



● 作者/Paul J. Hwang ● 譯者/章昌文 ● 審者/劉宗翰

海運網路安全觀

Cybersecurity: An introduction

取材/2019年4月美國陸戰隊月報(*Marine Corps Gazette*, April/2019)

隨著港口各項基礎設施的數位化，美國海運產業將更容易受到網路恐怖主義的危害，這種威脅攸關國家安全，不管是軍方還是民間單位都應及早研擬有效防範措施。

網路安全已成為美國數位基礎設施漸增的隱憂，網路恐怖主義是游擊戰的升級版，網路恐怖分子無需實際現身即可進行攻擊，這是可從世界任何地方發動的非傳統戰爭進階版，能就地購置技術且神不知鬼不覺的執行。按美國國土安全部的說法，當敵國政府、恐怖團體、心懷怨懟的員工或惡意入侵者等非授權人員，試圖「未經授權取用管制系統裝置與/或數據傳輸路徑使用的網路」時，就會有網路威脅。¹ 網路戰是會用在未來戰場的尖端武器，對美國重要的是，別認為網路安全不是切實可行且迫在眉睫的威脅。隨著技術進步與美國基礎設施的數位化，網際空間將成為新的戰場，但不幸的是，對美國經濟來說，最脆弱領域的其中之一就是海運產業。

隨著美國海運產業其港口的現代化，使之更容易受到網路恐怖主義的危害，實際上，海運產業就連防止過去的



數位化已成社會進步的趨勢，但網路安全維護卻無法與時俱進，也成為國家安全的最大隱憂。(Source: Reuters/達志)



安全威脅都已力有未逮，如果今日有名網路恐怖分子要以某個港口為目標，港口根本無從做好準備；美國的港口沒有偵測、防止，或從網路攻擊中復原的能力，海運產業公司領導人勢必要開始密切關注網路世界中漸增的安全威脅，尤其因為港口已開始倚賴自動裝運及自動港埠營運，港口安全分析師必須擬定計畫，以確保港口免遭網路恐怖分子的危害。

二十一世紀的恐怖主義

恐怖主義概念是慣常性演變的。在911攻擊前，傳統恐怖分子攻擊係指敵對國家或恐怖分子組織利用大規模毀滅性武器發動攻擊。然而，

二十一世紀恐怖主義概念改變了，在此新的時代，安全分析師的思考必須含括新式威脅及想定，由於蓋達組織等激進組織的崛起，恐怖主義已經歷具代表性與引人注目的恐怖主義新形式。這些恐怖主義的新形式超出化學、生物與核子作戰的概念，二十一世紀的恐怖主義利用地鐵車輛和飛機之類的平凡物品作為致命武器。² 平凡物品的易取得性，正是造成這些新式、具代表性與引人注目的恐怖主義形式危險的原因。在過去，只有受過高等教育的化學家、生物學家，或是核子工程師才能協助製作大規模毀滅性武器。然而，二十一世紀的恐怖主義已逐步發展成使用像電腦和網路之類容易取用的物品，現在，世界上

隨著美國港口的現代化，也使其更容易受到網路恐怖主義的威脅。

(Source: US Coast Guard/Henry G. Dunphy)



任何人都可以展開對美國的攻擊。

在美國的網路恐怖主義

按參議員努恩(Sam Nunn, 民主黨—喬治亞州)在1998年2月26日的說法,有11套美軍系統曾受到電子攻擊,因為犯案者透過阿拉伯聯合大公國的電腦系統改道攻擊,使美軍無從辨識。網路恐怖分子並未存取機密系統或紀錄。不過,他們成功存取了軍方的後勤、行政及會計系統。在入侵這些系統之後,網路恐怖分子完全掌控美國在海外及國內軍事行動所需的核⼼數據。³在最近的新聞中,白宮通報在提供總統行政辦公室使用的非機密網路中,從2014年10月至2015年4月間有一系列可疑的活動,儘管駭客存取的並非高度機密資訊,但駭客確實存取有關總統公開和非公開行程的敏感資訊,美國密勤局(U.S. Secret Service, USSS)和其他情報機關雖無法確認誰是犯案者。不過,他們懷疑這些網路攻擊有可能是俄國人搞鬼。⁴

我們有多脆弱?

