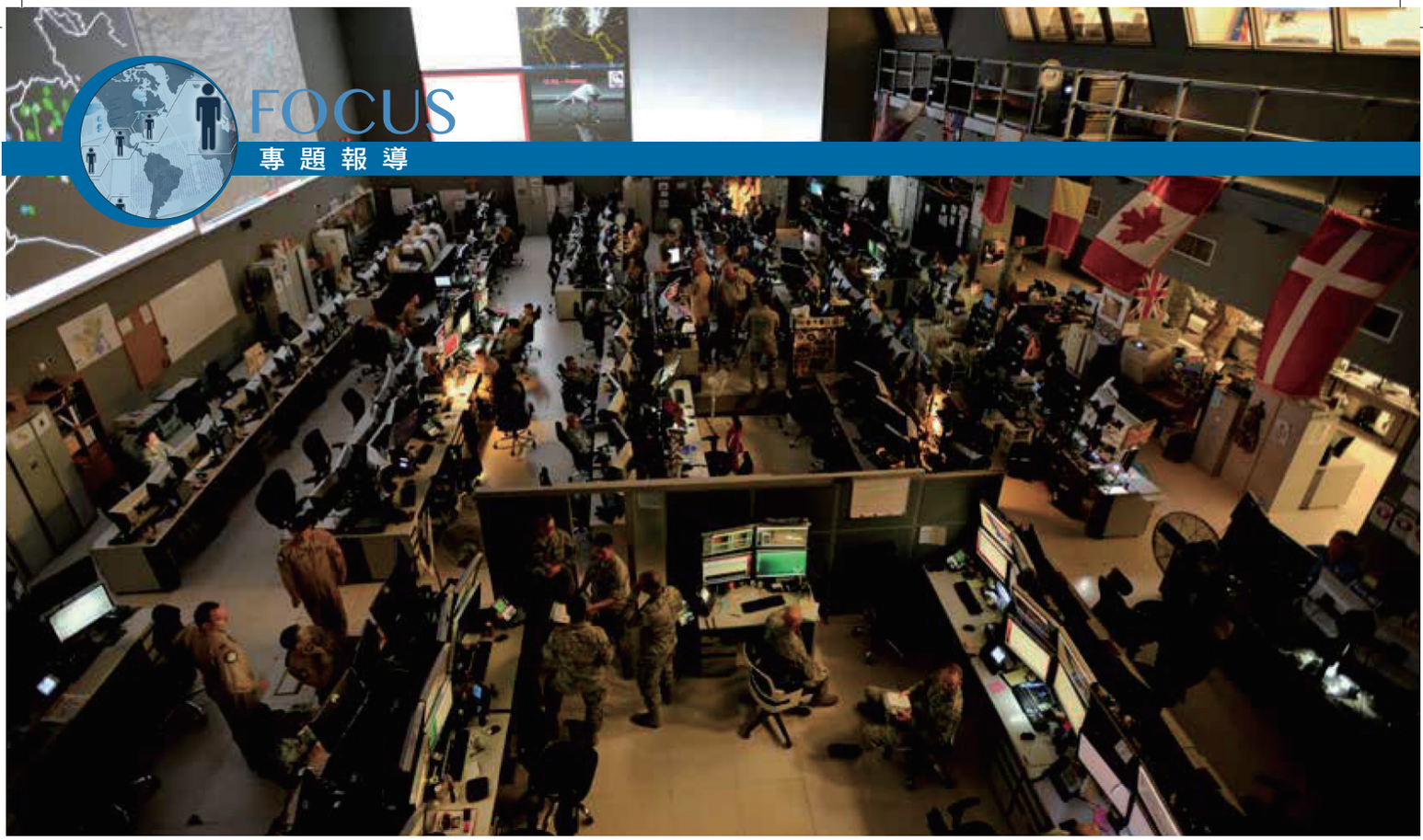


● 作者/Edwin Y. Chua ● 譯者/黃依歆 ● 審者/馬浩翔

新興政戰手段：以網攻卡達為例

Political Warfare with Other Means: 2017 Cyber Attacks on Qatar

取材/2018年第四季美國聯合部隊季刊(*Joint Force Quarterly*, 4th Quarter/2018)

