● 作者/Scott J. Tosi ● 譯者/黃文啟 ● 審者/劉宗翰

北韓網路戰力

North Korean Cyber Support to Combat Operations

取材/2017年7-8月美國軍事評論雙月刊(*Military Review*, July-August/2017)

自2014年索尼影業的網攻事件發生以來，已澈底改變世人對北韓網路戰力的認知，其已成爲全球性的戰略威脅。鑑此，北韓未來在戰術與野戰層級之網路戰運用，恐將對美韓聯軍確保朝鮮半島安全構成更嚴峻之挑戰。

直到2014年為止，某些西方網路專家在描述北韓(朝鮮民主主義人民共和國)網路能力時，仍然抱持相當無關緊要的態度，諸如安德斯(Jason Andress)和文特非爾德(Steve Winterfield)兩人在所著《網路戰：安全從業人員的技術、戰術和工具》(*Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*)一書中，就稱北韓執行網路攻擊的能力「……令人質疑，但其實際上應具有能力。」[1]但在2014年11月喧騰一時的網路攻擊事件，被認定是北韓為了報復索尼公司(Sony Corporation)上檔《名嘴出任務》(*The Interview*)電影的舉措，其後更澈底改變美國對北韓網路戰力的認知──從原本只是專門針對南韓(大韓民國)進行局部騷擾的小問題，變成全球性重大戰略威脅。[2]

2015年10月28日，北韓領導人金正恩視察位於平壤的科技大樓。
(Source: North Korea's Korean Central News Agency)

雖然北韓在索尼網攻事件發生後已被視為重大戰略網路威脅，但仍須考量其未來可能在戰術層級運用網路戰力，作為其作戰策略的延伸手段。由於南韓與美軍部隊對於戰術層級運用網路攻擊的作戰手段不熟悉，因而此種威脅更甚於任何基於政治動機所進行戰略層級的網路攻擊。北韓軍隊在戰術層級的軍備，就科技程度而言係相

當落伍。然而，證據顯示北韓人民軍在戰鬥行動中會採取網路作戰，以擾亂敵軍指管並降低自身在科技上的不利條件；因此，美國和夥伴國部隊必須做好因應此種威脅的準備。[3]

北韓軍事戰略

想瞭解北韓在戰時藉由戰術層級網路行動以支援作戰部隊的最可能方式，可以思考這個日益遭到孤立且科技條件不斷衰退國家的歷史目的和推斷軍事理論。據朝鮮問題專家明尼克(James M. Minnich)表示，在1950至1953年的韓戰未能統一朝鮮半島後，赤化南韓、必要時使用武力的「國家目標」(*kukka mokp'yo*)，就一直是北韓所追求之主要目的。[4] 然而，如2012年美軍致國會的報告中所述，北韓軍事政策與政治侵略態度之真正目的，卻是要控制並鎮壓北韓人民，以確保其統治權力，而非統一朝鮮半島。[5] 儘管如此，諸如2010年延坪島砲擊和2015年漣川砲戰等事件，都顯示出小規模挑釁行為有可能引爆雙方開戰。此外，戰鬥也可能引發全面戰爭。不論透過意外的武力升高行為或預先準備之猝然入侵，北韓有著全面開戰的意願。[6]

在韓戰戰敗之後，北韓模仿蘇聯和共軍模式以擴編與整建其軍隊。據明尼克表示，北韓後來持續從俄羅斯與中共取得影響力、裝備和準則。[7] 為了避免當年曠日廢時南侵戰爭的相同命運，北韓軍隊似乎已經發展出一套「奇襲戰略」(*kisub chol-lyak*)，希望以快速決戰、遂行混合戰術來對付朝鮮半島的南韓及美國聯軍。[8] 由於北韓經濟愈來愈無法支撐持久戰，此種作法逐漸不符時宜。據明尼克表示，為了達速戰速決的戰術目標，北韓開始以「大規模傳統與化學砲彈和飛彈攻擊，同步配合特戰部隊小組」的概念，編組軍隊遂行戰鬥。[9] 外界對於北韓特戰部隊的兵力判斷各有出入，從8萬到18萬名不等，這支部隊可以對南韓遂行不對稱攻擊，意在使大規模輕裝步兵部隊能發動後續攻擊。[10]

