

● 作者/Warren W. Choi & Olivia A. Garard ● 譯者/黃文啟 ● 審者/林政龍

如何反制小型無人機

Countering Small Unmanned Aircraft: It Takes a System

取材/2018年2月美國陸戰隊月報(Marine Corps Gazette, February/2018)

小型無人機是當代作戰環境的要素，其快速之非正規發展已逐步改變戰場原有之樣貌，美軍極須發展無人機反制系統，以強化反制無人機之作戰能力。

小型無人飛機系統(small unmanned aircraft system, SUAS, 下稱小型無人機)在實際面與數字面而言，皆呈現爆炸性成長。在美國第51屆美式足球超級盃總決賽中場表演節目中，英特爾公司安排了一場由300架無人機組成的集群飛行機隊，在歌手女神卡卡演唱後方升空伴舞及盤旋。¹ 就在幾週之後，中共在廣州年度元宵節慶典中以1,000架燈光無人機進行另一場類似煙火秀的飛行展示。² 如蜂群般的無人機令觀眾目不暇給外，更發現連美國的敵人也開始使用同類型無人機攻擊美軍。隨著科技與日俱進，好戰分子也同樣會在戰場上使用除LED燈光之外的小型無人機繼續製造浩劫。在戰爭



當人們更加依賴小型無人航空器和無人機的同時，也須做好反制敵人運用類似戰力的萬全準備。(Source: USMC/Shawn Valosin)

瞬息萬變的交互作用中，敵人使用小型無人機勢必成為一個不斷演變的問題。而在本文中，筆者將探討美軍面對敵軍小型無人機的各项弱點，並研擬反制手段的可行作法。

全新的可能性

戰爭是促進創新的強大推動力。正如克勞塞維茨所言，「戰鬥的必要性會讓人們很快想出各類特殊發明，以爭取戰場之有利態勢。」³ 小型無人機正是此類優勢之一。對於美軍戰鬥部隊而言，小型無人機可讓基層戰術部隊獲得偵察、監視、目標獲得及其他戰力。誠如任何新興科技不斷推陳出新一樣，只要美軍一推出任何創新裝備，敵人通常也會隨後跟進。

現代化衝突的核心圈，正是各型即興拼湊式武器之溫床。在伊拉克和敘利亞的戰場上，親伊斯蘭國和反伊斯蘭國的好戰團體，都是利用地下工程師迅速將各類無人機送往戰場執行任務。⁴ 在商用小型無人機普及化與相對廉價化的推波助瀾之下，也造就美陸戰隊退役上校哈姆斯(T. X. Hammes)所稱

的「空權民主化」(democratization of airpower)一詞。⁵ 非國家行為者現已擁有前所未有各型無人機的空域使用管道及機動能力。現在的空間早已不再是傳統大型飛機獨霸的領域，

「無人機對空權的影響，幾乎等同AK-47突擊步槍在小口徑武器界所扮演的角色一樣舉足輕重。」⁶

其實只須稍稍打開一點眼界，放縱一下思想，就可能借用技術綜合時代湧現的大量新技術和新因素的槓桿，撬動因思維的滯後而生鏽的軍事革命之輪。

喬良與王湘穗1999年所著《超限戰》

當前，吾人或許還能對此種迫切性戰略威脅的存在置之不理。如同法蘭基(Ulrike Franke)在〈飛行應急爆炸裝置：下一個重大威脅〉(Flying IEDs: The Next Big Threat)一文所做的分析，目前好戰分子所使用的小型無人機在短期內仍無法「澈底改變戰鬥型態。」但在未來，「部隊

極可能會遭遇愈來愈多難以攔截的精密系統。」⁷ 所有小型無人機都可直接成為武器系統的攜行載臺，而其廣泛之運用方式，將依照使用者想像空間而無限度的擴張。

敵人使用四軸飛行器對友軍部隊投射40公釐槍榴彈的攻擊行為，只是剛開始的第一步。⁸ 現今發達的商用科技，結合可棄式投送載臺，將可對美國的作戰行動造成各種非傳統性效應。只要配備內建處理器與簡單錐形裝藥，價值5,000美元的裝備就可以發揮如夢魘般的災難性效果——而一群小型無人機就能自動摧毀飛行線上價值高達10億美元的F-35戰機。⁹ 微型無人機可輕易讓F-22戰機停飛，¹⁰ 就如同維吉尼亞州的蜂襲事件一般。¹¹ 四軸飛行器可攜帶放射性物質，¹² 小型無人機則可以透過商用農藥噴灑技術，散播生物戰劑、催淚瓦斯、¹³ 沙林毒氣或VX神經毒劑。¹⁴ 一架具有縱火功能的小型無人機就可讓社會陷入一片混亂，¹⁵ 而小型無人機也能對美軍資訊科技系統進行精密的間諜刺探行動。¹⁶ 這些可能性是永無止盡