網路安全與在生活中利用科技的每個人都有關聯,網路威脅不僅適用國家安全,也適用個人安全。在對抗網路恐怖分子方面,美國人民有多安全?答案是:沒人能高枕無憂,在使用電話、電腦、甚至是嬰兒監聽器的每個人日常生活中,網路威脅都是迫在眉睫的問題。2013年8月14日,在美國休士頓的一戶人家深夜聽到有聲音對兩歲大的女兒說話,這對夫婦大吃一驚,當搜尋其孩子的房間時,發現嬰兒監聽器被入侵了,這對夫

婦說,有個男子的聲音正對他們女兒喊叫「醒過來」。⁵休士頓當局調查了該房屋後,總結說有名網路罪犯入侵這對夫婦的嬰兒監視器網路,藉由入侵該網路,這名駭客得以與孩童說話,並看見這對夫婦房屋的內部,這對夫婦從未想過會成為網路犯罪的受害者。

不幸的是,與這對住休士頓的夫婦一樣,美國絕大部分人都輕忽網路威脅的嚴重程度,社會上往往認為,網路攻擊僅限於對政府組織和排行榜500大財富的公司。換句話說,社會相信網路攻擊只會對有錢或有權的大型實體。不過,網路恐怖分子對其目標是來者不拒的,這些身分不明的罪犯使弱勢群體受害,而這些往往是在美國生活的大多數人。

另一個脆弱目標的代表性案例,是在行動裝置上使用應用軟體的那些人。2014年10月1日,SnoopWall——專精網路防衛的公司——測試並安裝十個不同的安卓手電筒應用軟體後,發現令人不安的資訊。該網路防衛公司發現,任何下載此應用程式並同意條件的用戶,接收的不只是一個手電筒應用程式而已,若接受應用程式的條件,就是讓應用程式擁有者有權使用顧客的個人資訊,網路安全小組發現,這允許應用程式擁有者使用顧客全球定位系統位置、接觸清單、網路操作系統,以及線上銀行資訊的權利。⁶遺憾的是,顧客一旦下載該應用程式並接受條款,損害早就已經造成了。

網路罪犯現在已能存取受害者的個人資訊了,這些不是賣給跟蹤者用於尋找地址,就是給其他需要受害者銀行資訊的罪犯。手電筒應用程式之



類的網路攻擊僅只是小規模威脅，隨著美國的經濟和基礎設施轉變到數位時代，網路安全變得讓人日益憂心，技術愈進步，網路攻擊就變得愈先進。

網路威脅的分類

SRA國際公司——專精網路安全並為美國政府提供盜版解決方案的公司——製作出一個美國網路安全威脅的先後順序表，該先後順序表也顯示出過去六十年間網路安全威脅的演化與進展。根據該網路安全演變的先後順序表，網路威脅就像普通感冒和流行性感冒，每次專家從病毒製造出疫苗治癒病人，病毒就適應該疫苗，還變得更加頑強。就像感冒與流行性感冒一樣，網路威脅與網路安全保護軟體(也就是防火牆和加密代碼)不斷適應演化，要完全防止網路攻擊的發生幾乎不可能，但基於兩個原因，組織仍須去認識它們的潛在威脅：阻擋所能掌控的部分，並讓公司能在攻擊過後改善其還原能力。

美國政府責任署(U.S. Government Accountability Office)將網路安全劃分成兩個不同類

別：第一類含有不同類型的網路威脅資訊；第二類則含有網路罪犯和網路恐怖分子通常會使用的網路攻擊類型資訊。⁷ 因此當務之急是列出並確認組織或個人，將來可能面對的不同型態網路威脅與攻擊。

第一類的主要網路威脅是違規事件，官方對違規事件的定義是不當使用或不當處理敏感資料。⁸ 據美國政府責任署表示，違規事件的主要犯案者是粗心的雇員。違規者使用的個人裝備(亦即私人電子郵件、膝上型電腦及網路)往往會對既有的安全網路有害。⁹ 一名政府雇員可將其個人隨身碟插入安全網路而不必擔心網路威脅；不過，當雇員將其隨身碟帶回家完成其未竟工作時，問題就來了。當雇員將隨身碟插入其私人電腦那一刻，原本安全的系統就變得易遭破壞，在雇員回來工作之後，他就會危害到整個民間組織或政府機構安全網路的完整性。希拉蕊(Hillary Rodham Clinton)在任國務卿時就違規網路安全規定，她因使用其個人、未經加密的電子郵件而違犯規定。¹⁰ 對一般平民百姓

來說，使用其個人電子郵件不是個問題；不過，當一名國家外交官利用其個人郵件來傳遞機密與敏感資訊時，就成了重大問題。所幸，這種特定網路威脅是可以輕易避免的，政府和非政府組織必須確保其雇員不因粗心大意而危害到自身網路安全。

