作者/Marietje Schaake　譯者/王建基　審者/洪琬婷

當前網路攻擊事件層出不窮，唯有建構完整安全防護體制與定期演練，才能有效因應該項威脅。(Source: US Cyber Command)

建構反制數位威脅的國際法律規範

The Lawless Realm: Countering the Real Cyberthreat

取材/2020年11-12月美國外交事務雙月刊(*Foreign Affairs*, November-December/2020)

近年來各國決策者皆關注發生「數位珍珠港事變」的可能性。面對此種跨國威脅，各國領袖應在國際層次上合作，共同建構新的法律規範來加以因應，方能確保自由、合乎規則的秩序能續存於數位時代。

2019年夏天，挪威國會、紐西蘭證券交易所與梵蒂岡教廷等政府機構，均遭駭客攻擊。入侵者未發一槍一彈、未破門而入、未引爆炸彈，而是侵入這些機構之內部網路，企圖竊取資料、擾亂日常作業，或者勒索、敲詐受害者。此類事件只不過是冰山一角。當今網路攻擊層出不窮，許多網路入侵事件不是沒被察覺，就是遭刻意隱匿。在民主國家中，僅有情報單位與私人企業，能夠深入瞭解網路攻擊及其所造成之風險。其他人則必須設法探求數位世界表像下的實情。

多年來，關切此一新興威脅的決策者早已指出的確可能會爆發「網路珍珠港事變」(Cyber-Pearl Harbor)。一旦如此，各國關鍵數位基礎設施，必將在劫難逃。雖然眼前多數威脅的規模沒有這麼龐大，仍能造成重大危害。2017年，有駭客利用微軟Windows作業系統漏洞，使150國的30餘萬套電腦系統感染惡意病毒。這種稱為「想哭」(WannaCry)的病毒，侵入了個人、企業與政府機關，例如英國醫療保健服務(National Health Service, NHS)系統的1萬9,000筆掛號資料因而取消，造成將近1億美元的損失。專家根據所有舉報資料推估，全球因「想哭」病毒侵擾所造成之損失，高達約40餘億美元。經英美調查人員追查，最後發現該惡意程式是出自北韓境內之駭客。

「想哭」病毒是種少見、眾所皆知的事件，也只是那普遍而且不易覺察或瞭解的大型事件之一環：利用陰謀達成其地緣政治或犯罪目標之惡意行為者，能藉由「想哭」利用整個數位世界的種種弱點。網路攻擊與入侵事件大多難以察覺，因其往往是以一連串長期小動作蠶食鯨吞，而非採取一次致命打擊。決策者不應執著於高能見度之突發事件，而是要致力重振民主制度在確保網路公共安全方面所扮演之角色，要落實這點，各國政府就必須承認，私人企業確實掌握著數位世界大權。民主國家已對私人企業讓利過多。政府機關大多要看私人企業的臉色行事；這些機關無法對提供醫療院所、電力網路或智慧裝置應用軟體的公司企業進行深入調查。立法機構與地方議會，亦無從探知上述系統進行過何種程度的壓力測試。這類不對等狀況，賦予了私人企業一種政府所夢寐以求的優勢：肩負國家安全重任的政府機關，如今往往深陷於仰賴商業數據方能履行職責之尷尬境地。政府正面臨挑戰，那就是要以極快速度理解數位領域衝突與風險，但是他們已經浪費許多時間，導致未能透過諸般作為，來治理這片法外之地。

被弱化的國家

幾世紀以來，國家一直獨占動武權。但自從數位化與網路武器孕育出不對稱力量後，此一獨占權便逐漸旁落。的確，包括美國在內的許多民主國家，已發展出許多強有力網路工具、以此建立精密監視系統並對敵人發動攻擊。同時，已開發國家亦與那些在科技領域運用不對等力量的私人企業相互角力、搶食各種數據，並爭奪某些國家重要功能，保護關鍵基礎設施就是其中一項。

各國私人企業不但建立數位世界的架構，亦管理絕大多數數據流。他們往往是網路攻擊的受

害者，但在其未能保護資料庫並讓客戶個資外洩時，反而變相成為網路攻擊的同謀。更糟的是，這些企業甚至還在研發出新科技後，將其售予全球各地的敵人。威權(以及諸多民主)政府會僱用駭客從事不法勾當，並購買商用數位監視與控制系統。例如，有家稱為「沙德萬」(Sandvine)的美商公司，受指控曾提供白俄羅斯政府相關科技，讓該國在2020年夏天國內爆發反政府示威期間，用來切斷大部分網路，使民眾難以上網。民兵團體與幫派之類的非國家行為者，亦能透過網路攻擊，造成不對稱危害，使相對強大的國家、公司企業與國際組織蒙受損害。

