網際空間特種作戰的戰略發展

Strategic Development of Special Warfare in Cyberspace

譯者簡介

鄧炘傑備役少校，管院專9期、國防大學政治作戰學院英文正規班、中原大學企管研究所碩士；曾任排長、連長、地區補給庫分庫長、教準部編譯官，現任特約翻譯、華語／英語專業領隊／導遊。

Today, small teams of special operators armed with asymmetric cyber-tools, irregular warfare tactics, and mass disinformation can have truly strategic effects. -General Joseph L. Votel, USA[1]

今天，擁有不對稱網際工具，採用非正規戰術，大量散布假消息的特戰小組，足以產生真正的戰略效果。-----美軍上將Joseph L. Votel[1]

Why are regional powers such as Iran and Russia better prepared for cyber-enabled special warfare operations than the United States? How do Iran and Russia empower their tactical operators, while the United States masses its cyber-authorities and cyber-capabilities at the strategic level? Why are U.S. policies, authorities, and doctrine for cyber-enabled special operations so immature despite their first announcement over 20 years ago ?[2] Although these

1 General Joseph L. Votel, USA, commander of U.S. Special Operations Command, email correspondence with author, December 18, 2014.

2 於下頁。

are serious questions, what is even graver for the Nation is addressing the root question: How does the United States develop a strategic cyber-enabled special warfare capability?

為什麼像伊朗、俄羅斯這類地區性強權，在網際特種作戰方面，會做得比美國好呢？當美國將網際網路相關權責單位及其能力集中於戰略層級之際，伊朗和俄羅斯又是如何強化其戰術層級的運作？早在20多年前就已經起步，但是美國在網路化特種作戰方面的政策、權責區分和準則發展，為何還是未臻成熟？[2]雖然以上這些都是嚴肅的問題，但是對美國而言，最值得深思的還是這個根本性的問題：美國應如何發展戰略性的網路化特種作戰能力？

As far back as 1993, cyber-thinkers John Arquilla and David Ronfeldt in their seminal study Cyberwar Is Coming! fore-shadowed recent cyber-special operations forces (SOF) actions by Iran and Russia. The prescient notion that "numerous dispersed small groups using the latest communications technologies could act conjointly"[3] to master networks and achieve a decisive advantage over their adversaries has been played out repeatedly. As predicted by Arquilla and Ronfeldt, "We're no longer just hurling mass and energy at our opponents in warfare; now we're using information, and the more you have, the less of the older kind of weapons you need."[4] As senior leaders have recently recognized, groups of special operators armed with asymmetric cyber tools, irregular warfare tactics, and mass disinformation can have strategic effects.[5]

時間拉回到1993年，網路思想家約翰・阿奇拉和大衛・朗費德在他們深入淺出的論文〈網路戰爭已經來臨！〉中就已經預言今日伊朗和俄羅斯在建置網路化特戰部隊的相關作為。該文提到：分散各處的許多小單位，只要運用最新通訊科技就能整合行動。[3]

2 Maren Leed, Offensive Cyber Capabilities at the Operational Level: The Way Ahead (Washington, DC: Center for Strategic and International Studies and Georgia Tech Research Institute, 2013), 12, available at 〈http://csis.org/files/publication/130916_Leed_OffensiveCyberCapabilities_Web.pdf〉.

3 John Arquilla and David Ronfeldt, eds., Networks and Netwars: The Future of Terror, Crime, and Militancy (Santa Monica, CA: RAND, 2001), 2, available at 〈www.prgs.edu/ content/dam/rand/pubs/monograph_reports/MR1382/MR1382.ch1.pdf〉.

4 Tom Gjelten, "First Strike: U.S. Cyber Warriors Seize the Offensive," World Affairs (January-February 2013), 1-2, available at 〈www.worldaffairsjournal.org/article/firststrike-us-cyber-warriors-seize-offensive〉.

5 Votel.

這種掌握網際網路的概念，可以一再展現完勝敵手的絕對優勢。就像阿奇拉和朗費德所預期的，「我們不再需要大量的有形力量來對付敵人；資訊科技用得愈多，傳統武器相對需求就愈少」。[4]就像資深幹部最近學到的，擁有不對稱網際工具，採用非正規戰術，大量散布假消息的特戰小組，足以產生真正的戰略效果。[5]

This article argues that Iran and Russia have already successfully employed cyber-enabled special warfare as a strategic tool to accomplish their national objectives. Both countries have integrated cyber-SOF that clearly demonstrate they understand how to leverage this tool's potential within the asymmetric nature of conflict. The countries' asymmetric innovations serve as powerful examples of an irregular pathway for aspiring regional powers to circumvent U.S. military dominance and secure their strategic interests.[6] The diffusion of inexpensive yet sophisticated technology makes it easier for potential adversaries to develop significant capabilities every year. Thus, the time has come for the United States to make a strategic choice to develop cyber-enabled special warfare as an instrument to protect and project its own national interests.

本文認為伊朗和俄羅斯已經可以成功地運用網路化特戰方式作為戰略工具，達成其國家目標。這兩個國家將網路與特戰部隊結合，展現出他們已經能掌握衝突的不對稱特性，發揮此一工具的強大潛力。這些國家針對不對稱的創新作為，為世界各地區強權開啟了足以抵銷美國軍事優勢的非正規管道，進而保障他們的戰略利益。[6]這類廉價又不甚複雜的技術持續擴散，使得美國的潛在敵人更形茁壯，也一年比一年容易。因此，對美國來說，做出戰略性抉擇發展網路化特種作戰，作為保護並擴張美國國家利益的手段，已經刻不容緩。

Russia

In February 2013, Russian Chief of the General Staff Valery Gerasimov published an article titled "The Value of Science in Prediction" in the obscure military journal Military-Industrial Courier. In the article, General Gerasimov heralded a game-changing new generation

6 Dan Madden et al., Special Warfare: The Missing Middle in U.S. Coercive Options (Santa Monica, CA: RAND, 2014), 1-4.

of warfare whose strategic value would exceed the "power of force of weapons in their effectiveness."[7] He called for widespread asymmetric actions to nullify enemy advantages through "special-operations forces and internal opposition to create a permanently operating front through the entire territory of the enemy state, as well as informational actions, devices, and means that are constantly being perfected."[8]

俄羅斯

2013年2月，俄羅斯參謀總長瓦拉利・格拉西莫夫在素以艱澀難懂著稱的軍事期刊《軍事工業宅急便》中刊出了一篇文章，標題是「科學價值之預言」；格拉西莫夫上將在文中預告，下一個世代將產生一種改變規則的作戰方式，而其戰略價值將超越軍事武器。[7]他表示，「運用特種作戰部隊和(敵人)內部的反對勢力，透過不斷更新的資訊作戰、工具及手段，可以在整個敵境建立永久性的戰爭面」。而透過這些不對稱的手法，可以有效癱瘓敵人的既有優勢。[8]

In spring 2014, Russia successfully demonstrated its new understanding of how to integrate asymmetric technology into unconventional warfare (UW) operations by supporting paramilitary separatists in eastern Ukraine.[9] Russia dispatched small teams of unmarked Spetsnaz, or special forces, across the Ukrainian border to seize government buildings and weapons armories, and then turn them over to pro-Russian separatist militias.[10] Concurrently, Russia disconnected, jammed, and attacked digital, telephone, and cyber communications throughout Ukraine. Russia enlisted virtual "privateers" and bounty hunters to conduct cyber attacks against Ukrainian government information and logistic infrastructure, from Internet

7 Valery Gerasimov, "The Value of Science in Prediction," Military-Industrial Courier, February 27-March 5, 2013.

8 Towards the Next Defense and Security Review: Part Two-NATO, HC 358 (London: House of Commons Defense Committee, August 5, 2014), 13.