第二類的主要網路攻擊是惡意程式碼，這類型網路攻擊最常見的是由網路駭客所為，惡意程式碼是成功安裝或執行的惡意軟體(亦即木馬、蠕蟲、間諜軟體或最高權力的使用者套件)，這類型攻擊可以藉由手動、透過電子郵件，或任何其他有創意的方式成功執行，惡意軟體很容易藉由安裝諾頓防毒(Norton AntiVirus)之類的防毒軟體來防止。¹¹

另一類型的網路攻擊是共謀，不過應歸屬第二類，共謀是敏感與機密資訊的散布/洩漏，網路恐怖分子也使用共謀來遂行對其他國家或組織的諜報。¹² 與其他的威脅和攻擊不同，共謀是最難預防或偵測的網路威脅/攻擊之一，為了使組織不成為這類型攻擊的受害

者，必須定期偵檢其安全網路是否有任何可疑的網路活動。此外，組織必須持續升級或變換安全網路，由於網路威脅/攻擊會適應目前的預防措施(正如疫苗和流行感冒一樣)，公司和組織必須一直使自身網路安全軟體與時俱進。

美國因其日益增加的數位基礎設施，察覺潛在威脅這點尤其重要，隨著社會的日漸現代化，政府同樣必須適應變遷。例如，社群媒體在美國已成為溝通的第一線，儘管仍有少數美國公民倚賴報紙、收音機和電視來接收當前的新聞，大部分較年輕一代的公民則只倚賴社群媒體(亦即臉書和推特)來獲得最新的消息，為擴展與他們的接觸，政府組織利用社群媒體來作為溝通工具。近年來，白

宮開設官方的推特、Instagram、YouTube及臉書帳號，國防部同樣也更新溝通方式。與白宮一樣，陸、海、空軍及陸戰隊也都開設官方的社群媒體平臺。

其他像通訊社、醫療服務及執法機構之類的組織，也都成了數位時代的受害者，另一個正緩慢展開現代化的產業是海運產業，像是洛杉磯港(Port of Los Angeles)和長灘港(Port of Long Beach)等加州主要港口，已著手利用現代技術，由於美國的數位基礎設施開始增長，網路威脅已經成為對國家安全和國家生計的嚴重威脅。

網路威脅的風險評估

為闡明網路安全並與其他威脅相互比較，本文提供一張機率與影響的列表(如表1)，另為

便於理解該議題的嚴重性，也構思一張網路安全的風險評估表(如表2)。

對美國海運產業的網路威脅

對網路威脅的風險評估，可說明一次重大網路攻擊對美國數位基礎設施將造成的衝擊，幸好美國有安全機構(亦即國家安全局和中央情報局)專門負責監測或防止任何外國或國內的網際空間威脅。遺憾的是，安全機構並無法維護美國經濟的每個部分，海運產業就是沒受到美國安全機構嚴密保護的許多產業其中之一。

誰有興趣駭侵港口

海運產業的潛在網路罪犯名單是數不勝數，此一產業會成首要目標的原因在於它是一個重要的經濟產業，欠缺網路安全的海運產業，將吸引每日在尋求能輕鬆獲利的駭客。此外，像販毒集團、人口走私販之類的犯罪組織，也想駭侵並竄改港口的裝載清單。最後，恐怖組織和敵對國家亦有意藉由關閉美國港口來摧毀美國經濟。無

表1					
	機率 →				
機率 ↓	1	2	3	4	5
1	(1)	(2)	(3)	(4)	(5)
2	(2)	(4)	(6)	(8)	(10)
3	(3)	(6)	(9)	(12)	(15)
4	(4)	(8)	(12)	(16)	(20)
5	(5)	(10)	(15) 灣區大地震	(20) 核彈攻擊美國	(25) 網路末日 決戰



論理由為何，因為可以輕易匿名，這些犯案者對執行港口的網路攻擊都感興趣。

無人船運

海運產業不僅脆弱，它還是網路恐怖主義最可能的目標之一，全球貿易有95%是靠船隻運送，根據美國運輸部的資料，美國53%進口和38%出口是由海上船隻輸送。¹³ 此外，海運產業在2011年美國經濟上估計值約1兆3,000億美元，¹⁴ 對海

運產業的一次重大網路攻擊，就有可能嚴重損害美國經濟，當海運產業開始朝無人船運和港口施行時尤其如此，技術的演進，卻對港口賴以更容易、更快速及更有效運作的技術產生危害。¹⁵ 值得注意的是，海運產業須以安全來換取效能。目前，勞斯萊斯公司(Rolls-Royce Holdings)——總部設在挪威的英國海洋技術公司——正在研發能自動運送貨物的無人船隻。¹⁶ 儘管此項專案看來像是技術的突破，但卻有可能成為網路威脅的攝食