2017年網攻事件造成卡達雪崩式斷交危機，究其主因源自於一則鄰國釋出的假新聞。該起事件以網路遂行政治作戰，並結合所有國力因素的運用，提醒吾人慎防跨國偽造資訊對國家可能造成的重大影響，並應在網路攻擊試圖形塑輿論前迅速回報，即時澄清立場。

現代最兩難的事情之一，就是科技能賦權我們對世界做出卓越貢獻，但也能用來逐步侵蝕我們，造成巨大的傷害。

——美國前總統歐巴馬

2017年5月24日，卡達國營通訊社報導該國國王塔米姆(Tamim bin Hamad Al Thani)表態支持哈馬斯、真主黨、伊朗及以色列。[1] 該則新聞旋即激起與卡達同屬海灣合作理事會(Gulf Cooperation Council)成員的沙烏地阿拉伯、阿拉伯聯合大公國、巴林等成員國與卡達斷交，另外非屬成員國埃及也在隨後跟進。[2] 這四國羅列出13項要求

清單，意在使卡達的國家政策與其他波斯灣阿拉伯國家同調。[3] 然而，卡達通訊社立刻在其官網與推特帳號上否認這則報導，並將之歸咎於是由網路攻擊所造成。[4] 這起網路攻擊透過該通訊社名義散播錯誤且混淆視聽的資訊，象徵著利用網路手段遂行政治作戰進入新階段。本文試圖分析該次攻擊目的、目標閱聽人、攻擊手段、成果，以及發展中科技之運用，亦說明防禦上述攻擊需要來自個人、組織、政府與國際社會的多重努力。

政治分析家、前中情局國家情報委員會副主席福勒(Graham Fuller)提出假設，2017年網路攻擊的目標在迫使卡達外交政策與沙烏地阿拉伯一致、終止其與伊朗的友好關係、切斷與土耳其的軍事合作，以及終結其對半島電視臺新聞網的資助。[5] 卡達由於與伊朗共同開發南帕斯(South Pars)天然氣田，因此兩國的外交關係相當密切。[6] 而在2014年，卡達也與土耳其簽署一份防禦協定，同意土國在卡達境內建立軍事基地。[7] 福勒認為這些國際合作讓卡達得以擺脫沙烏地阿拉伯的影響，獨立擘劃外交政策。中東地區在「阿拉伯之春」後，威權主義政權統治倍感威脅，許多阿拉伯國家領導人將半島電視臺新聞頻道視為渠等控制該區域資訊的威脅因素。[8] 該網路攻擊的目標閱聽人並非僅針對卡達的政治菁英，也鎖定海灣合作理事會的其他國家(亦即科威特及阿曼)領導人，還有美國的關鍵決策者。該則假新聞透過凸顯卡達與伊朗及哈馬斯(美國認定的恐怖團體)間的關係，試圖在政治上分化卡達與美國的關係，且預謀讓其他海灣合作理事會成員國在宗教立場上一致，共同支持沙烏地聯盟的伊斯蘭教遜尼派分支，以對抗伊朗的什葉派。

2017年，在卡達國營通訊社報導國王塔米姆表態支持哈馬斯及真主黨等團體後，激起數個邦交國與其斷交。
(Source: Wiki)

為了引起這些閱聽人的注意，作為沙烏地聯盟成員之一的阿拉伯聯合大公國以置入假新聞的方式，發動了針對卡達通訊社的網路攻擊計畫。2017年4月起，駭客開始行動並完全控制卡達通訊社的網絡、電子郵件帳號、網站及社群媒體平臺。[9] 在卡達通訊社的科技專家重掌控制權前，假新聞早已於5月24日至25日大量散布。[10] 該網路攻擊支持一場更廣泛規模的行動，包含諸如外交、軍事與經濟作為等所有國力要素。事發後，沙烏地聯盟切斷與卡達間的外交關係，並限期卡達公民在14天內離境，同時禁止他們的國民赴卡達旅遊或居住。[11] 在沙烏地阿拉伯的外交壓力下，葉門、馬爾地夫與利比亞紛紛與卡達斷交。[12] 沙烏地聯盟國家也對卡達籍飛機關閉領空，並禁止所有掛有卡達國旗或為卡達服務的船隻停泊於任何港口。[13] 沙國也關閉了與卡達相連的唯一陸地邊界。[14] 這些橫跨陸、海、空領域的行動都是為了切斷卡達的補給路線，威脅其經濟狀況。