9 U.S. Army doctrine defines unconventional warfare as "activities conducted to enable a resistance movement or insurgency to coerce, disrupt, or overthrow a government or occupying power by operating through or withan underground, auxiliary, and guerrilla force in a denied area." See Army Doctrine Reference Publication 3-05, Special Operations (Washington, DC: Headquarters Department of the Army, August 31, 2012), 1-5.

10 Michael Gordon, "Russia Displays a New Military Prowess in Ukraine's East," New York Times, April 24, 2014, 2.

servers to railway control systems.[11] Russia bankrolled a "troll army" to wage deza, a Russian hacktivist term for disinformation, paying millions for each troll to post 50 pro-Russian comments a day on social media, blogs, and news sites that were critical of Russia's actions.[12] Russia surged epic streams of disinformation, both inside and outside Ukraine, not only to obscure its cyber-enabled UW campaign, but also to create complete political illusions: "Russia doesn't deal in petty disinformation, forgeries, lies, leaks, and cyber-sabotage usually associated with informational warfare……It reinvents reality, creating mass hallucinations that translate into political action."[13]

2014年春天，俄羅斯藉著對東烏克蘭準軍事性分離主義分子的支持，向世人展示他們已經知道如何將非對稱性技術，整合到非常規(UW)作戰之中。[9]俄羅斯先派遣便裝特戰人員，沿著烏克蘭邊境，控制了政府組織的建築物和軍械庫，再把這些設施移交給支持俄羅斯的分離主義民兵組織[10]。同一時間，俄羅斯將烏克蘭全境的電話、電子和網路通訊等，全部加以攻擊、干擾和截斷。俄羅斯還徵募了一批「武裝商船」(譯註：或譯為「私掠船」，指戰時特准掠捕敵方商用船隻的武裝民船)和賞金獵人，對烏克蘭政府網路伺服器、鐵道控制系統等資訊設施和物流基礎建設，實施網路攻擊。[11]此外，俄羅斯還資助網路駭客，只要每天在社群媒體、部落格和新聞網站上貼出50則對俄羅斯有利的訊息，就可以獲得數以百萬的獎金。[12]這些在烏克蘭境內、境外如排山倒海一般出現的資訊，不但掩蓋了俄羅斯藉著網路發起的非正規作戰行動，還企圖建立群眾的政治性錯覺：俄羅斯不會用資訊戰常用的造假、謊言、爆料等負面資訊或網路破壞，來達成他們資訊作戰的目的……。但這一連串做法的真相是，要造成社會大眾的錯誤認知，以創造出俄羅斯政治性行動的正當性。[13]

In response, during a North Atlantic Treaty Organization (NATO) security summit in September 2014, the Supreme Allied Commander Europe, General Phillip Breedlove, USAF,

11 Tom Fox-Brewster, "Russian Malware Used by 'Privateer' Hackers Against Ukrainian Government," The Guardian (London), September 25, 2014, 1-2.

12 Misha Japaridze, "Inside Russia's Disinformation Campaign," DefenseOne.com, August 12, 2014, available at 〈www.defenseone.com/ technology/2014/08/inside-russias-disinformation-campaign/91286/〉.

13 Peter Pomerantsev, "How Russia Is Revolutionizing Information Warfare," DefenseOne.com, September 9, 2014, available at 〈www.defenseone.com/threats/2014/09/ how-russia-revolutionizing-information-warfare/93635/〉.

proclaimed that Russia's "hybridized" UW in eastern Ukraine represented "the most amazing information warfare blitzkrieg we have ever seen in the history of information warfare."[14] General Breedlove urged the Alliance to develop new capabilities to counter Russia's mastery of UW, propaganda campaigns, and cyber assaults immediately.[15] NATO and the West were caught off guard by Russia's ability to advance its political objectives using nontraditional means in a manner once "not even considered warfare by the West."[16]

2014年9月，北約組織(NATO)為了因應相關局勢變化，召開了一次安全高峰會。會中，歐洲盟軍統帥美國空軍上將飛利浦・布利德洛夫就公開表明，俄羅斯在東烏克蘭採取的「混種」非正規作戰，「在資訊作戰史上，是我們所見過最驚人的資訊閃擊戰」。[14]布利德洛夫上將會中呼籲盟軍立即針對俄羅斯的非正規戰、宣傳戰和網路突襲，研擬反制新方法。[15]俄羅斯以非傳統手段達成其政治目的的能力，「採用的戰法，某種程度上西方想都沒想過」，北約組織和西方國家一時嚇得有點不知所措。[16]

Russia did not use Spetsnaz, information operations (IO), or cyber capabilities in a piecemeal manner to accomplish its objectives. Instead, as General Gerasimov described, "Wars are no longer declared"; they simply happen when SOF armed with advanced technology and mass information create the conditions for conventional forces to achieve strategic objectives "under the guise of peacekeeping and crisis."[17] In other words, choreographed cyber disinformation and cyber attack bought time and space for laptop-carrying Spetsnaz to conduct unconventional warfare "between the states of war and peace."[18] Russia's cybere-nabled UW was a brilliant success, not simply for its cyber-SOF hybridization, but also for successfully invading a signature partner nation of the European Union without sparking any meaningful

14 John Vandiver, "SACEUR: Allies Must Prepare for Russia 'Hybrid War,'" Stars and Stripes, September 6, 2014, available at 〈www. stripes.com/news/saceur-allies-must-preparefor-russia-hybrid-war-1.301464〉.

15 Ibid.

16 "Cyber Security Pro: Finland Under Hybrid Warfare Attack," Yle.fi, September 13, 2014, available at 〈http://yle.fi/uutiset/ cyber_security_pro_finland_under_hybrid_warfare_attack/7470050〉.

17 Robert Coalson, "Top Russian General Lays Bare Putin's Plan for Ukraine," World Post, September 2, 2014, available at 〈www. huffingtonpost.com/robert-coalson/valerygerasimov-putin-ukraine_b_5748480.html〉.

18 Ibid.

Western military response.

俄羅斯特戰部隊與網路戰並非分別零星運用來達成其作戰目的，而是像布利德洛夫上將所形容的，「開戰已經不需要再作宣告」；當具備先進技術和掌握足夠資訊的特戰人員「在維護和平和危機處理的外衣之下」，為傳統部隊開創有利條件以達成戰略目標，一切就這麼發生了。[17]換句話說，事先寫好劇本的網路訊息和網路攻擊，為網路特攻戰士爭取了時間與空間，「在和戰混沌的狀態下」來遂行非傳統作戰。[18]俄羅斯透過網路遂行的非正規戰大獲全勝，不只因為有效地執行了網路化的特種作戰，還在於成功的入侵了歐洲聯盟國家，卻沒有引起西方的軍事反應與干預。

Iran

In summer 2009, the Iranian regime strangled the Green Movement with the very tools that were supposed to liberate it: information and communication technologies (ICTs). The regime exploited "emancipating" ICTs to target activists, induce fear, and expand military and paramilitary suppression of cyberspace.[19] Shortly after the Green Movement began, the government dispatched its Islamic Revolutionary Guard Corps (IRGC) to break the "counterrevolutionaries." Charged with fighting domestic and foreign threats to the regime, the IRGC mobilized its subordinate Basij cyber units and its notorious clandestine paramilitary wing, the IRGC-Quds Force (IRGC-QF). The IRGC commander, Major General Mohammad Ali Jafari, quickly restructured and integrated Iran's cyber, paramilitary, and clandestine capabilities into a brutal national tool to terrorize Green Movement dissidents into "inaction and passivity."[20]

伊朗

2009年夏天，伊朗政府採取非常嚴厲的手段扼殺發起「綠色革命」的反對勢力，一

19 Saeid Golkar, "Liberation or Suppression Technologies? The Internet, the Green Movement and the Regime in Iran," International Journal of Emerging Technologies and Society 9, no. 1 (May 2011), 50.