表2

風險評估公式：風險=f (威脅X弱點X影響)

威脅(意願X能力)：

• 意願

• 外部威脅

• 敵對國家、恐怖組織和罪犯(抗議人士—激進駭客、情報—諜報活動、政治)

• 內部威脅

• 政府雇員&民間承包商(財務、抗議人士—激進駭客、聲譽)

• 能力

• 所有具備對美國進行網路攻擊的技術、技能和資源的潛在威脅/恐怖分子。

弱點(機會或機率)：

• 機會

• 由於可從任何地方匿名進行網路攻擊，大部分網路恐怖分子每天都有絕佳機會。

• 機率

• 美國每一天都會遭到網路恐怖分子攻擊(數千次)

影響(破壞或成本)：

• 破壞

• 網路攻擊將造成美國極大的傷害

• 有可能拖垮美國的經濟

• 有可能危及美國國防部&武器系統

• 成本

一次網路攻擊「可能」造成美國數兆美元的損失

說明：此一風險評估係摘錄自海上安全(GMA 330)在2015年4月7日提出的網路安全報告。

(Source: Dalbec, Eddy, Hwang, & Meza, 2015)



勞斯萊斯公司所研發以操作員體驗為概念的統一艦橋。(Source: Rolls-Royce)

場，如果此項研發成果引進美國，將更增添美國海運產業面對網路恐怖主義的易損性。

勞斯萊斯公司目前研發了一種稱為操作員體驗概念的統一艦橋(unified bridge)，這將成為無人船隻的控制室，操作員體驗概念負責平臺供應船的前置規劃與督導，這是種負責運送非危險貨物的自動化船艦。統一艦橋將充當戰術管制中心，用來作為資訊與數據處理的中樞，平臺供應船的

操作人員可藉由輸入計算與數據到電腦，產生合適的操作設定檔來控制船隻，在選擇最適合的操作設定檔後，就會將關鍵操作數據和支援圖形送往無人船隻，而有了這些資訊，平臺供應船就能自動導引到達目的地。¹⁷ 從安全角度來看，一名網路恐怖分子就能輕易駭入統一艦橋，掌控整個船隊的平臺供應船，藉由掌控平臺供應船，網路恐怖分子可以將船上貨物變現，或是利用船隻作為



武器。

為解決對無人船運的網路威脅，公司必須投資情報小組，賦予阻止任何可能的網路威脅之責，儘管網路威脅在其攻擊前很難偵測與嚇阻，但並非無此可能。像勞斯萊斯之類的無人船運公司，必須僱用一個會致力確保統一艦橋安全網路的工作小組，在一次網路攻擊的事件中，公司必須找到問題，並妥善處置，保護系統將來不會遭到攻擊，為確保牢靠且安全的無人船運，這些公司必須不惜代價保護統一艦橋的安全網路。

對艦艇燃料的威脅

根據在博銳律師事務所(Blank Rome Limited Liability Company)的卡波尼(Steven L. Caponi)與貝爾蒙特(Kate B. Belmont)表示，到2020年，全世界銷售的艦艇燃料將達到每年平均5億噸，每公噸平均成本約為750美元，這等於年度艦艇燃料的銷售量為5兆美元，艦艇燃料的交易通常是透過電子郵件完成，利用電子郵件作為交易手段，使得艦艇燃料產業成了網路攻擊的脆弱目標，網路恐怖分子將電子郵件交易視為「易受攻擊的目標」(soft target)，意味著該產業極易受到網路威脅的影響。¹⁸

駭客攻擊艦艇燃料產業的方式是透過偽造發票，由於一家艦艇燃料公司是透過一連串的電子郵件與其顧客協商交易，駭客會等到雙方達成協議，一旦訂定協議，駭客會在艦艇燃料公司的正式發票送達該顧客之前將其攔截，駭客隨後寄出含有其銀行帳戶號碼的偽造發票，就可以等著收錢，在錢到手之後，駭客接著將錢轉到另一個境外

的銀行帳戶，在數星期未收到錢後，艦艇燃料公司重寄了一份發票給其顧客，而顧客就必須再付一次錢。¹⁹

艦艇燃料產業的網路安全議題不難預防，艦艇燃料產業必須採取的第一個行動，就是找出一個替代且安全的方法與其顧客溝通，如果燃料產業想繼續利用電子郵件，就必須有安全加密的電子郵件帳號，創造一個安全加密的電子郵件帳號，這與美國國務院員工所用的方法一樣。