各國當局往往對網路攻擊理解不足，找出犯案者亦十分不易。因此，攻擊者通常熟知脫罪竅門，懂得如何施展狡詐手段，從法律真空地帶攫取利益：僅有極少數機制可促成國際合作與協調，將網路攻擊者緝捕歸案、繩之以法。「偽旗行動」(False Flag Operations，行為者隱藏其身分並嫁禍他人之舉)在數位世界早已司空見慣。從世界另一端所發動的入侵行動，能在幾毫秒之內完成，幾乎不露痕跡。數位創新之速度，遠超過各國防範網路攻擊、追究駭客罪責，以及制定有關加密標準、數據防護與產品責任(要求生產者或賣方對其所製、所售物品負責)等事項法律的能力。

各國亦無從管制其行為可能危及公共安全之私人企業；確實在某些案例中，國家會發現自己不得不依賴此類公司。2020年初，Clearview AI臉部辨識公司資料庫遭入侵，才揭開了這家公司的神秘面紗，其不僅將技術與資料庫售予執法機關，居然還賣給許多私人企業。這起管理失當案顯示，私人企業如何在未獲當事人同意且在不透明的情況下，將關於人民的資訊秘密交付他人；以及這種公司在面對居心叵測的對象時，顯得多麼脆弱。然而，執法單位對於Clearview AI等科技公司的依賴，卻是日漸加深。

社會對於可連網數位裝置依賴日深的情況，會形成更多弱點。精明且主動之駭客，便能從民眾家中物聯網的電冰箱上，或在遍佈感測器的智能城區街道中，找出許多可用來癱瘓大規模系統的登錄點(Entry Point)。光這點就夠讓各國國防單位與情報機構如履薄冰，忙著派人四處站崗，緊盯是否有此類敵人現身。但由於數位科技普及，如今早已無處不是網路戰最前線。無論是醫院裡的醫師、大學實驗室裡的教授，還是某些國家高壓統治下的人權運動人士，都必須對抗網路威脅。

此類民間目標，並未隨時做好防禦準備。公共機構所採用的，往往是防護不足的網路系統，即便在處理機敏資訊時亦復如是。例如，醫療診所寧可增聘醫師，而不想雇用網路安全專家，這實在是無可厚非。公立大學可能願意添購電腦讓學生用，而不願購買昂貴之防護措施，來確保新購電腦系統的安全。選舉委員會可能不再採用紙本投票而決定裝設投票機，卻對於適切之保全作為毫無所悉，也不曉得有關保障選票安全這項先決條件，還有哪些方面可投入資金予以補強。以上種種立意良善的作為，其用意本身值得嘉許，但同時也使社會更顯破綻處處。

賦予更大職權

民主國家中公、私部門間的不平衡狀況，顯然

是另一個危險場域：私人企業能出售網路武器予獨裁政權。僅有少數幾項法律規範這些公司，應如何進行數位監視、阻斷與因應系統入侵。敘利亞就是一例。在該國內戰爆發之際，阿薩德(Bashar al-Assad)政府便曾運用網路戰手段，打擊國外敵人與國內反對派。進行網路戰的駭客，隸屬所謂「敘利亞電子軍」(Syrian Electronic Army，宣稱是獨立作業，與敘利亞政府無涉)，在竄改《紐約時報》(*The New York Times*)與英國國家廣播公司(BBC)等諸多西方媒體網站內容，以及駭入美陸戰隊網站後，受到全球關切。上述曇花一現的宣傳勝利，比起2011年和平抗議活動期間，敘利亞政府攻擊國內反對人士與人權鬥士的數位科技手段，那真是小巫見大巫。當年，敘利亞政府以精密的數位科技，蒐集異議者之間的通聯內容，並據以將其入罪、監禁。

世上最殘暴的政權採取這種高壓手段，實在不足為奇；奇怪的是，竟然有歐洲企業助紂為虐。阿薩德政府所採用的科技與專業技能，係來自一家名為AREA的義大利公司。AREA公司所出售之科技，可讓敘利亞當局監視全國通信、蒐集與掃描臉書貼文、Google檢索內容、簡訊與通話，進而找出關鍵字與特定人士間的關聯。之後亦根據所得結果，將異議民眾一網打盡，並對其施以酷刑、痛下殺手。

並非只有敘利亞從國外引進科技來鎮壓異己。過去數十年，總部設於西方國家的諸多企業，就曾對埃及、伊朗、沙烏地阿拉伯、阿拉伯聯合大公國及其他威權政府，設計並且販售類似的科技產品。若民主國家未能制止其境內公司，而放任這些公司對獨裁政府出售攻擊性駭客系統，那就是妨害其自身良善外交政策。但問題似乎並未解決。先前有評估報告指出，至2021年，此類系統之年銷售額將可能提升至數千億美元。中共現正也亟欲打入這塊市場。中國大陸早已是全球打壓異己專用科技之發展與出口大國，這些科技包括臉部辨識科技與預測性執法系統等。