20 Mark Dubowitz and Matthew Levitt, Subcommittee on International Human Rights of the Standing Committee on Foreign Affairs and International Development, Statements, House of Commons Chambre Des Communes Canada, 41st Parliament, 1st sess., May 30, 2013, available at 〈www.parl.gc.ca/HousePublications/Publication.aspx?Mode=1&DocId=61 91680&Language=E〉.

般都認為採取的是資訊與通信技術(ICTs)手段。當局剝奪激進份子使用ICTs的權利，製造恐怖氣氛，同時擴大軍事或準軍事的網路制壓。[19]綠色革命剛開始不久，伊朗政府就派出伊斯蘭革命衛隊(IRGC)來打擊反動份子。為了打擊國內外威脅政府的反動勢力，革命衛隊調集了其附庸的青年志願軍(Basij)網路單位，以及神祕且惡名昭彰的準軍事側翼組織，革命衛隊聖城旅(IRGC-QF)。革命衛隊指揮官，穆罕默德・阿里・賈發里少將，迅速的改組並整合伊朗的網路、準軍事單位及地下組織，形成一股令人膽寒的國家勢力，鎮壓綠色革命反對勢力。[20]

The Basij used various devious cyber-intimidation methods against activists, such as sending threatening emails and Internet messages, publishing activists' photos and offering rewards for their capture on government Web sites, infiltrating social media networks, seeding disinformation, sowing leader mistrust, and staging false events to arrest people who showed up.[21] The Basij also institutionalized cyber skills on "blogging, social networking sites, psychological operations, online spying……mobile phones and their capabilities, and computer games with the aim of targeted entry in the virtual world."[22] In concert with Basij cyber-targeting activities, the IRGC-QF tracked, imprisoned, tortured, or assassinated regime threats.[23] Iran had set in motion a new symbiotic cycle of mis-attributable/non-attributable cyber-targeting activities married to old-fashioned brute force. Iran would subsequently strengthen its marriage of counterinsurgency (COIN) and cyber activities in Syria.

青年志願軍使用各種網路恐嚇的手段來打擊反政府份子，包括發送威脅信函、將激進份子的相片公布在政府網站以獎金懸賞、滲入社群媒體網絡散播不實消息、汙衊反政府領導人士，並羅織罪名加以逮捕。[21]青年志願軍將網路虛擬手法充分運用在部落格、社群網站，甚至結合心理戰和網路間諜；只要有行動電話在手，就可以像在電腦上玩遊戲一般鎖定真實世界的敵人。[22]當青年志願軍在網路上鎖定特定份子，革命衛隊聖城旅隨之加以追蹤、監禁、拷問或是暗殺。[23]伊朗現在已經建立起一套網路鎖定和實體行動相互配合的共生模式。之後，伊朗在敘利亞以網路與綏靖作戰之結合，會更上層樓。

21 Golkar, 62.

22 Ibid., 63.

23 Dubowitz and Levitt, 2.

Syria

In 2012, Iran dispatched IRGC-QF operators and ICT experts, who had mastered their craft in breaking the Green Movement, to Syria to advise pro-Bashar al-Asad forces.[24] Iran sent "several hundred members of the Revolutionary Guards al Quds force" to Syria armed with domestic COIN expertise, money, arms, and advanced equipment "designed to disrupt communications, the Internet, email, and cell phone communications."[25] Operations in Syria fell under the command of Major General Qasem Soleimani, an infamous figure described by General David Petraeus as "truly evil" and characterized by a senior Central Intelligence Agency officer as the "single most powerful operative in the Middle East."[26]

敘利亞

2012年，伊朗派出革命衛隊聖城旅作業小組，和資訊與通信技術(ICTs)專家到敘利亞協助親阿賽德政府軍部隊；[24]這些專家對打擊綠色革命組織已經駕輕就熟。伊朗派去這批幾百人的聖城旅成員，本身就具備境內綏靖專業，加上金錢援助、武器和先進裝備等豐富資源，目的就是為了要教會敘利亞部隊如何干擾並截斷網路、電子郵件和手機通訊。[25]伊朗人在敘利亞的行動，由奎松・索雷馬尼少將指揮，這位指揮官曾被中央情報局局長大衛・彼得雷烏斯形容為「相當邪惡」，另外一位中情局資深官員，則認為這個人是「中東地區最厲害的特務」。[26]

Under Soleimani's authority, Quds Force operators trained proxy Hizballah and Syrian elements in Iranian camps such as Amir Al-Momenin and integrated themselves into key command and control centers across Syria.[27] According to Dexter Filkins, "To save Assad, Soleimani called on every asset he had built since taking over the Quds Force: Hezbollah fighters, Shiite militiamen from around the Arab world and all the money and materiel he could

24 Farnaz Fassihi, Jay Solomon, and Sam Dagher, "Iranians Dial Up Presence in Syria," Wall Street Journal, September 16, 2013.

25 Ephraim Kam, "The Axis of Evil in Action: Iranian Support for Syria," Institute for National Security Studies Insight No. 372 (October 10, 2012), 3, available at 〈www.inss. org.il/index.aspx?id=4538&articleid=5207〉.

26 Dexter Filkins, "The Shadow Commander," The New Yorker, September, 20, 2013, 3.

27 Fassihi, Solomon, and Dagher.

squeeze out of……Assad's own besieged government."[28] Inside Syrian operation centers, Quds Force operators initially provided advice on techniques for suppressing social media and deterring civil disobedience, but soon escalated "with all kinds of kinetic options" to crush the rebellion, just like they had done at home.[29] The Quds Force showed a ruthless understanding of cyber-enabled COIN using "their intelligence networks to train the Syrian army how to fight people without killing; how to use force to cause injury, without being accused of a massacre ……teaching them how to control Web sites and social media and how to jam television channels."[30]

在索雷馬尼領導下，聖城旅作業人員在Amir Al-Momenin等伊朗營區，訓練敘利亞真主黨員，讓他們能自我整合成為整個敘利亞主要的指管中心。[27]根據作家德克斯特・菲爾金斯形容：為了拯救敘利亞總統阿賽德的政權，索馬雷尼集中革命衛隊聖城旅的所有資源，宣布「阿拉伯世界的真主黨戰士和什葉派民兵，所有金錢和物資都應該拿來解救阿賽德政府的危機」。[28]在敘利亞作業中心裡，聖城旅作業人員傳授如何壓制社群媒體，和對付陳情抗議人員的各種技巧；但是很快的，就進展到實質摧毀反對組織的各種方法，就像他們在伊朗對付綠色革命勢力一樣。[29]聖城旅成員傳授的冷血網路手法，運用情報網絡，訓練敘利亞軍隊如何對人民只傷不殺，就不會被控以屠殺罪行；還教導他們如何控制資訊網站、社群媒體，和如何遮斷電視頻道。[30]

As with the 2009 attacks on the Green Movement, the Quds Force backed up its cyber-targeting activities with brute force. By this time, however, operatives had learned to distance themselves from the Iranian-trained Syrian, Iraqi, and Hizballah proxies doing the dirty work. As a RAND paper pointed out, "Iran has skillfully employed its own special warfare capabilities as part of a long-term regional strategy, using state and nonstate proxies to advance its regional interests."[31] At the same time, the Syrian Electronic Army (SEA) benefited from Iranian expertise, money, and technology to attack anti-Assad social media and Web sites.[32] The

28 Filkins, 30.

29 Dubowitz and Levitt, 6.

30 "Iran Confirms Sending Troops to Syria, Says Bloodshed Otherwise Would Be Worse," Al Arabiya, May 28, 2012.

