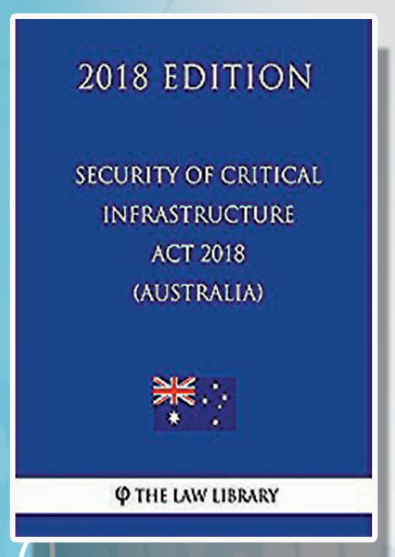
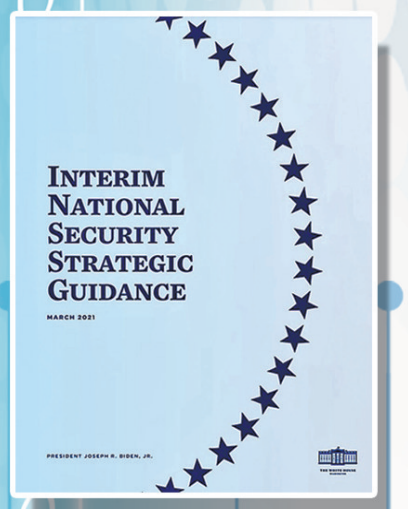
在數碼化時代，數據推動各項業務發展，成為社會產業建設的基礎，網絡一旦受到攻擊，就會造成相關業務甚至產業停擺。隨着政府、公共服務機構和基礎設施部門成為勒索軟件等惡意程式的攻擊目標，其影響力與破壞力也不斷增加，網絡安全不再局限於個別企業的自身防護，開始成為涉及產業鏈以至國家安全的重要問題，故此全球多國均制訂網絡安全法案，安全合規不但成為企業「必修課」，網絡安全更被許多國家提升至頂層戰略高度。

◆多國已將網絡安全提升至頂層戰略高度，圖為美軍在參與網絡防禦演練。 網上圖片



◆澳洲已經推出法案，強制規定責任實體報告網絡安全事件。 網上圖片



◆美國政府在《國家安全戰略中期指導方針》強調，需應對網絡攻擊。 網上圖片

保護用戶數據提升至頂層戰略

全球保護網安 法規愈發嚴密

美國白宮去年發布《國家安全戰略中期指導方針》，將提升網絡安全作為美國政府首要任務，並建立新的網絡空間安全和新興技術局，推動網絡安全國際間協作。澳洲政府前年也制訂網絡安全戰略，計劃投資16.7億美元建立新的網絡安全和執法能力。

美澳強制企業上報安全事故

在從宏觀監管角度治理網絡安全問題時，落實安全事故強制報告制度，已被多國以法律法規形式加以確認。美國證券交易委員會在2011年已要求上市公司，必須上報網絡安全事故及數據洩露事件，否則面臨調查。今年3月，美國眾議院通過《關鍵基礎設施網絡事件報告》法案，要求關鍵基礎設施所有者和運營商，需向網絡安全和基礎設施安全局報告網絡事件及勒索軟件付款。至今全美50州中，大多數已頒布相關法令，要求機構在發生個人信息數據洩露事件時及時通知用戶。

愛爾蘭禁擅用被盜數據

澳洲《2018年關鍵基礎設施安全法案》修正案於去年12月正式生效，引入網絡安全事件強制性報告義務，要求責任實體須在意識到網絡事件對關鍵基礎設施資產可用性產生「重大影響」後的12小時內報告。

此外，近年部分國家也嘗試從立法角度對相關企業支付贖金、提供支付渠道、傳播被盜數據等行為加以限制。前年10月，美國財政部國外資產控制辦公室發布公告表示，通過援引《國際緊急經濟許可權法》與《禁止與敵國貿易法》，與法律禁止的對象進行交易可能會被追究民事責任。向受害者提供支付給勒索軟件贖金渠道的公司，也需考慮自身是否具有金融犯罪執法網所規定的監督義務。

愛爾蘭衞生服務系統（HSE）去年5月遭Conti勒索軟件攻擊，影響多家醫院運作，HSE其後表示收到攻擊者給出的勒索金額，但「根據國家政策」不會支付贖金。隨後部分被竊的患者機密信息被公布在安全防護網站VirusTotal上，HSE之後獲法院頒令，要求禁止對被盜數據進行任何形式的處理、發布、共享或銷售行為。

歐盟推高額行政罰款

隨着各國對數據安全重視程度的不斷提升，企業須滿足嚴格合規要求，否則面臨高額行政罰款。愛爾蘭數據保護委員會3月宣布，由於Facebook（Fb）的母公司Meta違反歐盟《通用數據保護條例》，對其處以1,700萬歐元罰款。 ◆綜合報道

英分類網絡行為 嚴打起底煽暴

英國為限制和規範網上行為，皇家檢察署早於2016年便推出新法例，規定網絡暴力及網上起底行為均屬違法，並詳細解釋哪些行為或會違反法例，例如建立煽動暴力的標籤，又或鼓吹他人轉發具攻擊性的圖片。英政府今年初則發布《國家網絡安全戰略》文件，列出管理網絡安全風險、防範網絡攻擊、檢測網絡安全事件、將網絡安全事件的影響降至最低，以及培養正確網絡安全技能、知識和文化為五大目標，加強應對網絡風險。