非國家行為者持有這些科技，也是一大問題：此類行為者能藉由網路攻擊，使遠比他們強大的國家、組織與企業元氣大傷。2015年，摩根大通銀行(JPMorgan Chase)8,300萬個帳戶被駭，四位元兇最終被捕。2017年，一位獨自行動、名為「拉斯普丁」(Rasputin)的駭客，侵入美國各大學與政府機關，後續顯然是希望出售所竊資訊。2020年初，一位17歲的佛羅里達青少年夥同另外兩位駭客，試圖操控130位知名人士的推特(Twitter)帳號，包括美國前總統歐巴馬與時任副總統的拜登，並貼文誘騙民眾，把錢匯入某一比特幣(Bitcoin)帳號。實際上，駭客操控這些帳號，甚至可以犯下情節更重大的惡行，包括企圖升高地緣政治衝突，或使股市崩盤。

出高價者，即可獲得若干高階駭客之服務。在眾多雇用駭客的企業中，最臭名遠播的就是「暗物質」(DarkMatter)網路安全公司。這家公司總部位於阿拉伯聯合大公國，其曾雇用美國國安局與以色列國防軍前情報官，創造出私人情報服務，並模糊了個人企業與政府機關間的界線。此類具有頂級技能的企業，可能會吸引一些惡名昭彰的顧客，包括威權政體甚或是恐怖分子團體。

諸多民主國家已盡其所能管理數位世界以及

網路武器市場，但若干科技公司卻著手採取行動。WhatsApp透過其母公司臉書，在2019年春季，對以色列行動裝置監視公司NSO Group提出告訴。訴狀指出，此公司暗地裡利用WhatsApp之漏洞，從客戶電話非法擷取資訊。臉書也主張該集團之行為係屬違法。同時NSO Group在以色列也成為另一起官司的被告。2018年，某位沙烏地阿拉伯異議人士宣稱，該國當局使用NSO Group科技竊取其通信內容，包括其與哈紹吉(Jamal Khashoggi，同年於土耳其慘遭沙烏地幹員殺害的記者)之通話內容。國際間咸認有45國使用同一套NSO Group產品，其中包括墨西哥與西班牙等民主國家。

制定規範

各國不應將產品、服務是否可能對其情報單位不利的決定權，交由私人企業做主。民主國家應將行為準則與法規範疇延伸至數位網路世界，進而保障其安全。如同認可規範戰爭行為與核武的國際法般，各國理應、亦應在打擊網路空間威脅方面達成協議。犯下網路攻擊罪行的攻擊者，已經逍遙法外多時。民主政府尤應採取諸般作為，平衡國家與私人企業之間的權力，因為私人企業在數位網路世界所擔負之角色實過於龐大。

決策者的第一步，應從清楚定義何種數位化系統攸關公眾利益、公共安全，以及社會機能方面做起。各國官員須將相關系統(例如投票系統)定位為關鍵基礎設施，訂定一套明確標準與法規規範加以約束，而主要由私人企業掌控之系統，亦復如是。世界各國大多離這道戰線還很遠。一直到了2017年1月，美國國土安全部(Department of Homeland Security)方將選舉相關系統定義為關鍵基礎設施。

各國官員往往無法獲得有關公共服務風險之資訊，但他們應該對此瞭如指掌才是。例如，有關醫療院所、投開票所、稅務機關及其他重要機構，在遭受網路攻擊後之恢復力的壓力測試評估結果，應通告各官員周知。此外，各國政府亦應思考中央與地方官員該如何獲得數位系統、制定責任機制，以使私人企業對其產品所造成之後果負起責任。與Clearview AI同等類型之科技公司，不應獲准在網路搜刮資料來建立臉部資料庫，並將該資料庫售予執法機關。在如此龐大科技權力被授予Clearview AI這類稽核不周、且監管不嚴的私人企業下，警方愈來愈難依法行事。

商業秘密與非公開協議，往往使公眾無從得知此類科技公司營運方式之相關資訊。於是各國政府便要費盡心力對付實際威脅，以及存在已久的風險。諸多私人企業所享有的類似法律防護罩，也會妨害外部針對其產品在有意或無心達成之效果所做的獨立研究。這種諱莫如深的障礙，會使得公眾無法在充分理解的狀況下，對數位化與相關安全議題進行論辯，也會使政府無法利用證據以制定政策。各國政府應制定各項標準與法規，以確保私人企業提供具有實際意義的資訊。