北韓原本很可能認為以砲戰和特種作戰掩護大規模南侵部隊，即足以在美軍增援部隊抵達前，快速打亂、混淆、超越並澈底擊潰駐防朝鮮半島的南韓及美國聯軍。然而，這項戰略在1990年代初期蘇聯瓦解及蘇聯軍備援助中斷後遭到撼動。但更令其震撼的，無疑是美國在1991年以迅雷不及掩耳之勢，輕易擊潰海珊的伊拉克軍隊，而伊拉克原本就是打算運用北韓長期規劃對付南韓的方式，以類似戰術和武器來對付美國。[11] 海珊擁有數量優勢的軍隊卻敗在美軍手中，無疑敲醒了中共和北韓，因為兩者都是依賴科技水準落後，但數量優勢的部隊，來快速壓制敵軍。在兩軍實兵戰鬥的狀況下，科技證明遠遠重於數量的壓倒性優勢。同時，由於北韓經濟與農業的快速衰落，更讓美國科技優勢能輕易擊潰北韓軍隊的可能性大增，因為上列因素削弱了其投射和維持軍隊作戰的能力。[12]

北韓開始發展核武就是因應這些變局的作法之一。[13] 雖然美國在「沙漠風暴作戰行動」中的勝利，顯示出其可以在傳統戰爭中快速且澈底地擊潰北韓軍隊，只不過可能會讓朝鮮半島平民付出高昂的生命代價，但

北韓的核武卻會讓美國或南韓挑起戰爭時，面臨南韓和美軍目標遭到大規模毀滅的高度風險。

儘管如此，發展核武嚇阻選項雖然可以鞏固北韓的守勢政治目的，但卻幾乎無助於達成其「國家目標」。針對這方面，北韓似乎是模仿中共在沙漠風暴作戰行動後所做表面上的準則改變。

在美國擊潰伊拉克軍隊(1990年全世界排名第五大軍隊)僅僅五週之後，共軍顯然已經開始評估美國的作戰戰略和戰術。[14] 在1990年代，中共所擬定的混合戰戰略是以相對廉價的科技方法，藉由間接攻擊方式抵銷美國在質方面的軍事優勢。1999年，〈超限戰：中共摧毀美國的主計畫〉(Unrestricted Warfare: China's Master Plan to Destroy America)一文(係取自1999年兩位共軍大校著作的英文摘譯版)即可看出共軍的新方法，其內容說明運用各種不對稱措施以擊敗美國，包含採取資訊戰在內的所有必要手段，以削弱美軍對戰場狀況的掌握能力。[15] 國家安全研究學者克拉克(Richard A. Clarke)和納克(Robert Knake)主張，此種戰略促使中共開始發展大規模網路戰，包含竊取科技資訊和情監偵資產的戰術目標情資，以扳回戰場對抗行動中的劣勢。[16]

由於相信核武可以嚇阻外敵對北韓本土發動攻擊，而且熬過了1990年代的經濟與農業危機後，北韓在2000年代初期遭遇到與中共在波灣戰爭後面臨的相同難局，當年中共顯然看出自己很容易被美國先進的武器科技所擊敗。北韓大體上採取三種方式因應此種難局：擴編特戰部隊以遂行非正規作戰；增加電子戰和訊號情報資產以遂行干擾行動；最重要的則是在121局、91號辦公室和110號實驗室主導下發展戰術與戰略網路作戰。[17] 如同北韓的其他面向一樣，這些祕密組織的相關資訊都非常難以查證。

外界廣泛報導北韓軍隊的駭客，曾在中國大陸瀋陽的七寶山飯店(攝於2005年4月17日)作業，北韓擁有該飯店的部分股權。此類報導有其可能性，部分原因在於從中國大陸境內運作的明顯優點，諸如可快速獲得多條通信線路，更別提還有現代化設備、訓練、後勤支援和可靠的電力。(See, for example, James Cook, ee, for example, Jamesxury Chinese Hotel Where North Korea Keeps Its Army of Hackers," Business Insider website, 2 December 2014, accessed 12 June 2017, http://www.businessinsider.com/photos-chinese-hotel-where-north-korea-keeps-hackers-2014-12).