31 Madden et al., 2.

SEA "aggressively engaged in a wide range of online activities to punish perceived opponents and to force the online narrative in favor of the Assad regime."[33] The SEA used distributed denial-of-service attacks, jammed online portals, overloaded networks, and used malware to thwart opponents' messages and actions.[34] Supporting the efforts from Iran, the Basij actively disseminated propaganda, developed increasingly advanced cyberspace capabilities, and professionalized offensive paramilitary hacker field training.[35] It seems that the Basij inundated the Internet with disinformation to obscure Iran's true complicity in Syria and redirect any blame as a Western conspiracy to overthrow Assad.

在2009年打擊綠色革命勢力時，聖城旅在網路鎖定對象後就動用暴力；聖城旅特工在幹這些下三濫髒活的手法上，遠比敘利亞、伊拉克，以及真主黨高明。蘭德公司的報告曾經披露：「伊朗已經可以很細膩的運用特種作戰技巧，協助推動長期地區戰略，並動用國家與非國家資源，鞏固其地區利益」。[31]於此同時，敘利亞電戰部隊(SEA)在伊朗的專家、資金和技術支援下，攻擊反阿賽德社群媒體和網站。[32]電戰部隊積極涉入廣泛的在線活動，懲罰所有敵人，強迫他們在線上頌揚阿賽德政權。[33]電戰部隊採用分散式拒絕服務攻擊、遮蔽線上入口、灌爆網站，同時以惡意軟件來破壞對手傳送的信息與動作。[34]在伊朗支持下，青年志願軍積極宣傳，網路空間能力日益精進，並對準軍事駭客實施更專業化的攻擊性訓練。[35]判斷青年志願軍在網路以大量資訊，遮掩在敘利亞的真正目的，並將責任轉嫁給西方國家推翻阿賽德政權的陰謀上。

Iran succeeded against the Green Movement and anti-Assad forces by interweaving ICT efforts to identify key human and information networks with brute force. Beginning with Jafari's reorganization of the IRGC, Iran's cyber-enabled COIN was later perfected

32 Gabi Siboni and Sami Kronenfeld, "Developments in Iranian Cyber Warfare, 2013-2014," Institute for National Security Studies Insight No. 536 (April 3, 2014), 1, available at 〈www.inss.org.il/index.aspx?id=4538&articleid=6809〉.

33 Max Fisher and Jared Keller, "Syria Digital Counter-Revolutionaries," The Atlantic, August 31, 2011, available at 〈www.theatlantic. com/international/archive/2011/08/syriasdigital-counter-revolutionaries/244382/〉.

34 Ibid.

35 Gabi Siboni and Sami Kronenfeld, "Iran's Cyber Warfare," Institute for National Security Studies Insight No. 375 (October 15, 2012), 3, available at 〈www.inss.org.il/index. aspx?id=4538&articleid=5203〉.

with Soleimani's operations in Syria. Throughout both campaigns, the Basij cyber force was a "core state instrument of suppression," honing its techniques to provide cover for Iran's ruthless actions.[36] Iran's cyber-enabled COIN is a stunning success, not only for its cyber-SOF hybridization but also for crushing two separate rebellions and never triggering any meaningful Western military response.

伊朗成功的壓制住綠色革命和反阿賽德政權的勢力，靠的是靈活運用資訊與通信技術，並配合其他手段找出關鍵人物和關鍵的資訊網站。因為共和衛隊指揮官的認可，伊朗在敘利亞網路化綏靖作戰作為，透過索雷馬尼的運籌，執行得非常成功。綜觀這兩次行動，青年志願軍的網路戰力可說是壓制對手的核心工具；他們提供了側翼掩護，讓伊朗方面的冷血行動如虎添翼。[36]伊朗網路化綏靖作戰的成功，不只因為完美地整合了網路和特種部隊的戰力，更在於扳倒了兩次的反對行動，卻並未引起西方的軍事反應。

Lessons Learned

There are four primary lessons learned from the actions of Iran and Russia that inform a conceptual framework for aligning cyber capabilities to U.S. special warfare operations.

1. There is a distinction between the offensive cyber tools the IRGC-QF and Spetsnaz employed at the tactical level and those that exist at the strategic level. Iranian and Russian operators targeted tactical-level "circumscribed or closed networks,"[37] such as local communications, social media, and regional Internet and logistic infrastructure, while seemingly keeping their more sophisticated open network tools in reserve.

2. Cyber-enabled special warfare is primarily a proxy-executed endeavor that values minimal source attribution. As described by General Gerasimov, "Longdistance, contactless actions against the enemy are becoming the main means of achieving combat and operational goals."[38] Cyber-enabled SOF generally avoid direct force-on-force engagement and strive to operate in the gray areas between peace and war. As observed in Ukraine and Syria, cyber-enabled violence seeks to retain a modicum of deniability, letting proxies execute the dirty

36 Dubowitz and Levitt, 6.

37 Leed, 12.

38 Coalson, 3.

guerrilla tactics of assassination, sabotage, and ambush. Russia and Iran retained the strategic flexibility to cut and run should things go awry.

3. ICT exploitation, cyber attack, and IO play significant roles in cyber-enabled irregular campaigns. Properly conducted, traditional special warfare campaigns extend to far more than SOF; "they involve the comprehensive orchestration of broader capabilities to advance policy objectives."[39] Likewise, for these campaigns to work, expertise from other arenas must be integrated and synchronized.

4. Cyber-enabled special warfare could both deter conflict and be applied throughout the spectrum of conflict because it "is well suited to all phases of operation, from shaping the environment through intense warfare through reconstruction."[40] Even though Iran and Russia have operated at the malicious end of the spectrum, cyber-enabled special warfare has a constructive side, too. The proliferation of low-cost information and communication technologies benefits partner nations in the building of security, thereby helping to keep conflicts from breaking out.

