Democratization of Irregular Warfare: Emerging Technology and the Russo-Ukrainian War

非正規戰的大衆化：新興科技與烏俄戰爭

譯者簡介

劉宗翰陸軍中校，國防管理學院93年班，政治大學外交系戰略所碩士；曾任經理官、保修官，現任國防部政務辦公室史政編譯處編譯官。

資料來源：軍事評論雙月刊(Military Review)，2024年11、12月，頁45～54。

作者：特雷斯頓・惠特(Treston Wheat)博士為英國前瞻觀點(Insight Forward)公司的情報研究專家，亦擔任萊利風險(Riley Risk)公司的地緣政治特別顧問，美國喬治城大學兼任教授。

大衛・基里琴科(David Kirichenko)為亨利・傑克遜協會(Henry Jackson Society)的副研究員。

Warfare went through drastic changes over the past millennia, but a consistent theme throughout these changes has been the increasing democratization of conflict. What was once chivalric orders gave way to mercenaries and militias, and then Napoleon Bonaparte radically altered war by raising popular armies not bound by the same hierarchical requirements as other militaries. The nineteenth and twentieth centuries saw mass mobilization through the draft, and the citizen-soldier became a critical symbol of militaries in republics and democracies. During World War II, people normally disenfranchised from society and politics were even included

 DOI：10.6892/AB.202508_61(602).0006

in the war effort, such as women taking a far more active role than ever before in conflict.[1] The history of war over the past five hundred years includes the further democratization of military power. Today, technological development has furthered democratization to a level never seen before because weapons of war like drones and cyber capabilities are available to the masses at an extremely low cost as a barrier to entry.

千年以來戰爭歷經重大變化，但在這些變化中有一個始終不變的主題，就是衝突逐漸走向大眾化。曾經叱咤風雲的騎士團後來讓位給傭兵與民兵，然後拿破崙組建大不同於同質階層限制的大軍軍隊，使得戰爭型態發生巨變。19與20世紀的徵兵制，大規模的軍事動員，公民戰士成為共和國與民主國家軍隊的重要象徵。在第二次世界大戰期間，原本社會與政治上的邊緣人，也不免捲入戰事之中，例如女性在戰爭的角色比以往更為積極。[1] 五百年來的戰史軌跡，軍事力量益發往大眾化趨勢發展。如今，科技發展進一步將戰爭的大眾化推向空前的水平，因為像是無人機與網路戰等武器，能以極低的成本大量取得並加以運用。

Russia's invasion of Ukraine provides a useful case study in how democratization has happened in three critical areas of modern warfare: drones, cyberattacks, and influence operations. The availability of the technology for regular citizens to participate in warfare has changed the way conflicts are fought, and Ukrainian citizens have demonstrated mechanisms that citizens of other countries can utilize in their own conflicts. This aspect of war is important for government analysts and scholars to understand because wars of the future are extremely likely to include this element. For example, should the United States ever go to war with China over Taiwan, netizens will likely spend an extraordinary amount of time on cyberspace defending their country's online and physical infrastructure. The Russo-Ukrainian War provides an ongoing natural experiment in how democratization of warfare is taking place, which will allow scholarship to develop concerning this novel approach to war.

1 Williamson Murray and Allan Millett, A War to Be Won: Fighting the Second World War (Cambridge, MA: Belknap Press, 2001), 550-53.

俄羅斯入侵烏克蘭顯示現代戰爭的三個關鍵領域：無人機、網路攻擊、影響力作戰，是現代戰爭逐漸走向大眾化的很有用戰例。普通公民能夠取得戰爭技術參與戰爭，已改變衝突的作戰方式，烏克蘭人民向各國公民展示了在他們自己的衝突中得以運用的機制。瞭解戰爭型態對於政府分析人士和學者來說很重要，因為未來戰爭必須考慮這個要素。舉例而言，若美國未來捲入臺海戰爭，網民可能會在網路空間上花費大量時間以捍衛他們的國家，防範實體基礎設施不被破壞。烏俄戰爭也為戰爭大眾化的進程，提供一項持續進行中順勢而成的實驗，讓學術界能展開這種新型態戰爭的研究。

Crowdsourcing Drones Supplies

Civilian funding of the military is not new to warfare (beyond the normal taxes as well). A significant portion of the American Revolution was funded through the confiscation of property, and average citizens would buy bonds to raise money for the war effort during World War II. However, the Russo-Ukrainian War has shown a different side of this kind of funding as citizens and supporters are directly buying military equipment for the soldiers on the front lines. In modern parlance, people are crowdfunding the war in Ukraine, which shows a novel way that warfare is unfolding and the aspect of the democratization of irregular war.