根據2016年的法例，網上起底屬違法行為之列，若有人將他人的家庭住址、銀行資料或其他私人信息發布到網上，又或發布他人帶有侮辱性質的圖片，也涉及違法。該法例同時規定兩名未成年人在相互准許的情況下發送色情短訊，不屬於違法行為，除非短訊涉及暴力違法內容。

建新協調中心 冀「統一防禦」

有人批評法例過於嚴苛，是一種變相的審查制度。官方則回應稱這些條款旨在保障網絡安全，並稱資料顯示每4名青少年中，就有1人曾遭受網絡暴力。

英國是全球最早將網絡安全提升至國家戰略高度的大國之一，早在2009年6月便發布首份國家網絡安全戰略文件，用以指導和加強國家網絡安全建設。內閣辦公室每年發布報告，總結過去一年網絡安全工作的進展，並提出下一年的工作計劃。政府今年1月發布《國家網絡安全戰略》文件，闡釋政府如何確保公共部門有效應對網絡威脅，並描繪了戰略願景，即確保政府核心功能對網絡攻擊具有韌性。

新版網絡安全戰略提出在內閣辦公室建立新的政府協調中心，加強在公共部門之間的網絡安全工作協調，更快速地識別、調查和協調政府對公共網絡系統攻擊的反應，以確保信息共享更及時，實現「統一防禦」，還會建立跨政府部門漏洞報告服務體系，加強漏洞管理。 ◆綜合報道

醫院屢遭網攻癱瘓 法急撥10億歐元加強防護

法國總統馬克龍去年曾宣布，政府斥資10億歐元加強網絡安全建設、應對網絡攻擊行為。這項計劃聚焦加強網絡安全人員的教育培訓、探索技術解決方案，以便更好地保護企業和社區。

手術器械失靈 電話也打不到

法國西南部城市達克斯和東部城市索恩河畔自由城的醫院，於去年初遭到大規模網絡攻擊。法國負責數碼經濟產業事務的國務部長塞德里克·奧表示，該兩家醫院的信息系統遭受「勒索軟件」攻擊，導致系統癱瘓，醫院工作無法正常進行。不僅患者資料無法正常讀改、電話無法接通、床位和醫生無法分配，甚至手術器械也未能正常操作，一些外科手術因此被迫推遲，患者也被迫分流至其他醫院。

塞德里克·奧表示，法國前年發生27宗針對醫院信息系統的大型網絡攻擊。法國傳媒則指出，醫院並非唯一受到黑客威脅的機構，地方政府部門以及交通、信息和銀行機構也經常成為攻擊對象。此外，針對個人的小規模黑客行為同樣顯著增加，加強網絡安全建設迫在眉睫。

根據計劃，法國政府會斥資1.4億歐元用於相關人員的教育和培訓，並建設佔地2萬平方米的「網絡校園」，不僅提供培訓，還匯集了網絡安全領域60多個公私機構，是一個更有效率、更安全的網絡建設「孵化器」。

法國政府還會投入1.36億歐元用於建立國家信息安全局「網絡消防員」項目，通過在各地建立應急機構，在網絡襲擊發生時迅速採取應對行動。法國國家信息安全局局長普帕爾指出，網絡安全風險的增加，要求政府和相關機構必須改變做法，將安全問題列入預算和治理機制中，他還稱網絡安全行業的迅速發展，也將帶來大量就業機會。 ◆綜合報道

日持續完善網安架構 強化人才培育

在數碼經濟重要性日增及互聯網逐漸普及下，日本網絡安全領域面臨的威脅不斷加劇，故此日本持續重視強化網絡安全治理，根據自身情況推出相關政策與法律文件。

日本在2013年的《國家安全戰略》中，將「網絡攻擊」視為新威脅之一，認為提高網絡安全性和保護網絡空間，是國家安全的重心工作之一。日本近年積極構建自身網絡安全保障體系，完善網絡空間法律框架，並組建網絡空間安全機構等，旨在推行經濟治理與安全治理兩線融合的新時代網絡安全治理戰略。

推多部專項法律

在2014年11月，日本國會通過《網絡安全基本法》，旨在加強日本政府與民間在網絡安全領域的協調和運用，更好應對網絡攻擊，包括規定設立網絡安全戰略總部，負責制訂網絡安全戰略。在2018年，為應對網絡威脅不斷加劇與籌備保障東京奧運會與殘奧會，內閣提交法案對《網絡安全基本法》作出修正，並成立網絡安全委員會，使各種公共與私人實體可相互合作和共享網絡安全信息。日本還推出多部專項法律，例如《電訊事業法》主要保障公民通訊的保密性，規定不得違反電訊業務運營商的通訊保密規定。

經過多年建設，日本在網絡安全治理領域已構建較完善的組織和機構體系，形成以網絡安全戰略總部和網絡安全策略和事件應對國家中心為核心，以防衛省、經濟產業省、總務省、法務省等部門下屬機構為羽翼的機構體系。

公務員上培訓班 演習網絡防禦

在具體政策實踐上，日本進一步加強網絡人才教育與培養，於2017年發布《網絡安全人力資源開發計劃》，提出有利於改變企業網絡安全人才的培育導向，突出私營企業在網絡安全人才培育中的作用。其次，日本政府各部門均主辦網絡安全人才培訓班，強化網絡安全人才的培育。政府還通過組織網絡防禦演習，從實踐層面加強網絡安全人才的能力。

網絡安全威脅已成為全球的非傳統安全問題，日本謀求國際層面的網絡安全合作治理，包括美日兩國啟動多層次的網絡安全對話合作機制，以及促進與英國、法國等國家的雙邊網絡安全合作，分享網絡安全治理經驗，並致力打擊網絡恐怖主義。

◆綜合報道