的，且創新的腳步才剛剛邁出而已。

隱藏性差距

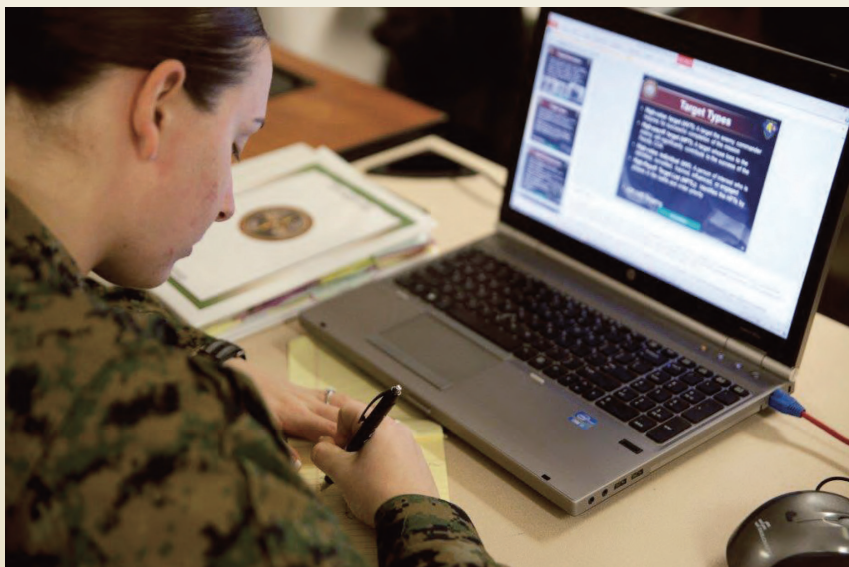
2015年，一名業餘無人機玩家操控一架小型無人機意外撞入白宮草坪，而祕勤局幹員對此事之預警，僅能靠視覺和聽覺進行辨別。¹⁷ 美國政府最高層級維安漏洞，亦存在於遍布全美各地區的陸戰隊基地中。而目前得知陸戰隊唯一配發各單位使用的小型無人機反制系統(counter-SUAS, C-SUAS)，只有「無人機防禦者」(Drone Defender) 一型。¹⁸ 該項裝備主要用於切斷小型無人機用來飛行操控的射頻通信鏈路，以及/或

全球衛星定位系統訊號。其方式是採用干擾系統鏈路，導致航空器無法導航，並使作業人員無法正常操控該飛機。

遺憾的是，像陸戰隊配發的「無人機防禦者」反制系統，只要利用內建式導航裝置就可輕易迴避其干擾。¹⁹ 目前商用小型無人機一般都配備鏈路中斷處理程式，可使其在沒有通信鏈路的狀況下，仍能按照預設路線飛行，甚至還可預判小型無人機喪失鏈路的狀況，預先將敵人位置輸入鏈路中斷路線的指定位置，這項功能早在「禽爪強擊2016演習」(Talon Reach 2016)中就已獲得驗證。不僅如此，小型無人機即便不使用全

球衛星定位系統也能飛行——其他方法還包含慣性導航、目視導航、²⁰ 熱尋標酬載、射頻尋標器、或是夜間成像偵測與測距系統等。²¹ 未來隨著內建處理技術與機器學習科技進步，小型無人機將能以更強大之自主性來執行任務，並在無外在輸入狀況下搜尋所望目標的性能必然大幅提升。

小型無人機偵測活動是美軍迄今尚未做好萬全準備的高度棘手問題。由於商用小型無人機大多數都是採低空、慢速、體積小，以致於讓擅長偵測更大型、更快速航空器的現行雷達系統難以掌握其動態。²² ²³ 此類威脅的多樣性，種類從低空、慢速、體積小的小型無人機到以色列航太工業公司的「哈若普」(Harop)滯空彈藥²⁴ 等不一而足²⁵——迫使美軍必須採取多重反制作法。偵測小型無人機需要多組感測器，主要是因為現有偵測方法不具備充足的精確度。而有希望用於搜尋此類無人機和作業人員的解決方案，其中包含影像分析、陸基與無人機機載雷達、²⁶ 聲波偵測器，²⁷ 以及射頻偵測裝置等，²⁸