民眾籌獲的無人機供應

民間資助軍方並不是戰爭中的新現象(除了正常稅收之外)。美國革命時，大部分資金來自沒收民間財產；在第二次世界大戰期間，平民以購買戰爭債券來為政府籌集軍費。然而，烏俄戰爭展現另一種的資助方式，民眾與支持者直接購買軍事裝備，提供前線戰士使用。以現代角度來看，人們正在為烏克蘭的戰爭進行集資，凸顯出戰爭以另一種新的方式發展，以及非正規戰的大眾化面向。

Lt. Col. Pavlo Kurylenko, a top Ukrainian military commander, said, “We’re only holding back the Russians with crowdfunded drones.”[2] He further mentioned that 90

2　於下頁。

percent of first-person view (FPV) supplies are provided by volunteers or military divisions themselves. With drones in such short supply, demand far outstrips supply. It is quickly becoming a battle of drones, and many Ukrainian units on the front line are dependent on volunteers who bring them drones.[3] Volunteer organizations like Dzyga's Paw have not only built military tech supply chains for Ukrainian units but were also at the forefront of driving drone operations innovation at the start of the war.[4] A soldier using an FPV drone can effectively neutralize heavy armor worth millions of dollars with a drone that costs just $300.[5] FPV drones equipped with cameras transmit live video to goggles or screens, letting pilots navigate via the drone's perspective. Primarily used as kamikaze drones with explosive payloads, they provide detailed views crucial for tasks demanding precision and swift pilot responses.

烏克蘭表現優異的軍事指揮官帕夫洛・庫雷連科中校表示：「我們之所以能抵擋俄軍，全靠民眾集資的無人機。」[2] 他進一步提到，九成的「第一人稱視角」(FPV)的無人機都是由志願者捐贈或軍方提供。由於無人機極度短缺，需求量遠超過供應量。這場戰爭迅速演變為一場無人機之戰，許多烏克蘭第一線部隊依賴志願者所提供的無人機，[3] 像是「狗爪」這樣的志願者組織，不僅為烏軍建立軍事技術供應鏈，而且也在開戰後引領無人機作戰的創新發展。[4] 一名士兵使用「第一人稱視角」的無人機，成本僅300美元，[5] 就可以有效摧毀價值數百萬美元的重型裝甲車。若再配備攝影機，就能將即時影像傳輸至目鏡顯示幕或螢幕，讓操作員可以從無人機視角進行飛航操作。這類「第一人稱視角」的無人機大多是攜帶爆炸物並進行自殺式攻擊，它們提供關鍵細節的視角，有助於執行精準打擊任務，同時也強化領航員的反應速度。

2 David Knowles, "'We're Only Holding Back the Russians with Crowdfunded Drones,' Says Ukraine Commander," Telegraph (website), 12 April 2024, https://www.telegraph.co.uk/world-news/2024/04/12/only-crowdfunded-drones-holding-the-russians-back-ukraine/.

3 David Kirichenko, "A War for the Soul of Humanity," Ukrainian Research Institute, 7 December 2023, https://war.huri.harvard.edu/2023/12/07/a-war-for-the-soul-of-humanity/.

4 David Kirichenko, "How Geeks of War Mobilized Ukraine Drone Operations," Asia Times, 19 July 2024, https://asiatimes.com/2024/07/how-geeks-of-war-mobilized-ukraine-drone-operations.

5 David Kirichenko, "Drone Arms Race on Battlefield Ukraine," Kyiv Post (website), 7 January 2024, https://www.kyivpost.com/ post/26425.

Paul Lushenko of the U.S. Army War College notes that drones have given "asymmetric advantages to the militaries of lesser states."[6] Drones have been so effective in warfare that Ukraine had to sideline the U.S. Abrams tanks because drones have been too effective at spotting tanks and hitting them.[7] Soldiers and heavy armor simply can't move around on the battlefield anymore without being spotted. The security world has been concerned about the ubiquity and cheapness of drones for some time, but the Russo-Ukrainian War shows the advantages in irregular warfare of this technology. Russia has significantly more manpower and resources than Ukraine. However, in typical irregular warfare, the weaker side can use novel technologies (or older technology that is adaptable) to outmaneuver the more advanced forces.

美國陸軍戰爭學院保羅・盧申科指出，無人機提供「實力較弱的國家軍隊不對稱優勢。」[6]無人機在戰爭中的效能如此之高，以至於烏克蘭不得不讓美軍艾布蘭戰車退居二線，因為無人機在偵察並攻擊戰車方面太有效率了。[7]戰士與重型裝甲車根本無法在戰場上移動，因為無法避免被無人機偵獲。世界各國本來就對無人機的無所不在與低成本相當重視，剛好烏俄戰爭又證實這項技術在非正規戰中的優勢。俄羅斯在人力和資源方面遠優於烏克蘭，但在典型的非正規戰中，較弱一方可以利用新技術(或改良舊技術)來戰勝較先進的部隊。

Ukraine relies not only on volunteers to source drones for the military but to also drive innovation and production of drones.[8] Numerous volunteers work in garage-style shops to make improvements to drones and are even setting up repair shops near the front line. If soldiers retrieve a damaged drone, they send it to volunteer organizations who help repair the drones for soldiers.[9] Ukrainian charities run supply chains to source drones for soldiers to help them on

6 Ibid.

7 Sally Guyoncourt, "Why Tanks on Both Sides Are Being Sidelined on Ukraine's Battlefields," iNews, 27 April 2024, https:// inews.co.uk/news/world/ukraine-us-tanks-russia-drones-3025730.