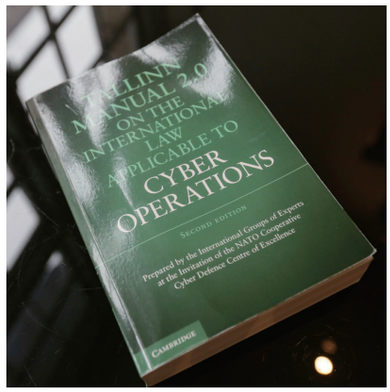
未能得逞

儘管動用了所有國力要素，沙烏地聯盟並沒有成功離間卡達、海灣合作理事會成員國與美國。卡達並未屈服於聯盟所提出的13項要求條件。[15] 但事發後美國國務卿隨即呼籲要透過外交途徑解決危機，而國防部與駐卡達的美國大使也公開肯定卡達政府同意美軍設立烏代德空軍基地(Al Udeid Air Base)的作為，以及卡達對區域安全的承諾。[16] 此外，其他兩個海灣合作理事會成員國科威特與阿曼，也沒跟卡達斷交。在駭客攻擊卡達不到一個月內，美國情報官員將網路攻擊歸咎於阿拉伯聯合大公國，並聲明攻擊行動係由該國政府的高階官員所主導。[17] 事實上，由於土耳其與伊朗直接運送食物與基本補給品予卡達，上述陸、海、空領域的封鎖並未造成嚴重影響。[18] 另外，為了嚇阻沙烏地阿拉伯可能採取的任何軍事行動，土耳其也派駐了更多軍隊至其設在卡達的基地。[19] 即便該網路攻擊搭配運用所有國力的手段，但仍然未能得逞，這也印證了某些網路安全學者的假設，渠等認為網路攻擊鮮少能達到所望目標，成功的強迫手段則需要像美國這種具備壓倒性國力的國家才可能達到。[20]

然而，隨著孤立卡達的計謀曝光，事後也沒有任何針對阿拉伯聯合大公國的網攻行為有所公開懲戒或作為。此一惡例可能會促使未來敵人評估運用網路攻擊來遂行政治作戰。這類攻擊的擴散意味著「網路的戰略邏輯正轉向某種擾亂與持續性騷擾，用以顯示能力與情勢升高的威脅性。」[21]

放眼未來

未來網路攻擊與資訊戰將會利用可操縱聲音與影像的軟體。2016年11月，以生產Photoshop軟體聞名的Adobe公司公布「聲音計畫」(Project VoCo)，這款音效編輯軟體能夠錄音並修改音檔，以原講者的聲音發出其並未說過的字句。[22] 另一家BabelOn公司則正在研發一款軟體，其能同步將某人的聲音翻譯成另一種語言。[23] 另外，美國華盛頓大學的學者則正在進行實驗，研究如何運用人工智慧將音檔轉換成人類真實的發音嘴型，可用來偽造公眾人物的演說影片。[24] 這類科技的廣泛運用模糊了真假間的界線，使有心人士能以不斷進行扭曲事實的行動，去重傷某些領導人或國家的聲譽，以削弱他們的軟實力與影響力。



「北約合作網路防禦卓越中心」先後針對網路戰議題釋出了兩版的《塔林手冊》，期能發展網路規範。(Source: Wiki)

強力且多面向的防禦行動有其必要，藉由個人、組織、政府與國際社會的行動，才能對抗這類新式軟體與人工智慧的濫用。Adobe公司承認旗下軟體可能遭到濫用，而這正是建立公眾覺知、向民眾預警這些潛伏影響力行動的大好機會。吾人需要投注更多心力，發展軟體來即時阻止這樣的影音操縱。