為發揮最大偵測效果，有必要結合感測器輸入資料。(Source: USMC/Laura Marcado)

不過上述方案沒有一項裝置能獨自發揮充分偵測能力。

反制小型無人機的難度與偵測它的道理一樣困難。鑑於干擾裝置的效能有限，以致於衍生出「硬殺」(編者按，係指以實體彈藥進行直接攻擊)解決方案的必要性，而蒼蠅拍外形的無人機已在民用²⁹及軍用³⁰功能上展現其潛力。但在相同的情況下，敵人找出反制無人機捕捉網的方法只是時間早晚的問題。於此同時，某個美國盟邦還曾使用愛國者飛彈去擊落一架200美元的無人機。³¹美軍現在除了目視偵察和編制直射武器外，根本沒有專門用於偵知與摧毀小型無人飛行系統威脅的裝備，同時也沒有具備可發現直接操控那些小型無人機作業人員的能力。由於軍事處置手段付之闕如，法國陸軍在荷蘭警方證明其概念可行後，現在也開始訓練老鷹來捕捉小型無人機。³²而老鷹在美國國防戰略運用上，唯一應該存在的地方只有陸戰隊的軍徽。

重新省思系統

小型無人機反制系統必須結



美陸軍正在測試無人機防禦者系統。(Source: DoD)

合各種不同的裝備，並透過模組化、網路化架構進行功能整合。傳統整體防空系統為了發揮防空功能結合了必要的各個功能(例如，偵測、戰場管理及制壓手段等)。小型無人機反制系統也是同樣的道理，但由於戰場狀況變化迅速且加上偵測及摧毀困難，因此反制系統必須運用網路化科技以提高裝備反應速度與精準度。理想的反制系統應能整合各種偵測裝置所提供的資訊，評估威脅本質、接著能快速採取適當的反制機制。美軍需要一套由模組化套件構成的系統體系(system of

systems)，以肆應戰場狀況瞬息萬變的要求。

系統體系的執行重點並非在於單一反制能力，而是透過網路化來整合各型感測器與武器。目前各界所取得的共識是，這個問題沒有單一性軍品解決方案，至少現況是如此。³³小型無人機的威脅變化多端，而敵人多變的戰術戰法，也非任何單一科技就能持續削弱敵小型無人機的戰力。因此小型無人機反制系統，必須能整合多重不同種類的情資來源，以蒐集精確且能據以行動之資訊。就傳統整體防空系統而言，早期

預警雷達只能提供目標的距離，而非空中威脅的詳細情資。相對地，目獲雷達則能提供目標詳細情資，但卻無法提供早期預警雷達所能掌握之目標距離。同樣地，熱影像感測裝置或光學攝影機也許無法以高精確度方式，偵知小型無人機的活動範圍，但兩者如果能結合使用，就可比對其他情資，提供所偵獲小型無人機之額外情資來源。運用諸如「牛頭人」(Minotaur)感測系統等戰力，小型無人機反制系統可以整合、安排、比對和重複對照各種感測器輸入資訊，以充分提高偵知機率。³⁴ 人工智慧可以過濾龐大的感測器資訊，而深度學習運算程式則能不斷強化威脅確認精確度，並判定制壓或摧毀目標的適切方法。³⁵

隨著物聯網陸續運用於戰場，大量新式感測器亦隨之問世，但美軍必須找出更佳的方法結合感測器並有效分發各種資料。美陸戰隊第5團第3營在「1-17號整合訓練演習」(ITX 1-17)中即凸顯此項問題：「戰場上因部署小型無人機、無人機、多功能無人科技組合光學系統(MUTT optics)、軍刀(SABER)系統等諸多裝備所增加之感測器，目前並未透過地面網路進行資源共享。」小型無人飛機反制系統的構建基礎主要在於某種通信架構——就像可能是中高度長續航力無人機——能鏈結各式感測器、軟體和武器系統。³⁶ 美軍不僅需要運用通信架構傳輸資訊，同時也需要針對資訊整合方式進行標準化——使數據鏈路實體架構到軟體語言及通信協定皆能前後連貫。美軍必須運用標準作業方式，讓不同運用的軟體能彼此構連，以利各種類型工具能有效整合，並製造其他新的作業工具。這是絕對必要的資訊科技骨幹：