(Source: Flickr/tack well)

北韓網路組織

據報導指出，121局、91號辦公室和110號實驗室隸屬總參謀部轄下專門從事情報蒐集之「偵察總局」(Reconnaissance General Bureau, RGB)中六個局的成員。施道安(Andrew Scobell)和桑福(John M. Sanford)指出，雖然總參謀部負責北韓人民軍的指管，但卻是人民武裝部隊部(Ministry of People's Armed Forces, MPAF)的所屬機關。[18] 此種安排讓偵察總局可以從指揮鏈最高層進行直接作戰管制，以確保網路部隊可以獨立遂行作戰，支援朝鮮人民軍的作戰需求。

121局據悉由情報蒐集部門和攻擊部門所組成。該單位被認定主要以平壤與大陸瀋陽的七寶山飯店為基地進行運作。[19] 91號辦公室據信是以平壤為基地執行偵察總局所交待的駭客行動。[20] 110號實驗室據信是透過駭客攻擊及將電腦病毒植入敵方網路，遂行技術偵察、電腦網路入侵和情報蒐集。[21]

雖然北韓內部似乎還有許多其他的網路組織，但偵察總局以外的單位主要是從事內部政治控制，或對其他國家散播政治宣傳。因此，渠等任務跟戰術或野戰層級戰鬥行動的作戰網路支援關係甚微。

研判北韓網路部隊的編制人數可能有1,800名到近6,000名駭客和電腦專家，使其擁有僅次於美國和俄羅斯的第三大網路機關。[22]較高人數判斷據悉來自2015年初的南韓情資，但該數據無法獲得證明。此外，該統計數字是否包含91號辦公室和110號實驗室亦無從得知，但由於南韓希望影響美國將北韓網路威脅視為優先處理對象，因此這兩個單位的人數可能也包含在內(某些人認為南韓的研判數據偏頗而不夠精確)。此外，南韓是根據2013年的數據做出研判，如同其他有關北韓的相關情資一樣，早已過時。

不論如何，對於北韓網路組織缺乏具體瞭解，還因為其網際網路使用管道的本質而變得更不明確。北韓將網路區隔為兩個部分。只有政府和軍事機關可以使用以中國大陸為中繼的對外網路，北韓駭客就是用此一網路遂行網路攻擊。另一個部分則是僅有當局選定內容且嚴密監控內部網路的「光明網」。[23] 2013年1月，據悉北韓在平壤開設了一家「網咖」，但一般民眾在這家網咖還是只能使用光明網。[24] 使用中國大陸網路連結全球網際網路，讓北韓駭客擁有可否認其網路入侵和攻擊行為責任的緩衝地帶。此外，北韓駭客還能安全地進行對外攻擊，同時避免南韓和美國對其進行攻擊。[25]

然而，利用第三方作為對外網際網路管道，也使北韓網路行動必須依賴中共及其他夥伴的持續合作。儘管近年來這個孤立國度的支持度不斷降低，但中共的支持似乎在平時仍然十分穩固。只是萬一戰爭爆發，就不保證其還會支持北韓了。

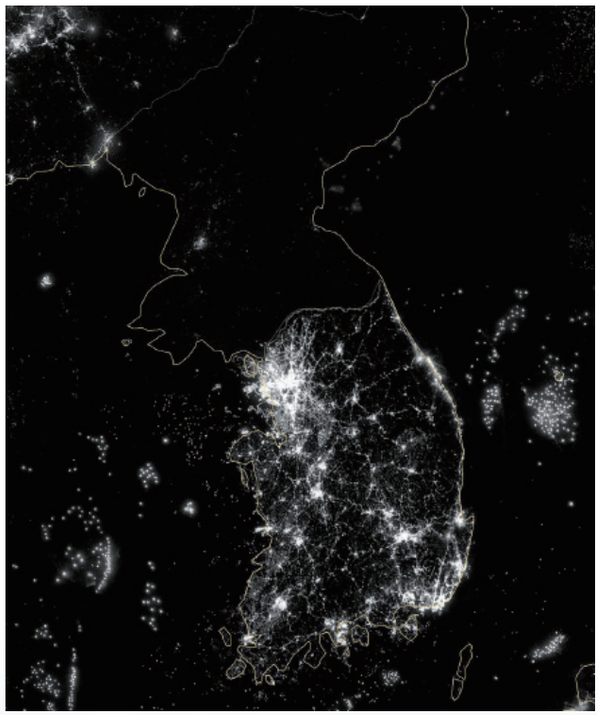
由於連結程度低可以發揮防護外來攻擊的效果，北韓因而可以將重點放在發展攻擊性網路戰力。即便遭到損害，也幾乎無多少北韓的系統或網路作戰能力會遭到削弱。[26] 北韓駭客的多次高調網路攻擊，主要都是為達成其戰略與政治訴求。然而，在全面戰爭爆發時，對戰鬥部隊的網路支援極可能仍是北韓戰略之重要環節。