有卡達的前車之鑑，各個政府與組織應準備好採取透明化政策，並在網路攻擊試圖形塑言論時迅速回報、澄清自身立場，以預防不實資訊的散布。另外，政府與組織也要在採取對外作為時堅守上述態度，慎防危機發生時有任何不肖人士利用假造的圖片、影片或音檔。舉例來說，在2018年美國國防戰略的摘要中，即呼籲美國在展現其對盟國的承諾時要保持「戰略上的可預測性」，以遏阻侵略事件發生。[25] 再者，應進一步強化國際規範以對抗各種形式的網路攻擊，並提高有心國家發動類似攻擊之成本。設於愛沙尼亞的「北約合作網路防禦卓越中心」(NATO Cooperative Cyber Defense Center of Excellence)為有助於發展這種網路規範的組織之一，該中心先後針對網路戰議題釋出了兩版的《塔林手冊》(Tallinn Manual)。[26] 即便針對卡達的網攻終告失敗，該事件卻顯示運用新

註釋

1. Bethan McKernan, "Qatar Accuses UAE of Violating International Law by Hacking State News Agency," *Independent*, July 17, 2017, available at <www.independent.co.uk/news/world/middle-east/qatar-uaeinternational-law-hacking-news-agency-aljazeera-cyber-attack-gulf-united-arab-emirates-a7845456.html>.
2. Alex Shanahan, "U.S. Role, Stake in Gulf Feud," *Washington Report on Middle East Affairs* 36, no. 5 (August–September 2017), 46.
3. "Arab States Issue 13 Demands to End Qatar-Gulf Crisis," Al Jazeera, July 12, 2017, available at <www.aljazeera.com/news/2017/06/arab-states-issue-list-demandsqatar-crisis-17062 3022133024.html>.
4. "Foreign Minister: 'Qatar Will Address the Media Campaign Targeting It,'" Qatar Ministry of Foreign Affairs News, May 25, 2017, available at <https://mofa.gov.qa/en/all-mofa-news/details/2017/05/25/foreignminister-%27qatar-will-address-the-mediacampaign-targeting-it%27>.
5. Graham E. Fuller, "Does Qatar Really Threaten the Gulf?" *Washington Report on Middle East Affairs* 36, no. 5 (August–September 2017), 20.
6. "Qatar-Iran Ties: Sharing the World's Largest Gas Field," Al Jazeera, June 15, 2017, available at <www.aljazeera.com/indepth/interactive/2017/06/qatar-north-dome-iran-southpars-glance-lng-gas-field-170614131849685.html>.
7. "President Erdogan Visits Turkey Military Base in Qatar," *Hurriyet Daily News* (Istanbul), November 16, 2017, available at <www.hurriyetdailynews.com/president-erdogan-visitsturkey-military-base-in-qatar-122498>.
8. Fuller, "Does Qatar Really Threaten the Gulf?" 20.
9. "Qatar Says Cyberattack 'Originated from the UAE,'" Al Jazeera, July 20, 2017, available at <www.aljazeera.com/news/2017/07/qatar-sheds-light-cyberattack-official-media-170720151344996.html>.
10. Karen DeYoung and Ellen Nakashima, "UAE Orchestrated Hacking of Qatari Government Sites," *Washington Post*, July 16, 2017, available at <www.washingtonpost.com/world/national-security/uae-hacked-qatari-government-sites-sparking-regional-upheaval-according-to-us-intelligence-officials/2017/07/16/00c46e54-698f-11e7-8eb5-cbccc2e7bfbf_story.html?utm_term=.fef1e4846f4a>.
11. "Qatar Crisis: What You Need to Know," BBC, July 19, 2017, available at <www.bbc.com/news/world-middle-east-40173757>.
12. Noah Browning, "Arab Powers Sever Qatar Ties, Citing Support for Militants," Reuters, June 5, 2017, available at <www.reuters.com/article/us-gulf-qatar/arab-powers-sever-qatarties-citing-support-for-militants-idUSKBN-18W0DQ>.
13. "Qatar Crisis: What You Need to Know."
14. Ibid.
15. "Qatar Crisis: Saudi-Led Coalition Drops 13 Demands to End the Boycott," *Haaretz* (Tel Aviv), July 19, 2017, available at <www.haaretz.com/middle-east-news/qatar-crisis-saudi-led-coalition-drops-13-demands-to-end-the-