安特衛普港

一個海洋產業重大網路安全漏洞的案例就發生在安特衛普港(Port of Antwerp)，在2011至2013年間，比利時的港口經歷過一次重大破壞網路安全的事件，該次犯罪活動的犯案者是販毒集團，駭入該港口的資訊技術系統，以利追蹤海洛因和古柯鹼的運送，網路犯罪進行了數年都未被察覺。對安特衛普港的網路攻擊令全世界諸多港口大開眼界，在該件破壞網路安全事件之後，許多港口和船運公司開始密切注意其船運艙單是否有任何未經授權的更動。

為解決此一嚴重問題，所有港口都應該熟知自身網路系統，港口經營者理當監控每趟裝運的船運艙單，港口亦當投入一支專精阻止網路滲透的網路安全小組，安特衛普港的破壞網路安全事件對全世界的所有港口都應當是一次前車之鑑，海運產業要一直了解其船運艙單動態，並在其網路系統中尋找任何可疑的活動。

結論

網路安全是對美國和世界的外來威脅，這是個有可能將美國扔回石器時代的嚴重問題，網路威脅之所以危險是因為有利目標的可企及性，且不會有相關聯的風險。不同於大規模毀滅性武器，網路攻擊並不需要生化學家或核子工程師，其所需只有就地購置的電腦與一般電腦科學概念，而這是全世界成千上萬大學都可提供的主修課程。至於風險，網路恐怖主義/攻擊並不需要自然人現身以便執行網路攻擊。

在審慎分析海運產業與網路安全之後，海運業的準備顯然相當不足，不僅因為該產業不夠安全、還欠缺復原能力，也未備妥應該訂定網路攻擊發生後的應變計畫，荒謬的是，當海運安全部門欠缺偵測、摧毀及預防網路威脅能力之際，海運產業卻在發展自動化船艦與港埠營運。

當前急務是海運產業必須跟上目前世界網路威脅的最新發展，必須投入能專責阻止網路威脅的安全小組，在此產業努力爭取技術進步(亦即無人船運和自動化港口)之前，必須置重點在保護其弱點上。阻止網路恐怖主義的最佳方法之一，就是在教育機構和工作場所傳播覺知，單憑覺知就能阻止像違規者之類的無心之過，知道並承認威脅，正是阻止未來網路攻擊發生的第一步。

作者簡介

Paul J. Hwang少尉畢業於美國德州大學奧斯丁分校(University of Texas at Austin)，目前在美陸戰隊第2遠征軍第2陸戰隊師第2兩棲突擊營第2連服役。

Reprint from *Marine Corps Gazette* with permission.

註釋

1. Homeland Security, (Washington, DC), information available at <http://www.dhs.gov>.
2. Dr. Donna Nincic, "The Challenge of Maritime Terrorism," *Journal of Energy Security*, (2005).
3. Central Intelligence Agency, "Cyber Threats and the U.S. Economy," (Langley, MD: June 2008), available at <https://www.cia.gov>.
4. Cable News Network, "How Russians Hacked the White House," (New York: April 2007), available at <http://www.cnn.com>.
5. C. Ngak, "Baby Monitor Hacked, Spies on Texas child," *CBS News*, (New York: August 2013), available at <http://www.cbsnews.com>.
6. M. Kiebrich, "Is Your Flashlight App Stealing Info Off Your Phone?" (Online: November 2014), available at <http://www.9news.com>.
7. G. Wilshusen, "Information Security," (Washington, DC: GAO, June 2012), available at <http://www.gao.gov>.
8. Ibid.
9. Ibid.
10. Cable News Network, "Hillary Clinton Email: Did She Do Anything Wrong or Not?," (New York: March 2015), available at <http://www.cnn.com>.
11. Hwang, research presentation, unpublished, (January 2015).
12. "Information Security."
13. M. Chambers and M. Liu, "Maritime Trade and Transportation by the Numbers," Bureau of Transportation, (Washington, DC), available at <http://www.rita.gov>.
14. SelectUSA, "Industry Snapshots," (Online), available at <http://www.selectusa.commerce.gov>.
15. Hwang.
16. "Maritime trade and transportation by the numbers."
17. Rolls-Royce, "Customer Focus," (Online), available at <http://www.rolls-royce.com>.
18. S. Caponi and K. Belmont, "Bunkerspot," (Online: January 2015), available at <http://www.blankrome.com>.
19. Ibid.