網路戰具有其特殊性，在任何新方法或技術用於網路攻擊後，受害者可以在短時間內發展出反制措施，以防範未來類似攻擊。可能基於這個理由，北韓不曾(且極可能不會)在戰爭尚未爆發時，對南韓或美國實施大規模戰術或野戰層級的網路攻擊。相反地，北韓只針對敵人的網路進行小規模偵察或測試各種網攻方法。這種作法可降低敵人發展出反制措施，削弱北韓在全面戰爭時所望確保之優勢。

雖然美國及其夥伴國部隊對於北韓網路戰力所知極為有限，但可以利用中共和俄羅斯作為研究北韓的模式。身為北韓最緊密(且可能是唯一)盟友的中共，不僅提供北韓網路部隊對外的網路連結，還提供其作業基地(諸如七寶山飯店)和訓練。目前已知中共的網路行動主要都是以科技間諜活動為重點，北韓在某種程度上可能對此沒有太大興趣，因為其缺乏中共擁有製造或維護先進科技武器所需之基礎設施。相較之下，俄羅斯在2008年入侵喬治亞和2014年對烏克蘭的軍事行動所採取之網路活動，都可以看出北韓未來在朝鮮半島戰爭爆發時，極可能會採取那些戰術層級的網路行動。

北韓戰術層級的作戰網路支援

雖然朝鮮半島的陸、海、空戰爆發(或升高危機)會發生在某個特定日期和時間，但在開第一槍之前網路戰應該就已經開始很久了。[27] 吾人可以說，對北韓的網路戰早就已經開打，因此在全面戰爭爆發前必須增加網路偵測和攻擊的頻率和強度，才能有效支援傳統戰鬥部隊的行動。在戰



夜間衛星照片之南北韓比較。科技落後問題據悉已迫使北韓軍方駭客尋找境外地點作業，諸如中國大陸的七寶山飯店，以便在這些地方迅速取得科技和通信線遂行網路攻擊。(Source: NASA)

爭準備及其初期階段，北韓不對稱網路部隊應會利用單純的阻斷服務方式攻擊民間通信。

俄羅斯在2008年派兵越界入侵前數週，就已對喬治亞發動「分散式阻斷服務」(Distributed Denial of Service, DDoS)，以驗證其能力並對喬治亞網路進行偵測，俾規劃後續的攻擊行動。俄羅斯攻擊喬治亞的通信、癱瘓政府傳達與協調反制俄軍入侵的能力。[28] 俄羅斯的網路攻擊在執行方面結合了簡潔和精密度；如此一來俄羅斯就能以低廉代價癱瘓喬治亞的指揮和通信。原本情報單位和空中武力必須耗時數日(甚或數週)進行的轟

炸和協調作為，但利用安全無虞的俄羅斯電腦，只要花幾分鐘就能達到相同效果。美國及其夥伴國部隊可以合理推斷，像北韓這種科技落後且海空兵力落伍的國家，應該會採取類似攻擊手段。

再者，北韓似乎也已證明自己具備這種能力。從2014至2016年，北韓據悉曾對「超過14萬部」屬於南韓政府和企業的電腦進行駭客攻擊，還試圖攻擊南韓運輸系統的控制網路。[29] 這些極可能由121局所發動的網路攻擊行動，使北韓能接觸並監控南韓政府與企業的通信內容。

如果此種情況發生在南侵之時，北韓應該會癱瘓這14萬部電腦，使這些組織完全喪失通信能力。其也可能會關閉或澈底擾亂南韓的運輸網路。

此類攻擊若提高其範圍和攻擊性，將會完全切斷南韓通信及其軍方的資訊分享能力。若配合特戰部隊摧毀南韓的實體通信系統，則北韓就可能癱瘓韓美之通聯，讓戰場上的部隊陷於盲目狀態。在戰爭初期階段切斷通信功能，將大幅削弱韓美協調砲兵和空中資產的能力，讓北韓軍隊取得澈底擊潰非軍事區南韓及美國聯軍的時間和空間。

