中的個人信息。就此，保安局局長鄧炳強強調，特區政府對個人資料及營運資料沒有興趣，當局的關注只在於保障系統不被攻擊，確保系統為市民提供安全可靠的服務；任何人若表示有關法例是監控或取用資料，只是「呃你、嚇你」。事實上，有關的條例並不是香港所獨有，澳洲、英國以及新加坡早已有相關法例，相反香港現時只是追趕落後，補足現存法例的不足。

現時社會的日常運作早已離不開網絡，但不少機構為了節約成本，或是沒有意識到網絡安全的重要性，對於網絡安全往往掉以輕心。本港關鍵設施一旦遭受網絡攻擊，很可能會使關鍵基建運作大受影響，因此特區政府應盡快分析諮詢意見，早日提出立法建議，以督促相關機構提升本港關鍵基建網絡安全水平，確保本港關鍵基建正常運作。