經驗教訓

伊朗和俄羅斯對網路戰的運用，在概念架構方面有四點值得美國的特種作戰部門引為借鑑，分述如下：

1. 革命衛隊聖城旅和俄羅斯特種部隊，兩者的攻勢網路工具運用，在戰術與戰略層次均有所不同。伊朗和俄羅斯作業人員鎖定的是戰術層次的「限制型或封閉型網路」[37]，比如本土通訊網、社群媒體，和地區性網際網路及其後勤設施，似乎有意保留他們更複雜精密的開放網路手段，作為備援計畫。

2. 網路特種作戰基本上是一種代理人作戰型態，當事人很少露臉。誠如俄羅斯參謀總長格拉西莫夫上將所形容：長距離、避免接觸的行動，已經成為達成作戰目標最主要的方式。[38]網路特種作戰通常會避免與敵正面遭遇，遊走於和平與戰爭中間的灰色地帶。觀察烏克蘭和敘利亞境內發生的案例可以發現，以網路行動為主的特種作戰，結合網路的暴力旨在保留脫罪空間，卻讓代理人執行暗殺、破壞和伏擊等骯髒游擊戰。躲在後面的俄羅斯和伊朗，則保有或戰或止的戰略彈性，讓情勢隨著他們的意志發展下去。

39 Madden et al., 1-4.

40 Ibid., 9.

3. 資訊與通信技術運用、網路攻擊，以及資訊戰，在網路非正規作戰中，扮演了重要的角色。透過正確的引導，網路特戰遠比傳統特戰部隊寬廣；「對達成政策目標來說，遂行作戰牽涉各種不同戰力彼此的配合。」[39]因而欲使戰役運作順利，就必須整合各領域專家。

4. 網路化的特種作戰既可以嚇阻衝突，也可以應用在各種已經發生的衝突。因為它「非常適合運用於作戰各階段，從形塑環境到高強度作戰，一直到戰後重建。」[40] 儘管伊朗和俄羅斯都用在整個光譜最邪惡的部分，網路化特種作戰其實也具有建設性。低成本資訊與通信技術的普及，有利於夥伴國家確保安全，從而有助於避免爆發衝突。

Cloud-Powered Foreign Internal Defense

Cloud-powered foreign internal defense (FID) is both a technical computing concept and a metaphor for building partner capacity and trust through virtual means. Although not yet fully defined, FID clouds link cross disciplined communities together to better understand human, geographic, and virtual arenas, and then act conjointly on targeted overlaps. Technically speaking, FID clouds strengthen partner relationships through federated architectures that share data in real time, enhance automation, and diffuse analytic processes. Clouds have adjustable configurations that can take the shape of private, public, community, and hybrid models, each characterized by different software, platform, and infrastructure architectures.[41] FID clouds power encrypted mobile applications, analytic tools, and pooled data through smart technology in the hands of those involved with building security.

雲端外來內部防衛

以雲端技術為基礎的外來內部防衛(FID雲)，不只是一個技術性電腦運用概念，也是協助盟邦培養能力、建立信任的虛擬作為。雖然到目前為止都還未充分定義，FID雲已經用於連結跨領域通訊技術，以更清楚的掌握人員、地理和虛擬場所，並對重複鎖定的部分有效處理。技術方面來說，FID雲可以透過相同的內部結構，強化夥伴關係、即時分享資料、提高自動化，並普及分析程序。為了因應個人、公眾、社群或是這三者的混

41 Department of Defense (DOD) Chief Information Officer, Cloud Computing Strategy (Washington, DC: DOD, July 2012), 41, available at 〈www.defense.gov/news/dodcloudcomputingstrategy.pdf〉.

合型態等不同需求，雲端技術可以在軟體、平台和基礎設施方面，為每一次面對的不同目標調整型態以為因應。[41]若是牽涉到安全問題，雲端現有技術還可以對行動運用、分析工具和已蒐集資訊進行加密。

Although data are virtually tethered to a cloud, the real value lies in enabling the diffusion of timely information to elements at the tactical level. FID clouds are also a metaphor for persistent and vibrant partnerships because, like the technology, the data never rest and the networks do not go idle. This technology is simply a vehicle to empower a deeper, broader, and more contextual community of understanding for the sociocultural, political, and historical factors that all too frequently fuel strife. Instead of reactive relationships characterized by intermittent FID deployments, which achieve a spotty understanding, FID clouds are metaphors for building a more persistent form of capability, capacity, and trust between partnered nations.

儘管數據資料都儲存在雲端，其真正的價值，卻是在需要運用時將其傳播到戰術階層每一個單位去。FID雲有如一個可靠的好夥伴，因為數據資料隨時備便，網路永不斷線。這種技術只是提供一個載體，從社會文化、政治和歷史等各方面因素，進行深入且全面的分析，以瞭解何種狀況下較容易挑動或制止情勢發展。FID雲並非間歇啟動的被動狀態，以致對狀況只能得到點狀認識，而是持續不斷地建立夥伴關係國家之間的能力、容量與信任。

FID clouds lay a virtual foundation for future growth of diverse institutions, centers, and laboratories that can help close the seams between U.S. interagency community interests in a country. From a strategic U.S. Government perspective, FID clouds are a pragmatic "partner-centric approach to design campaigns around a partner's core interests, rather than hoping to transform them in ways that have frequently proved to be ephemeral."[42] FID clouds also provide strategic discretion "when a public relationship of a U.S. partner state is problematic because of the partner state's domestic politics."[43]

以虛擬平台作為發展基礎的FID雲，可以協助各不同機構、中心和實驗室的未來發

42 Ibid., 3.

43 Ibid., 4.

展，並協調整合美國在這個國家各個部會間的利益。從美國政府的戰略觀點來看，FID雲是一種非常實用的「以夥伴為中心的模式，圍繞夥伴的核心利益來設計各種活動，而不是企圖要改造夥伴；多次證明要改造夥伴，效益都是很短暫的」。[42]「當夥伴國家內部政治因素，使雙方關係產生問題時」，FID雲也提供了戰略選擇權。[43]

FID clouds provide other opportunities as well. The technology and relationships that they foster across communities can be quickly scaled up to respond to sudden emergencies such as humanitarian assistance/disaster relief operations, counter-genocide, or noncombatant evacuation missions. They can save money, time, and manpower by feeding information to decision-makers when time is of the essence. For partner-building efforts, FID clouds can store information hosted by indigenous non-U.S. social media platforms, enriching social network analysis, sociographic mapping, and behavior and sentiment trend analysis. Most importantly, FID clouds spread trust in a creative and super-empowered way that helps to establish long-lasting influence with allies, coalitions, and other partners.

FID雲也提供了其他的機會。在群組社群間發展出來的技術和連結，可以很快地對一些突發事件，例如人道協助、災難救助行動、反集體屠殺或非戰鬥性撤離任務等，採取迅速反應。當時間急迫時，這套系統可提供決策人員足夠資訊，因而節省可觀經費、時間和人力。FID雲可以在夥伴國家的本土社群平台上儲存資訊，增進其社群網絡分析、社會現況定位以及行為／情緒趨勢分析等各方面能力。最重要一點是，FID雲可以用極富創意的有效方式，建立彼此間的信任感，這對同盟國、聯盟和其他夥伴國家之間建立長久影響力，甚具意義。

Counter-network COIN

Counter-network COIN (CNCOIN) is a simple concept aimed at leveraging, harnessing, and exploiting social media networks.[44] Designed to break an adversary's asymmetric information advantage, CNCOIN employs nontechnical attacks against people to manipulate

44 Joint Publication 3-24, Counterinsurgency (Washington, DC: The Joint Staff, November 22, 2013), I-2, defines counterinsurgency as "comprehensive civilian and military efforts taken to defeat an insurgency and to address any core grievances."

their perceptions, behaviors, and actions. It puts a military twist on many of the ill-defined yet ubiquitous anti-social networking tactics practiced across cyberspace. Although these tactics are not clearly defined, this article characterizes them as actions that obscure a perpetrator's true identity while he manipulates social media for reasons other than what is stated. Although social media pose a wide array of opportunities for any anti-social network, ranging from criminally exploitative to benignly misrepresentative, from a military perspective, social media present a rich array of information on ways to influence psychological vulnerabilities and an ideal attack platform from which to do it.