雖然北韓攻擊南韓通信和重要網路會阻礙南韓及美國的行動，但兩國仍有其他替代通信手段可以反制北韓的侵略行動。然而，北韓可以攻擊南韓電力網以瓦解關鍵的備援通信手段，如此可能拖延兩國適時對侵略採取協同行動，而降低韓美聯軍對北韓軍隊的優勢。多年前，像北韓這樣科技落後的國家，此種攻擊行動必然會被視為不可能發生。但今日幾乎已能確定北韓在戰爭爆發時必然採取此類攻擊。

例如，俄羅斯駭客在2015年12月就是以網路攻擊造成烏克蘭大停電。他們先在烏國發電廠網路中植入惡意程式，並以遠端操蹤斷電裝置，切斷22萬5,000名居民的電力供應。[30] 俄羅斯接著又以假冒電話取代烏克蘭水電服務專線，以防止水電公司接到真正的客戶投訴。[31]

2013年4月13日，平壤萬景臺革命學院學生在學習電腦。該校係由北韓軍方設立，而校方行政人員表示其在1947年成立時，原本是用於收容為對抗日本佔領軍之朝鮮解放戰爭中喪失雙親的兒童。(Source: AP)

考量北韓網路機關似乎已經擁有技術純熟度，還有依照北韓與俄羅斯的關係，其極可能獲得俄羅斯支援，以利在未來對南韓電廠發動類似攻擊。

基本上，網路攻擊是彌補北韓幾乎已消失空中武力的不對稱方法。其能對南韓戰術與野戰層級造成損害，以強化北韓在南侵時發動「震撼與威懾」砲戰的效果。藉由癱瘓重要通信、運輸和支援基礎設施，北韓可引發南韓的慌亂與失序，以掩護其正規步兵部隊擊潰南韓及美國聯軍。

儘管如此，雖然這些方法相當有效，但121局不太可能有辦法完全癱瘓南韓的網路，不過局部性網路中斷運作仍可能嚴重妨礙南韓及美國在戰場上的行動。為了完全消弭韓美兩國的科技優勢，北韓必須採取更精密的網路攻擊，對付全球衛星定位系統、雷達、後勤支援系統和武器鎖定系統。北韓採取此類攻擊的確切方式為何並不在本文討論範圍。然而，仍必須嚴肅看待此種威脅，國防科學委員會(Defense Science Board)曾提出警告，「當美國本身和實力匹敵對手爆發全面性衝突時……美國的火砲、飛彈和炸彈可能無法發射，甚或將目標誤指成自身部隊。包含糧食、飲水、彈藥和油料等補給品，都可能無法適時送達需求地點。」[32]

雷達和全球衛星定位系統遭駭客攻擊或癱瘓，即便韓美聯軍能在幾天內修復，仍將使空中武力完全停擺，讓北韓部隊在戰場上獲得行動自由。此外，全球衛星定位系統中斷不僅會造成無法使用全球衛星定位系統導引的武器系統，但更危險的是會造成武器射向錯誤座標。美國衛星遭駭客攻擊(據悉中共已展現此種能力)將造成南韓及美國情報機關完全無法掌握北韓的地面機動狀況。[33]

如果北韓對支援朝鮮半島韓美聯軍的自動化後勤網路進行駭客攻擊，聯軍將很難維持作戰能力。一場單純分散式阻斷服務攻擊，只要藉著關閉系統或損害資料，就可以擾亂所有基本作戰補給品的追蹤、申請及運送作業，導致後勤補給品運送錯誤。南韓及美國聯軍很快就會發現自己沒有作戰所需的資源。

因此，北韓可以運用網路攻擊，以確保數量優勢和壓倒性火力能以劣勢取得勝利。若再搭配電子戰和主戰部隊後方潛伏的特戰部隊，此種方式將如《超限戰》一書的想法，造成南韓及美國聯軍喪失動能，陷於守勢和被動態勢。