型網路手段製造假新聞的可行性。運用網路手段可能會日益普及，特別是科技的進步使得發動網攻、偽造或扭曲資訊更為容易，而被發現的風險及不利因素仍然很低。美國應該建立面對上述風險的公眾覺知，並以強化公共外交作為先發制人的措施，並在國際上影響其盟國及夥伴，以建立規範來對抗這些攻擊，另外也應適時譴責發動這類攻擊的國家。預防性手段將能建置規範，來倡導使用網路的正當方法，並達到保護美國及其盟國的目標。

作者簡介

Edwin Y. Chua係新加坡陸軍少校。渠於美陸戰隊指參學院進修時撰寫本文，並獲得2018年美國參謀首長聯席會議主席戰略論文比賽戰略類組首獎(並列)。

Reprint from *Joint Force Quarterly* with permission.

boycott-1.5431407>.

16. "Tillerson Says Break with Qatar by Saudi Arabia, Others Won't Affect Counter-Terrorism," CNBC, June 5, 2017, available at <www.cnbc.com/2017/06/05/tillerson-says-break-with-qatar-by-saudi-arabia-others-wont-affect-counter-terrorism.html>; DeYoung and Nakashima, "UAE Orchestrated Hacking of Qatari Government Sites"; and Phil Stewart, "U.S. Military Praises Qatar, Despite Trump Tweet," Reuters, June 6, 2017, available at <www.reuters.com/article/us-gulf-qatar-usa-pentagon/u-s-military-praises-qatar-despitetrump-tweet-idUSKBN18X2G2>.
17. DeYoung and Nakashima, "UAE Orchestrated Hacking of Qatari Government Sites."
18. "Iran, Turkey Send Food to Qatar Amid Fears of Shortages," Voice of America, June 11, 2017, available at <www.voanews.com/a/tillerson-cavusoglu-qatar/3895653.html>.
19. "How Turkey Stood by Qatar Amid the Gulf Crisis," Al Jazeera, November 14, 2017, available at <www.aljazeera.com/news/2017/11/turkey-stood-qatar-gulfcrisis-171114135404142.html>.
20. Brandon Valeriano, Ryan C. Maness, and Benjamin Jensen, *Cyber Strategy* (New York: Oxford University Press, forthcoming), 111.
21. Brandon Valeriano, Ryan C. Maness, and Benjamin Jensen, "Cyberwarfare Has Taken a New Turn: Yes, It's Time to Worry," *Washington Post*, July 13, 2017, available at <www.washingtonpost.com/news/monkey-cage/wp/2017/07/13/cyber-warfare-has-takena-new-turn-yes-its-time-to-worry/?utm_term=.474c4314fa45>.
22. Matthew Gault, "After 20 Minutes of Listening, New Adobe Tool Can Make You Say Anything," *Motherboard*, November 5, 2016, available at <https://motherboard.vice.com/en_us/article/jpgkxp/after-20-minutes-of-listening-new-adobe-tool-can-make-you-sayanything>.
23. Nathan Ingraham, "BabelOn Is Trying to Create Photoshop for Your Voice," *Endgadget*, June 22, 2017, available at <www.engadget.com/2017/06/22/babelon-is-trying-to-create-photoshop-for-your-voice/>.
24. James Vincent, "New AI Research Makes It Easier to Create Fake Footage of Someone Speaking," *The Verge*, July 12, 2017, available at <www.theverge.com/2017/7/12/15957844/ai-fake-video-audio-speech-obama>.
25. *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge* (Washington, DC: Department of Defense, 2018), 5, available at <www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf>.
26. "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations to Be Launched," NATO Cooperative Cyber Defence Centre of Excellence, February 2, 2017, available at <https://ccdcoe.org/tallin-nmanual-20-international-law-applicable-cyberoperations-be-launched.html>.