如同HTML標準使用規範，迄今仍是被眾多網站廣泛分享使用，此等標準使用規範實為促成新領域誕生的誘因，而文化風格、用戶單位和企業方能藉此形成。此一原創力量的核心是簡明的技術規範：遵守協定規定，否則就隨實際狀況採取應變彈性作為。³⁷

其結果將是一種能以漸進累積但靈活應變方式修正的架構。美軍必須找出對付敵軍小型無人機的方法，但回歸此一問題的複雜與多重面向的本質，卻是需要一套能整合多種工具的作業系統。模組化的本質，將可使各單位能依據實際條件的容許範圍及敵人應變方式來量身打造不同裝備。在科技不斷進步之下，更高程度自主能力將伴隨更大的彈性作為。例如，人員在必要條件下仍可留在「環路中」(in the loop)，掌握感測器輸入資料並判別目標為友軍或敵軍，直到人員能更有效率執行該系統所指派的任務為止。建立一套整體性、模組化無人飛機反制網路的好處，在於該網路可讓現行的工具立即共同搭配使用，且易於與未來各種科技發展相容。

生鏽的軍事之輪

為了讓小型無人飛機反制系統能充分適應戰場環境作戰需求，美軍各機構應儘快瞭解其變化並加以因應處置。這意味著應充分運用諸如「快速反應能力辦公室」(Rapid Capabilities Office)及海外應變作戰基金等既有工具，以加速測試與部署。美軍應同時支持讓快速武獲作業的替代作



以色列航太工業公司所產製之哈比(Harpy)反雷達滯空巡航武器。(Source: Paris Air Show, 2007/I. Jastrow)

法制度化。³⁸ 此外，美軍應強化在他國境內的應變能力，就像遣派前進部署軟體工程師直接修改軟體程式代碼，³⁹ 而非讓這些新版軟體陷入冗長的行政申請程序之中。

由於商用科技的重要影響力與其他國家研發預算的增加，美國已無法繼續憑恃其科技優勢。⁴⁰ 多數商用小型無人機製造生產都位於中國大陸境內，而昔日原本最有發展前景的美國製造公司根本無法與中共抗衡。⁴¹ 當軟體所構成的各種通用科技能整併各種突破性能力時，美軍必須找出最有效運用現行科技的方法，而非只追求單獨管道。⁴²

美軍在創新過程的競爭對手是那些在自家後院上任意拼湊各式零件的人——就如同過去應急爆炸裝置的發展歷程。是以，美軍除了發展一套足以快速肆應環境的靈敏小型無人機防禦系統外，還必須確保所有機構皆能快速因應不斷變化環境而適時進行調整。這與民營企業在日益快速經濟體中所習得的經驗教訓是相同的——「所有企業不應只有在某件事情上表現卓著，而是應非常擅長學習如何從事各種新工作。」⁴³ 美軍各機構應具備高度靈敏性，以啟動生鏽的軍事之輪。

美陸軍史凱爾斯(Robert Scales)少將在《戰爭

規模：岌岌可危的美軍未來》(*Scales on War: The Future of America's Military at Risk*)一書中描述今日與明日的戰場為「形式多變……分散、非線性及基本上無一定空間形式且不受時間限制。」⁴⁴ 美軍在未來幾年很可能看到的小型無人機與小型無人機反制系統樣貌，將是一系列行動、反制、反反制作為，而美國與其敵人都在不斷肆應環境以爭取領先地位。美軍已不能繼續依賴線性與過時的工業化來發展各種軍需科技。⁴⁵ 正如同史凱爾斯所描述的戰場一樣，在反應上必須「分散、非線性及無固定形式」。阻止敵軍小型無人機，僅是一個美軍機構設法肆應變化以解決不斷變化問題所運用系統之一部而已。反制小型無人機威脅將不僅需取得突破單一科技之外的方法而已，美軍還必須有效運用系統來處理阻礙解決方案上的大型結構性漏洞。

作者簡介

Warren W. Choi係美陸戰隊無人飛行載具中隊區隊長兼助理作戰官；Olivia A. Garard係美陸戰隊無人飛行載具中隊區隊長兼航空安全官。

Reprint from *Marine Corps Gazette* with permission.