《超限戰》提出「黃金比例」和「邊緣主角」(side-principal)兩大定律。其想法是0.618或約三分之二的黃金比例，雖然通常用於藝術、建築和數學，但也可用於戰爭。兩位作者指出，伊拉克軍隊在遭美空軍削弱至僅剩原有戰力的0.618時，便宣告崩潰且戰爭也結束了。[34] 邊緣主角定律基本上認為可透過非戰爭行為贏得戰爭。若同時思考這兩種想法，便可明顯看出，中共雖然不認為自己可以用傳統戰鬥在戰爭中擊敗美國，但卻認為若非戰爭行動可用於削弱美軍實力至原有戰力的三分之二，就有可能擊敗美國。

對中共而言，達成此一目的之選項很多，因為其已擁有愈來愈多的資源，可用於執行長期非戰爭行動，不論在網路、金融或政治上皆然。對於北韓而

言，基於達成「國家目標」的訴求和極端有限之資源，選項就相對要少得多。北韓很可能會將黃金比例和邊緣主角定律，解讀為透過網路攻擊，結合無數其他不對稱手段，達到擊滅三分之一南韓及美國聯軍之目的。在系統遭癱或損害時，美國和南韓的作戰能力會遭到嚴重削弱或阻礙，以致北韓軍隊理論上能藉機發動大規模地面進犯。因此，網路攻擊是一種北韓極可能用於攻擊敵軍作戰支援系統的手段，藉此讓其數量優勢軍隊可以獲得在半島發動戰爭的空間、時間及行動自由。

網路攻擊還可搭配核彈製造電磁脈衝，癱瘓半徑450哩範圍內的所有電子裝置。[35]理論上，北韓可以在30哩高度的大氣層引爆核彈來製造此種效果。這種攻擊將使朝鮮半島的友軍部隊喪失科技優勢，造成使用電子元件的裝備完全無法使用。然而，由於核武報復的威脅，以及美國愈來愈可能支持打長期戰爭，最後極可能導致北韓遭澈底消滅，因此這種選項或許仍是不使用戰術核武攻擊的最後手段。

反制北韓網路戰力的解決方案

北韓領導階層可能相信，藉由網路戰力取得優勢，其能改變現有的戰術兵力平衡回到1950年代情況。在1950年6月時，美軍地面戰術部隊難堪地遭到訓練、裝備和戰備水準都不如美軍具數量優勢的敵軍擊敗。隨著美國持續從南韓撤出長駐戰鬥部隊並轉為扮演支援角色，駐朝鮮半島美軍已完全無法從事大規模防禦行動，美國應採取行動避免讓自己陷於類似1950年時的情況。

北韓的網路戰力並非毫無弱點。美國在2014年為報復索尼公司遭到駭客攻擊的事件，就曾對北韓發動分散式阻斷服務攻擊，造成光明網癱瘓。[36]然而，該次報復行動並未針對北韓網路機關(多數均以中國大陸為基地)，而只是癱瘓其內部網路。此次行動凸顯出北韓在全面戰爭中的一項重大弱點。北韓網路戰力完全得看中共的臉色。一旦中共認為在政治上已無法繼續支持北韓時，北韓的網路能力就將遭到大幅削弱。

為消弭北韓網路威脅的風險，美陸軍應積極與南韓部隊合作，重新評估渠等看待網路作戰的方式。為了預防萬一，美陸軍網路機關應嚴密監控在南韓境內與即將部署至南韓單位的網路，因為這些單位最可能成為北韓網路機關的攻擊目標。美陸軍領導階層不應主動移除所有已確認之北韓網路威脅，而是應評估容許敵人有限行動自由可獲得之情報利益，以研究敵軍在網路領域的戰術、技術與程序。

同時，美陸軍高層應開始從攻勢與守勢角度，深入研究如何將網路戰發展成兵力倍增器，而非視其為戰術或野戰層級外的項目。此外，駐韓的美陸軍部隊應與南韓部隊發展應變計畫，預判北韓可能發動類似本文所述之網路攻擊，同時應在網路戰環境下遂行訓練。美國與南韓部隊可透過此種方式，消弭來自北韓網軍的嚴重威脅。

作者簡介

Scott J. Tosi陸軍中尉現任第902軍事情報大隊第310軍事情報營第1連副連長。過去曾任駐韓(龍山區)美軍第501軍事情報旅旅部連副連長。他擁有伊利諾州立大學歷史與社會學教育學士，曾在伊利諾州布隆明頓的中學任教歷史與公民。