反制網路反暴動

網路化綏靖作戰(CNCOIN)乃是一個運用、駕馭、拓展社交媒體網絡的簡單概念。[44] 反網路綏靖作戰旨在打破對手的不對稱資訊的優勢，以非科技方式攻擊來操控人們的看法、行為和行動。對許多在網絡空間定義不明，卻廣為流傳的反社會網絡採取軍事行動。雖然這種戰術尚無明確定義，本文將其指向隱藏幕後的媒體操弄者。雖然社會媒體對任何反社會網絡提供廣泛的機會，從剝削到善意卻錯誤的都有，從軍事角度來看，社交媒體提供了一系列影響脆弱心理的資訊，然後加以攻擊的平台。

There are three broad functional categories for classifying CNCOIN: operations, intelligence, and IO. There are also several techniques within each functional category that help highlight its practice rather than define it outright. These techniques are by no means all encompassing or without overlap.

從廣泛的功能性來分類，網路化綏靖作戰(CNCOIN)基本可以區分以下三種型態：作戰、情報和資訊戰。每種型態下都包含許多種運用技巧，即使還是無法充分對CNCOIN加以定義，卻可以在實際運用方面凸顯它的重要性。這些運用手法彼此之間相互獨立，不致疊床架屋，彼此干擾。

The first CNCOIN category is operations. It includes but is not limited to cyber-pseudo and cyber-herding operations. A cyber-pseudo operation is a classic COIN strategy "in which government forces and guerrilla defectors portray themselves as insurgent units" to infiltrate enemy networks and apply advanced tradecraft inside the network to destroy

it.[45] A cyber-herding operation, on the other hand, "is the action by which an individual, group, or organization drives individuals, groups, or organizations to a desired location within the electronic realm."[46] The beauty of both techniques is that they drive invisible wedges between insurgents and their command and control by exploiting the inherent weaknesses of communication and communication platforms within every network. Cyber-pseudo and cyber-herding operations prey on an enemy network's natural need to maintain a low signature to survive. Both techniques target intermittent and decentralized insurgent leader communications, manipulating or replacing them, which synergistically leads to growing opportunities for the cyber counterinsurgent.[47] The virtual world simply amplifies the environmental factors because personalities are harder to authenticate as real or fictitious.[48] The lack of command and control authentication, communication frequency, and platform availability are key cyber-pseudo and cyber-herding pressure points to manipulate, misinform, or drive targets toward desired outcomes.

CNCOIN的第一種策略稱為作戰，基本分成網路偽冒(cyber-pseudo)和網路群集(cyber-herding)兩種方式。網路偽冒是典型綏靖作戰的手法，「政府軍隊和游擊隊都把自己看成叛亂份子」，運用先進的諜報技術，打入敵人的網路，從網路內部進行破壞。[45]另一方面，所謂網路群集，是指「個人、單位和組織都設法將自己、單位和組織驅動到所望的電子領域中」。[46]這兩種手法最精妙之處，是在敵對叛軍和指揮管制系統之間，利用其先天弱點，在通訊系統和平台上點燃無形的燎原星火。網路偽冒和網路群集之所以存在，完全是抓住對方在網路上的自然需求。這兩種方法鎖定叛軍領袖週期而零碎的通訊，加以操控、變造並取代；對反網路綏靖作戰來說，這些方式發揮的協同效應，增加了很多可以運用的機會。[47]在虛擬世界中，很單純的環境因子都可以被無限放大，原因就在於人性很難判斷其真偽。[48]缺乏對指管系統、通訊頻率及平台特性的辨識

45 Lawrence E. Cline, Pseudo Operations and Counterinsurgency Lessons from Other Countries (Carlisle, PA: U.S. Army War College, June 2005), 5, available at 〈www. strategicstudiesinstitute.army.mil/pdffiles/ pub607.pdf〉.

46 David B. Moon, "Cyber-Herding: Exploiting Islamic Extremists," in 2007 JSOU and NDIA SO/LIC Division Essays, Joint Special Operations University Report 0075 (Hurlburt Field, FL: JSOU, April 2007), 4, available at 〈www.dtic.mil/get-tr-doc/ pdf?AD=ADA495377〉.

47 Cline, 5.

48 Moon, 15.

能力，就是網路偽冒和網路群集得以操控、誤導，或驅使目標向所望結果發展的關鍵原因。

The second CNCOIN category is intelligence, which includes but is not limited to crowdsourcing and social networking analysis (SNA) exploitation techniques. Crowdsourcing is a practice that taps into large pools of diverse knowledge willingly provided by participants to solve problems with new ideas, services, or observations and quickly broaden the organizer's perspective.[49] SNA visually depicts and measures relationships, their density, and the centrality of social links in order to illuminate social network structures.[50] The social network visualizations, or sociograms, provide a unique window to assess, map, and even predict the intensity of relationship events over temporal, geospatial, and relational horizons.[51]

第二種是情報，包括「群眾外包」(crowdsourcing)和社會網絡分析(social networking analysis, SNA)兩種運用方式。群眾外包是從一大堆各種不同型態的知識或資訊中，由參與者志願性的用新構想、服務或觀察，汲取可用的部分以解決問題，或迅速地擴展上級人員的視野。[49]社會網絡分析則是具體描述、評量彼此間關係、親疏、社會連結向心力等，以有效發揮社會網絡結構的功能。[50]將社會網絡具體化，或製成社會關係分析表，提供了一個有助於評估、製圖的特殊窗口，甚至預測在某一時空下，因關係產生狀況的強度。[51]

During the September 2013 Zamboanga City crisis in the Philippines, rogue Moro National Liberation Front (MNLF) forces, dissatisfied with the state of national reconciliation, mobilized a force that seized over 200 civilian hostages, raided businesses, and burned buildings

49 Dragos Negoitescu and Mark Blaydes, "Crowdsourcing: Is NATO Ready?" Three Swords Magazine, no. 26 (2014), 2, available at 〈www.jwc.nato.int/images/stories/threeswords/crowdsourcing.pdf〉.

50 Seth Lucente and Greg Wilson, "Red Line: Social Media and Social Network Analysis for Unconventional Campaign Planning," Special Warfare 26, no. 3 (July-September 2013), 21-23, available at 〈www.dvidshub.net/publication/issues/12346〉.

51 Ibid.

52 Al Jacinto, "Zambo Propaganda, Drama Plays On," The Manila Times, September 28, 2013, available at 〈www.manilatimes.net/ zambo-propaganda-drama-plays-on/40435/〉.

throughout the city.[52] During the crisis, both crowdsourcing and SNA exploitation were successful techniques. Although inadvertently at first, Philippine security forces (PSF) used crowdsourcing techniques to encourage Zamboanga residents to spot and report information on rogue MNLF locations throughout the city. The PSF fused crowd-sourced information with intelligence analysis, informing both security and humanitarian operations. The PSF used SNA exploitation to assess populace support for rogue MNLF, as well as to counter and discredit rogue MNLF statements on social media by taking down propaganda Web sites that violated social media user agreements. The PSF also used crowd-sourced information to cordon pockets of rogue MNLF forces and raid ad hoc command posts. Although less sophisticated than Iran's cyber-enabled COIN, the PSF thwarted rogue MNLF asymmetric advantage by using social media to target key information and leadership nodes, following up with physical force to defeat them.