投鼠忌器的道理眾所皆知，但各民主政府仍依然運用其秘密網路戰攻擊武器，設法嚇阻敵人。這種舉措應有清楚明白

網路安全議題之防範，必須靠各國間相互合作，持續滾動修正相關法令規章。(Source: World Economic Forum)

的交戰準則。無論攻勢抑或守勢網路行動，皆應受民主與法治的監督，即便監督作業列屬機密也應如此。

自2018年美國前總統川普簽署了一份旨在以鬆散方式來管制數位武器運用之〈國家安全總統備忘錄〉(National Security Presidential Memorandum)後，美國隱蔽作戰的矛頭便轉向中共與俄羅斯。美國國會議員抱怨，川普當局從未讓其知悉備忘錄內容。少了民主機制監督，就會肇生問題。不應在沒有法律授權與適當獨立監督下，增加防禦性與攻擊性網路武器的使用，即便使用者是通常依法行事之民主國家也是如此。

除了確保軍方運用網路科技的作為會受充分監督外，各國政府亦須斬斷私部門與情報單位之間的緊密關係。「旋轉門機制」(Revolving Door)會助長數位武器之發展、生產與銷售。各國政府應採取增加廠商銷售執照申請之附帶要求，以及禁止將相關產品售予敵對國與專制政權等方式，俾有效管控商業監視與市場駭客行為。私人企業應恪遵人權普世原則行事。

巨額罰款、訂定刑責，甚或取締具有惡意功能的數位產品等，皆是立竿見影的方式。那些與獨裁政府簽訂條約而流於助紂為虐的私人企業，禁止其參與政府採購標案，必能迫其做出正確選擇，從而防止資訊流入敵手。監視、隱蔽駭客行為與資料竊取，絕不可視為合法商業服務項目。政府另應制定法規，禁止情報官員今日還在為國服務，轉眼便在民間公司建構軍武級的駭客系統。

同時，各國政府必須對必要的公私部門合作事宜，進行更高強度管控。公家單位經常要靠私人企業保護關鍵基礎設施，或監控數位系統之風險。在這種情形下，權責單位應建立一套明確的責任鍊與問責鍊。各民主國家政府機關間，在逐漸遭遇各種數位時代挑戰之際，亦須隨之強化相互協調能力。在政府各部門共同投入下，必有助於找出相互衝突的目標，並使各部之間思想觀念一致、權責劃分清楚。

民主社會能使民眾清楚瞭解網路攻擊所造成之傷害(確有網攻受害者存在)，因為民眾大都認為此類事件難以理解，而且都是由軍方神秘駭客所為。這種觀念應該加以改變。網路攻擊的後果會造成實質損害，受害者也遠不只國防部、情報單位、私人住宅、養老院、大學校園與醫師診間等。揭開此一威脅之神秘面紗並將之人性化，應可使更多人更嚴肅看待網路安全，及其使用數位科技的方式。若政府能保證私人企業更透明，那新聞媒體便能更仔細監視私人企業的一舉一動，進而使消費者知道更多。民眾的投入，必定有助於維繫此一變革所需的政治議題於不墜。

各國領導人應召集必要人士履行政治意志，在國際層面上敦促各國，持續滾動修正其行為準則、指導方針、規則命令與法律法條；因為網路空間的入侵者，全然視國界如無物。歐盟提出了一個典範，使有志一同的國家大致理解跨國界協調的作法。其會員國，對於涉及網路安全事項(包括資料保護，以及檢查外國投資歐洲公司所可能肇生之風險等)之相關法規，均已達成協議。各會員國刻正修正針對商售駭客系統出口之管制措施。歐盟會員國在集體層次上，對於制裁那些挹注於網路攻擊之資金亦已達成協議。

基於如此精神，世界各國必須對新規範達成協議：例如，何種程度之網路攻擊應視同戰爭行為？對於此類攻擊有何措施可作為適切因應對策？針對關鍵基礎設施所進行之網路攻擊會對日常生活造成真實災難與傷害，理應等同於對此類設施之傳統攻擊。對民主政府而言，現在正是時候開始嚴肅看待21世紀態勢多樣之衝突。

持續不斷的網路侵擾與攻擊，意味著在駭客與政府間的戰鬥中，民主國家正節節敗退。如果各國政府無法做得更好，權力平衡將更傾向惡意分子、私人企業與威權政體。但如果成功，透過民主機制所產生的諸多措施，就能管控當前無法無天的網路空間。此後。各國人民便能對數位時代自由法治下的秩序，重新建立起信心。

作者簡介

Marietje Schaake 係 CyberPeace Institute 董事長，以及美國史丹佛大學 (Standford University) 網路政策中心主任。