註釋

1. Jason Andress and Steve Winterfield, *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners,* 2nd ed. (Waltham, MA: Syngress, 2013), 73. Andress and Winterfield cite Jung Kwon Ho, "Mecca for North Korean Hackers," Daily NK online, 13 July 2009.
2. Clyde Stanhope, "How Bad is the North Korean Cyber Threat," Hackread website, 20 July 2016, accessed 2 May 2017, https://www.hackread.com/how-bad-is-the-north-korean-cyber-threat/; Office of the Secretary of Defense (OSD), "Military and Security Developments Involving the Democratic People's Republic of Korea: 2015," A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2012, accessed 4 May 2017, https://www.defense.gov/Portals/1/Documents/pubs/Military_and_Security_Developments_Involving_the_Democratic_Peoples_Republic_of_Korea_2015.PDF.
3. James M. Minnich, *The North Korean People's Army: Origins and Current Tactics* (Annapolis, MD: Naval Institute Press, 2005), 68.
4. Ibid.
5. OSD, "Military and Security Developments Involving the Democratic People's Republic of Korea: 2012," A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2012, 15 February 2013, accessed 6 May 2017, http://archive.defense.gov/pubs/Report_to_Congress_on_Military_and_Security_Developments_Involving_the_DPRK.pdf.
6. Daniel Wagner and Michael Doyle, "Scenarios for Conflict Between the Koreas," Huffington Post, 25 February 2012, accessed 2 May 2017, http://www.huffingtonpost.com/daniel-wagner/scenarios-for-conflict-be_b_1169871.html.
7. Minnich, *The North Korean People's Army,* 53–54.
8. Ibid., 73.
9. Ibid., 73–74.
10. Ibid.; Blaine Harden, "North Korea Massively Increases Its Special Forces," *Washington Post* website, 9 October 2009, accessed 3 May 2017, http://www.washingtonpost.com/wp-dyn/content/article/2009/10/08/AR2009100804018.html; OSD, "Military and Security Developments Involving the Democratic People's Republic of Korea: 2015."
11. Joseph Bermudez, *North Korea's Development of a Nuclear Weapons Strategy* (Washington, DC: US-Korea Institute at SAIS [Johns Hopkins School of Advanced International Studies], August 2015), accessed 4 May 2017, http://uskoreainstitute.org/wp-content/uploads/2016/02/NKNF_Nuclear-Weapons-Strategy_Bermudez.pdf.
12. Ibid.
13. Ibid.
14. James M. Broder and Douglas Jehl, "Iraqi Army: World's 5th Largest but Full of Vital Weaknesses," *Los Angeles Times* online, 13 August 1990, accessed 8 May 2017, http://articles.latimes.com/1990-08-13/news/mn-465_1_iraqi-army.
15. Richard A. Clarke and Robert Knake, *Cyber War: The Next Threat to National Security and What to Do about It* (New York: HarperCollins, 2010), 28–29; Qiao Liang and Wang Xiangsui, *Unrestricted Warfare: China's Master Plan to Destroy America,* summary translation (Panama City, Panama: Pan American Publishing, 2002).
16. Clarke and Knake, *Cyber War,* 30–32.
17. Harden, "North Korea Massively Increases Its Special Forces"; Stanhope, "How Bad is the North Korean Cyber Threat."
18. Andrew Scobell and John M. Sanford, *North Korea's Military Threat: Pyongyang's Conventional Forces, Weapons of Mass Destruction, and Ballistic Missiles* (Carlisle, PA: Strategic Studies Institute, 2007), 14–16; Hewlett-Packard [HP] Enterprise SR [Security Research]-FI_Team, "Profiling an Enigma: The Mystery of North Korea's Cyber Threat Landscape," HP Security Briefing, Episode 16, August 2014, HP Enterprise Community website, accessed 6 May 2017, http://community.hpe.com/hpeb/attachments/hpeb/off-by-on-software-security-blog/388/2/HPSR%20SecurityBriefing_Episode16_NorthKorea.pdf.
19. SR_Fl Team, "Profiling an Enigma: The Mystery of North Korea's Cyber Threat Landscape."