2013年9月在菲律賓三寶顏發生的衝突中，摩洛民族解放陣線(MNLF)部隊，因為跟政府的和解條件談不攏，發動攻擊並抓了兩百多個平民作為人質，突襲商業機構，並在市區四處放火劫掠。[52]在這場衝突中，菲律賓對群眾外包和社會網絡分析這兩種手法的運用，堪稱成功。一開始，菲律賓安全部隊(PSF)運用群眾外包策略，呼籲三寶顏當地居民將解放陣線成員在市區位置的資訊，標定之後回報。安全部隊融合群眾外包所獲得的資訊和情報分析相結合，同時採取維安和人道行動。安全部隊利用社會網絡分析技巧，評估了一般民眾對解放陣線的支持度，並且違反社群媒體使用者協議，設法控制了幾個宣傳網站，在社群媒體中打擊解放陣線。然後運用群眾情資，封鎖解放陣線外圍，並對其臨時指揮所發起攻擊。雖然比起伊朗的網路化綏靖作戰來說，菲律賓安全部隊採取的手段沒那麼複雜精確，但是他們運用社群媒體鎖定關鍵的資訊和指揮節點，接下來再使用兵力加以攻擊的一連串作為，完全消弭了摩洛民族解放陣線的不對稱優勢。

The third CNCOIN category is IO and includes but is not limited to cyber aggression, sock-puppeting, and astroturfing techniques. All three techniques exploit social media anonymously to misrepresent, misinform, and manipulate behavior, sentiment, and actions. Advanced by Diane Felmlee, cyber aggression "refers to electronic or online behavior intended to harm another person psychologically or damage his or her reputation" by using "email,

instant messaging, cell phones, digital messages, chat rooms, as well as social media, video, and gaming Web sites" and is wider in scope than common cyber bullying.[53] Its anonymous application could cause substantial psychological harm and negative consequences as messages are repeatedly viewed by the target or forwarded across social media sites.[54] Its value to CNCOIN is in exploiting sensitive digital information that could shame, demoralize, or traumatize targets into taking psychologically impaired actions. These deliberate cyber aggression operations could undermine the target's credibility, influence, and power to the point of triggering the target to neutralize himself or other insurgents.

網路化綏靖作戰(CNCOIN)的第三種方式是資訊戰，其作為包含網路侵犯、網路假身分，和製造假人氣三種手法。這三種手法都是透過社群媒體，以匿名方式扭曲、誤導，並試圖操控對方的行為、情緒和行動。社會學家黛安・費蒙麗對網路侵犯提出她的看法：是一種在電子或網路世界，蓄意破壞某人名譽，以對其心理造成傷害的行為。使用的方式有電子郵件、即時訊息、行動電話、數位訊息、聊天室，或其他社群媒體、遊戲網站等等，所影響的範圍，會比一般網路霸凌來得廣泛。[53]因為是用匿名方式進行，負面訊息如果持續出現在社群網站上，會對當事人造成很嚴重的心理創傷和不良影響。[54]對網路化綏靖作戰來說，這招之所以有效，是因為用了敏感的數位資訊來傳布，很容易讓當事人覺得丟臉、沮喪，從而由心理層面弱化其行動能力。這些蓄意的網路侵犯行為，可以造成當事人在可信度、影響力和權力方面的重大傷害，可以削弱其個人和相關組織的能力。

The other techniques, sock-puppeting and astro-turfing, are defined as fictitious online propaganda tools that disseminate contrived views to fabricate a broader illusion of support or nonsupport.[55] Astro-turfing is the same concept as sockpuppeting, but it is more sophisticated

53 Diane Felmlee and Robert Faris, "Toxic Ties: Networks of Friendship, Dating and Cyber Victimization," paper presented at the American Sociological Association Annual Meeting, Hilton, NY, August 9, 2013.

54 Ibid.

55 Alex Comninos, "Twitter Revolutions and Cyber Crackdowns: User-Generated Content and Social Networking in the Arab Spring and Beyond," Academia.edu, June 2011, 4, available at 〈http://academia.edu/633706/ Twitter_revolutions_and_cyber_crackdowns_User-generated_content_and_socialnetworking_in_the_Arab_spring _and_beyond〉.

and organized and is undertaken on a larger scale than sock-puppeting.[56] Both astro-turfing and sock-puppeting use virtual personas and "bots" to pump false information across cyberspace to incite reaction or mobilize mass action. As witnessed with Russia's army of trolls, botnets, and hired hackers in Ukraine, astro-turfing networks are awash with an arsenal of propaganda, pictures, and videos stoking conflict and obscuring actions on the ground. Counter-network IO becomes even more effective when combined with deliberate and misleading cyber-targeting activities, such as IRGC activities during the 2009 Green Movement.

其他的手法，像是網路假身分，和製造假人氣，則被定義為一種線上宣傳工具，散發經過設計的觀點觀點，為特定對象打造出群眾支持或不支持的假象。[55]這兩者概念大同小異，但製造假人氣比較起來，操作必須更精細、更有組織，執行起來也牽動更大規模[56]。這兩種手法都會使用虛擬角色及其變形，在網際空間以假資訊，煽動某些反應或是大規模行動。見證過俄羅斯軍隊在烏克蘭搧風點火、癱瘓網路、雇用網路駭客，會發現他們在網路上製造假人氣時，所使用的宣傳單、相片、影片多不勝數；這些也都是製造衝突和隱匿實際行動的手段之一。就像伊斯蘭革命衛隊2009年鎮壓綠色革命時期，深思熟慮之後才展開行動，加上誤導鎖定對象的行動，讓反制網路資訊戰的行動更有效率。

Cyber UW Pilot Teams

The third way to advance U.S. cyber-enabled special warfare is the Cyber UW Pilot Team, a capability meant to harness social media networks to shape a physical environment, establish regional mechanisms, and stitch together area complexes prior to executing UW operations. Cyber UW Pilot Teams are purpose-built around the nucleus of a Special Forces Operational Detachment Alpha, augmented with interagency and technical support, whose mission is to digitally prepare an area for UW operations.[57] The teams undertake the same traditional pilot team tasks that previously were accomplished upon infiltration in the physical domain, but do it through virtual means before they ever put boots on the ground in sensitive, hostile, or denied

56 Ibid., 14.

57 Patrick Duggan, "UW in Cyberspace: The Cyber UW Pilot Team Concept," Special Warfare 27, no. 1 (January-March 2014), 69, available at 〈http://static.dvidshub.net/media/pubs/pdf_14790.pdf〉.

areas.[58] By operating virtually, Cyber UW Pilot Teams could decrease the time, risk, exposure, and attribution to the U.S. and partnered resistance forces because most of their activities would have been digitally accomplished prior to physical infiltration.[59]

非正規網路先鋒隊

第三種強化美國網路特種作戰能力的方法，是建立非正規網路先鋒隊。這是一支在實施非正規作戰之前，掌控社群媒體網絡、形塑實體環境、建立地區性機制，並整合區域設施的特種武力。非正規網路先鋒隊的設立環繞於特種作戰第一分遣隊(Special Forces Operational Detachment Alpha)的核心，特別著重跨部會與技術支援；其任務就是針對某區域，隨時做好非正規作戰的數位整備工作。[57]網路先鋒隊所執行任務，與傳統先遣部隊大致相同，就是在進入敏感、敵對或是敵之後方區域前，先以虛擬方式滲入，並完成實體掌控的準備工作。[58]由於所有行動都在實兵滲透前，以虛擬方式進行，因而可以縮短時間、降低風險、減少曝光及美軍人員與合作之反抗軍的傷亡。[59]

Conceptually, Cyber UW Pilot Teams build human, physical, intelligence, and information infrastructures on social media platforms with cyber tools and advanced techniques. The teams could sharpen their localized language and cultural skills while deepening their understanding of the local human terrain. They could also identify resistance leaders, assess motivations, evaluate resistance capabilities, and assess overall support for U.S. Government objectives while simultaneously evaluating informal hierarchies, psychology, and behavior. In addition, the teams could blend into the white noise of the Internet by tapping into social media networks to "improve U.S. contextual understanding of potential partners and the situation on the ground before the United States commits to a course of action."[60]