註釋

1. Jacob Brogan, "How Intel Lit Up the Super Bowl with Drones—and Why," *Slate*, (Online: February 2017), available at <http://www.slate.com>
2. Keely Lockhart, "China Launches 1,000 Illuminated Drones into Night Sky in Record-Breaking Display," *The Telegraph*, (Online: February 2017), available at <http://www.telegraph.co.uk>
3. Carl von Clausewitz, *On War*, trans. Col J.J. Graham, (New York: Barnes and Noble Inc., 2004).
4. Adam Rawnsley and Austin Bodetti, "The Warbot Builders of the Middle East Spill Their Secrets," *Wired*, (Online: February 2017), available at <https://www.wired.com>
5. T.X. Hammes, "The Democratization of Airpower: The Insurgent and The Drone," *War on the Rocks*, (Online: October 2016), available at <https://warontherocks.com>
6. Ryan Faith, "Inside 'Black Dart,' the U.S. Military's War on Drones," *Vice News*, (Online: October 2014), available at <https://news.vice.com>
7. Ulrike Franke, "Flying IEDs: The Next Big Threat?" *War on the Rocks*, (Online: October 2016), available at <https://warontherocks.com>
8. David Hambling, "The Quadrotor Drone That Carries a Warhead," *Popular Mechanics*, (Online: April 2016), available at <http://www.popularmechanics.com>.
9. Author's personal interview with LtCol Noah M. Spataro, UAS Capabilities Integration and Requirements Officer.
10. Judy Dutton, "Drones' Future: Supersonic Swarms of Robot Bugs," *Wired*, (Online: June 2012), available at <https://www.wired.com>
11. David Cenciotti, "F-22 Raptor Grounded by Swarm of Almost 20,000 Bees," *The Aviationist*, (Online: August 2016), available at <https://theaviationist.com>.
12. "Japan Radioactive Drone: Tokyo Police Arrest Man," *BBC News*, (Online: April 2015), available at <http://www.bbc.com>.
13. David Hambling, "These 6 Drones Are Ready and Waiting to Tear Gas You," *Popular Mechanics*, (Online: February 2016), available at <http://www.popularmechanics.com>.
14. Friederike Nielsen, "Drones Could Deliver Biological Weapons," *Dedrone*, (Online: December 2015), available at <http://www.dedrone.com>.
15. Matt Novak, "Power Company Sends Fire-Spewing Drone to Burn Trash Off High-Voltage Wires," *Gizmodo*, (Online: February 2017), available at <http://gizmodo.com>.
16. Andy Greenberg, "Malware Lets a Drone Steal Data by Watching A Computer's Blinking LED," *Wired*, (Online: February 2017), available at <https://www.wired.com>.
17. Andrew Grossman and Jack Nicas, "White House Drone Crash Said to Be 'Recreational,'" *The Wall Street Journal*, (Online: January 2015), available at <https://www.wsj.com>.
18. Thomas Gibbons-Neff, "The U.S. is Apparently Using Anti-Drone Rifles Against the Islamic State," *The Washington Post*, (Online: July 2016), available at <https://www.washingtonpost.com>. 這套科技裝備的配發，賦予陸戰隊基層單位具有以兵力防護為由的電子攻擊能力，該型裝備的干擾器可使無人機無法對目標自動導航。
19. Kelsey D. Atherton, "American Anti-Drone Rifle Deployed in Iraq," *Popular Science*, (Online: July 2016), available at <http://www.popsoci.com>.
20. Nick Summers, "'BeeRotor' Drone Uses an Insect-Style Eye to Navigate Tight Spaces," *Engadget*, (Online: March 2015), available at <https://www.engadget.com>.
21. Lora Kolodny, "Exyn Unveils AI to Help Drones Fly Autonomously, Even Indoors or off the Grid," *Tech Crunch*, (Online: 21 February 2017), available at <https://techcrunch.com>. See also Gabriel C. Birch, John C. Griffin, and Matthew K. Erdman, "UAS Detection, Classification, and Neutralization," *Sandia National Laboratories*, (Online: Market Survey, 2015), available at <http://prod.sandia.gov>.
22. Lauren Walker, "Obama Responds to Drone Crashing at White House," *Newsweek*, (Online: January 2015), available at <http://www.newsweek.com>.
23. Jules Hurst, "Automated Eyes in the Sky," *The Strategy Bridge*, (Online: February 2017), available at <http://thesstrategybridge.org>.