20. Pierluigi Paganini, "Concerns Mount over North Korean Cyber Warfare Capabilities," Infosec Island website, 11 June 2012, accessed 14 February 2017, http://www.infosecisland.com/blogview/21577-Concerns-Mount-over-North-Korean-Cyber-Warfare-Capabilities.html.
21. "North Korea Launched Cyber Attacks, Says South," *The Guardian* website, 11 July 2009, accessed 4 May 2017, https://www.theguardian.com/world/2009/jul/11/south-korea-blames-north-korea-cyber-attacks.
22. Ju-min Park and James Pearson, "In North Korea, Hackers are a Handpicked, Pampered Elite," Reuters website, 5 December 2014, accessed 6 May 2017, http://www.reuters.com/article/us-sony-cybersecurity-northkorea-idUSKCN0JJ08B20141205; Darren Pauli, "NORKS Hacker Corps Reaches 5,900 Sworn Cyber Soldiers—Report," The Register website, 7 July 2014, accessed 6 May 2017, http://www.theregister.co.uk/2014/07/07/north_korea_employs_6000_leet_hackers_source_claims/.
23. Ashley Moreno, "Social Media in North Korea: The AP Bureau Chief from Pyongyang on Cell Service, Instagram, Etc.," *Austin Chronicle* website, 11 March 2013, accessed 4 May 2017, http://www.austinchronicle.com/daily/sxsw/2013-03-11/social-media-in-north-korea/.
24. Olga Khazan, "North Koreans Shouldn't Count on Using the New Google Maps," *Washington Post* website, 29 January 2013, accessed 3 May 2017, https://www.washingtonpost.com/news/worldviews/wp/2013/01/29/north-koreans-shouldnt-count-on-using-the-new-google-maps/.
25. OSD, "Military and Security Developments Involving the Democratic People's Republic of Korea: 2015."
26. Duk-Ki Kim, "The Republic of Korea's Counter-Asymmetric Strategy," *Naval War College Review* 65, no. 1 (Winter 2012): 68, accessed 8 May 2017, https://www.usnwc.edu/getattachment/8e487165-a3ef-4ebc-83ce-0ddd7898e16a/The-Republic-of-Korea-s-Counter-asymmetric-Strateg.aspx.
27. For another perspective on North Korean cyber war, see Kim, "The Republic of Korea's Counter-Asymmetric Strategy," 58.
28. John Markoff, "Before the Gunfire, Cyberattacks," *New York Times* website, 12 August 2008, accessed 3 May 2017, http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=0.
29. Jack Kim, "North Korea Mounts Long-Running Hack of South Korea Computers, Says Seoul," Reuters website, 13 June 2016, accessed 14 February 2017, http://www.reuters.com/article/us-northkorea-southkorea-cyber-idUSKCN0YZ0BE.
30. Dustin Volz, "U.S. Government Concludes Cyber Attack Caused Ukraine Power Outage," Reuters website, 25 February 2016, accessed 14 February 2017, http://www.reuters.com/article/us-ukraine-cybersecurity-idUSKCN0VY30K.
31. Ibid.
32. Defense Science Board, Task Force Report: *Resilient Military Systems and the Advanced Cyber Threat* (Washington, DC: Office of the Undersecretary of Defense for Acquisition, Technology and Logistics, January 2013), 5, accessed 3 May 2017, http://www.dtic.mil/docs/citations/ADA569975.
33. Mary Pat Flaherty, Jason Samenow, and Lisa Rein, "Chinese Hack U.S. Weather Systems, Satellite Network," *Washington Post* website, 12 November 2014, accessed 3 May 2017, https://www.washingtonpost.com/local/chinese-hack-us-weather-systems-satellite-network/2014/11/12/bef1206a-68e9-11e4-b053-65cea7903f2e_story.html.
34. Qiao Liang and Wang Xiangsui, *Unrestricted Warfare: China's Master Plan to Destroy America,* 153–69.
35. Andress and Winterfield, *Cyber Warfare,* 147.
36. Cecilia Kang, "North Korean Web Goes Dark Days after Obama Pledges Response to Sony Hack," *Washington Post* website, 22 December 2014, accessed 3 May 2017, https://www.washingtonpost.com/business/economy/north-korean-web-goes-dark-days-after-obama-pledges-response-to-sony-hack/2014/12/22/b76fa0a0-8a1d-11e4-9e8d-0c687bc18da4_story.html.