從概念上來說，非正規網路先鋒隊就是以網路工具和先進技術，在社群媒體平台上，建立起人員、實體、情報，與資訊基礎設施。先鋒隊成員精通當地語言，並熟悉當地文化與習慣，同時熟稔當地人文地形。他們能辨認出誰是反對勢力領袖、衡量其動機及能力，並整體評估當地對美國政府的支持程度；這需要同時從了解其意見領袖、心理狀

58 Ibid.

59 Ibid.

60 Madden et al., 1-4.

態和行為模式做起。此外，隊員們也要藉著混進當地社群媒體網絡，在一片網路雜音中，設法增加網民對美國的認識和好感，並在美國決定要對當地發起行動之前，先發掘潛在的夥伴和有利情況。[60]

Every Cyber UW Pilot Team would have tailored execution authorities and acceptable levels of UW infrastructure development. Once those levels are reached and authorities given, the same team that established the infrastructure virtually would ideally execute its own plan on the ground with the area complex and resistance forces they nurtured online. Cloaked in dual-purpose technology, indigenous equipment, and mobilized networks, these teams would digitally initiate and then physically execute their assigned UW operations from beginning to end.

每一支非正規網路先鋒隊都有其特定的任務執行權責體系，和相對層級的非正規作戰基礎設施發展。一旦符合以上條件，經授權後，建立虛擬基礎建設的先鋒隊，即可配合網路布建與反抗勢力執行任務。在軍民兩用的科技、當地設施和網路動員的掩護之下，這些先鋒隊員就能從數位戰場開始行動，配合實體作為全程展開非正規作戰，完成交付任務。

While there has long been recognition of the strategic role of cyber operations in U.S. national security, this awareness has not fully translated into the development of clear strategic-level thinking and operational capacity. For example, the Department of Defense Strategy for Operating in Cyberspace offers few solutions or specifics, but rather reiterates earlier cyber themes in a five-point outline.[61] The lack of well-defined ideas creates a vacuum in cyber strategy that puts the United States in danger of ceding its superior cyber-technological advantage to potential adversaries.[62] In contrast, the asymmetric innovations demonstrated by Iran and Russia present a template for other aspiring regional and global powers to imitate as an irregular pathway to circumventing U.S. military dominance and securing their strategic interests.[63] Moreover, the diffusion of inexpensive yet sophisticated technology increases this

61 Thomas M. Chen, An Assessment of the Department of Defense Strategy for Operating in Cyberspace (Carlisle, PA: U.S. Army War College, 2013), 30.

62 Ibid., 36-37.

63 Madden et al., 1-4.

potential every year. Iran and Russia have made the American lack of specificity in strategic-level cyberspace documents irrelevant, as the country does not need simply to write about strategy, but must now catch up.

雖然網路作戰在美國國家安全的戰略角色早被定位多時，但是這種認知，並沒有完整詮釋為明確的戰略思維並形成戰力。舉例來說，國防部網路作戰戰略雖然提供了一些方案和細節，其實不過是重複以往網路五個要點。[61]定義不明確的構想，只會導致網路戰略空洞化，讓美國面對潛在敵人，將享有的科技優勢拱手讓人。[62]相較之下，伊朗和俄羅斯在這方面展現的不對稱創意，對有意成為地區或全球強權的國家應如何透過非正規管道，規避美國的軍事獨霸，確保他們的戰略利益，樹立了一個足堪模仿的典範。[63]此外，這種廉價卻不甚複雜的技術每年都在持續擴散，讓潛在強權挑戰美國的趨勢更加明顯。伊朗和俄羅斯運用網路特種作戰的成效，已經讓美國是否具備戰略階層網路文件顯得無關緊要，需要的是如何迎頭趕上了。

Cyber-enabled special warfare is a strategic-level offensive capability gap that must be filled. Clearly, the United States must aggressively pursue a form of special warfare that integrates cyber operations into tactical-level irregular operations. A recent RAND report on special warfare concluded that "the United States needs to employ a more sophisticated form of special warfare to secure its interests……and given recent trends in security threats to the United States and its interests, special warfare may often be the most appropriate way of doing so."[64] Cyber-enabled special warfare is the answer in an increasingly interconnected global environment in which physical infrastructure is rapidly being assigned Internet Protocol addresses for assimilation into an "Internet of things." By the year 2020, over 50 billion machine-to-machine devices (compared to 13 billion today) will connect to cyberspace through "the embedding of computers, sensors, and Internet capabilities."[65] Cyber-enabled special warfare bridges the gap between the virtual and the physical by harnessing modern-day information networks and melding them with old-fashioned, faceto-face SOF partner engagement.

64 Ibid., 4.

65 Patrick Tucker, "The CIA Fears the Internet of Things," DefenseOne.com, July 24, 2014, available at 〈www.defenseone.com/ technology/2014/07/cia-fears-internetthings/89660/〉.

網路化特種作戰是必須彌補的攻勢戰略的戰力間隙。很明顯地，美國必須積極研發能夠將網路作戰，整合到戰術層級非正規作戰的一種新型態特種作戰。蘭德公司最近發表一篇有關特種作戰的報告中提到：「美國需要一種更複雜精密的特種作戰，以確保其利益……；以現階段的趨勢來說，想弭平對美國利益的威脅，最佳方式還是採取特種作戰。」[64]在目前這個互連緊密的全球環境之中，任何實體設施被賦予IP位址之後，都變成全球物聯網(Internet of things)的一分子；此時，網路特種作戰就是問題的答案。在2020年之前，在網際空間會有超過500億個機器對機器的設備(目前約有130億個)，透過電腦、感測器跟網路技術相互連結。[65]網路化特種作戰藉著駕馭現代通訊網路，合併傳統面對面的人員特種作戰，在虛擬和實體的鴻溝之間搭起一座橋樑。

Today's global environment impels the United States to adopt cyber-enabled special warfare as a strategic tool of national military strategy. The devastating examples of integrating offensive cyber capabilities into irregular tactics as demonstrated by Iran and Russia pave the way for other U.S. adversaries to soon follow. This article offers the Nation three new options for aligning emerging technology to special warfare missions: cloud-powered FID, counter-network COIN, and Cyber UW Pilot Team operations. Developing these three concepts to their fullest transcends simply maintaining a U.S. cyber-technology edge; their development projects revolutionary influence across the globe to build critical partnerships and shape issues across the spectrum of conflict. If successfully developed, cyber-enabled special warfare will become a powerful new strategic option for the Nation.

今日的全球化環境，迫使美國不得不將網路特種作戰，當成國家軍事戰略的重要工具。伊朗和俄羅斯將攻擊性網路能力，和非正規戰術結合在一起的案例，相信很快會被其他美國的對手學了去，用來對付美國。對於如何將新興的網路技術用於特種作戰任務，本文為美國提供了三種選擇：以雲端技術為基礎的外國內部防衛、反制網路化綏靖作戰和非正規網路先鋒隊。發展這三種新概念，重要性高於僅僅維持美國的網路技術優勢。這三種概念的發展，將會對於在全球建立重要夥伴關係、型塑爭論議題和衝突規模等方面，產生革命性的影響。這三種概念如果能成功發展，對美國來說，網路特種作戰，將會變成強而有力的戰略新選項。

作者：派翠克・麥可・杜根中校，於就讀美國陸軍戰爭學院時，寫下這篇文章。本文參加2015年參謀首長聯席會議主席徵選的戰略研究類論文中，獲得首獎。