24. J. Noel Williams, "Killing Sanctuary: The Coming Era of Small, Smart, Pervasive Lethality," *War on the Rocks*, (Online: September 2017), available at <https://warontherocks.com>.
25. Thomas Gibbons-Neff, "Israeli-Made Kamikaze Drone Spotted in Nagorno-Karabakh Conflict," *The Washington Post*, (Online: April 2016), available at <https://www.washingtonpost.com>.
26. Allistair Moses, Matthew J. Rutherford, and Kimon P. Valavanis, "Radar-Based Detection and Identification for Miniature Air Vehicles," *2011 IEEE Multi-Conference on Systems and Control*, available at <http://www.ssrc.dtc.umn.edu>.
27. "Copping a 'Copter: Dealing with Rogue Drones," *The Economist*, (Online: May 2015), available at <http://www.economist.com>.
28. Carl Engelking, "Malicious UAV Pilots Can't Hide From This Righteous Drone," *Discover*, (Online: April 2015), available at <http://blogs.discovermagazine.com>.
29. Kelsey D. Atherton, "Watch Japan's Police Drone Catch A Quadcopter," *Popular Science*, (Online: December 2015), available at <http://www.popsoci.com>.
30. Joint Improvised-Threat Defeat Organization, *Joint Improvised-Threat Defeat Organization's Counter-Unmanned Aerial System (C-UAS) Hard Kill Challenge*, (Washington, DC: 2016), available at <https://www.challenge.gov>.
31. Chris Baraniuk, "Small Drone 'Shot with Patriot Missile,'" *BBC*, (Online: March 2017), available at <http://www.bbc.com>.
32. *Radio French Internationale*, "Born Killers: French Army Grooms Eagles to Down Drones," (Online: February 2017), available at <http://en.rfi.fr>. See also Amar Toor, "Holland's Drone-Hunting Eagles are Ready to Fly," *The Verge*, (Online: September 2016), available at <http://www.theverge.com>.
33. United States Army, *Counter-Unmanned Aircraft System (C-UAS) Strategy Extract*, (Fort Eustis, VA: Army Capabilities Integration Center, October 2016), available at <http://www.arcic.army.mil>.
34. Leigh Giangreco, "Newest P-8A Poseidon Upgrade Includes 'Minotaur' Software," *Flight Global*, (Online: August 2016), available at <https://www.flightglobal.com>.
35. Steven Melendez, "The Eye in the Sky Gets a Brain That Knows What It's Seeing," *Fast Company*, (Online: January 2017), available at <https://www.fastcompany.com>.
36. Cummings et al., "Open Your Eyes and See the 21st Century MAGTF," *War on the Rocks*, (Online: September 2017), available at <https://warontherocks.com>.
37. Reid Williams, "Living Data Streams for Humans and Machines," *Medium*, (Online: January 2017), available at <https://medium.com>.
38. Ben FitzGerald and Kelley Saylor, "Creative Disruption: Technology, Strategy and the Future of the Global Defense Industry," *Center for a New American Security*, (Washington, DC: June 2014), available at <http://www.cnas.com>.
39. Author's personal interview with Capt Brett A. Friedman, Wargame Analyst, Ellis Group.
40. Ben FitzGerald, Alexandra Sander, and Jacqueline Parziale, "Future Foundry: A New Strategic Approach to Military-Technical Advantage," *Center for a New American Security*, (Online: December 2016), available at <https://www.cnas.org>.
41. Harry McNabb, "Eight Reasons Why Chinese Drone Manufacturers Are Dominating the Industry," *DroneLife*, (Online: September 2016), available at <http://drone-life.com>.
42. "Future Foundry."
43. Martin Reeves and Mike Deimler, "Adaptability: The New Competitive Advantage," *Harvard Business Review*, (Online: July-August 2011), available at <https://hbr.org>.
44. MG Robert Scales, USA(Ret), *Scales on War: The Future of America's Military at Risk*, (Annapolis, Naval Institute Press, 2016).
45. Aleksandr A. Svechin, *Strategy*, ed. Kent D. Lee, (Minneapolis: East View Information Services, Inc., 2004).