8 Alya Shandra, "Inside Ukraine's Secret FPV Drone Labs Racing to Stay Ahead of Russia," Euromaidan Press, 25 January 2024, https://euromaidanpress.com/2024/01/25/how-fpv-drones-became-ukraine-top-weapon/.

9 David Kirichenko, "Ukraine Now Has Drones Rescuing Fallen Drones from Hazardous Battlefields," Euromaidan Press, 7 May 2024, https://euromaidanpress.com/2024/05/07/ukraine-now-has-drones-rescuing-fallen-drones-from-hazardous-battlefields/.

the battlefield.[10] Drones not only have changed the battlefield in Ukraine, but democratization has also occurred through the fact that all sorts of individuals and organizations are able to get their hands on amateur drones that anyone can buy and then supply them directly to the front.

烏克蘭不僅依賴志願者為軍隊提供無人機，還靠這些人推動無人機的創新與生產。[8] 許多志願者在車庫間的工作環境中改良無人機，甚至在前線附近建立維修站。若官兵在回收受損的無人機後，會將它們送往志願者組織，協助官兵修復。[9] 烏克蘭的慈善機構則負責維持無人機之供應，為官兵提供無人機，以協助他們在戰場上作戰。[10] 無人機不僅改變了烏克蘭的戰場，還促成戰爭的大眾化現象，因為不管是個人和組織都可以購買業餘無人機，然後直接將其送至前線。

An ability to supply conflicts more directly will majorly alter warfare as great powers could find themselves at the mercy of crowdfunded militias and guerillas. Although that itself is not necessarily new as diasporas (e.g., the Irish Republican Army) supplied irregular operations through donations.[11] What is new is the ability to buy cheap arms and bring them directly to the soldiers. Importantly, emerging technology like drones is relatively cheap. Previously, weapons systems were extraordinarily expensive, and even donations from the diaspora could only supply limited arms. Drones, on the other hand, can be supplied more easily with only a few hundred dollars. These cheap drones, which previously people could buy off the store shelves, have the ability to neutralize tanks worth millions of dollars and have made tanks play more of a secondary role in the Russo-Ukrainian War.[12]

可以更直接地為衝突提供補給，將大幅改變戰爭模式，因為大國會發現自己受到民兵和游擊隊的制約，這並不是新出現的現象，因為以往海外離散團體也曾透過捐款來資

10 Volodymyr Hrebeniuk, Andrii Bobak, and Taras Paslavskyi, “How Ukrainian Charity Foundations Purchased Drones,” Vox Ukraine, 27 February 2024, https://voxukraine.org/en/how-ukrainian-charity-foundations-purchased-drones.

11 Ed Moloney, A Secret History of the IRA (New York: W. W. Norton, 2003), 460.

12 David Kirichenko, “The Era of the Cautious Tank,” Center for European Policy Analysis, 13 September 2024, https://cepa. org/article/the-era-of-the-cautious-tank/.

助非正規作戰如愛爾蘭共和軍。[11] 新的是在於如今可以購買廉價的武器並直接送至官兵手上。以往武器系統極為昂貴，即使是流離失所民眾捐款能提供的武器也有限，重要的是，像無人機之類的新興科技相對便宜廉價。此外，無人機只需幾百美元就可以輕鬆地獲得，這些人可以直接從商店購買具備摧毀數百萬美元戰車能力的無人機，這讓戰車在烏俄戰爭中的角色變成配角。[12]

As military strategies are considering the future of irregular warfare, they will need to consider this kind of crowdsourcing from either the diaspora or supportive citizens. There will need to be legal considerations for governments to work through as well. Supplying terrorist organizations (when they are officially designated as such) is illegal in Western countries, and geoeconomic considerations will need to take place. In addition, there will be security concerns even when crowdsourcing technology like drones for militaries and militias that are supported by Western governments. For example, drones made by Chinese manufacturers could have intentional vulnerabilities that leak data back to the enemy.

當軍事戰略家不斷在思索非正規戰的未來時，他們須考量到這種以海外離散團體或支持者發起的集資模式，各國政府也需要針對此類情況制定法律層面相應的作法。在西方國家與地緣經濟上資助恐怖份子組織(該組織為被正式認定時)是非法的。此外，為軍隊或民兵透過集資方式獲得的無人機及其技術，這種作法雖然獲得西方國家的支持，但仍要注意某些安全問題，例如中國製的無人機可能存在刻意設計的漏洞，會將數據洩漏給敵方。

Cyber Operations through a Volunteer Force

Russia's full-scale invasion of Ukraine in February 2022 unleashed the first all-out cyberwar between two nation-states.[13] Many feared that Ukraine would suffer from a "digital

13 David Kirichenko, "Lessons from the First Cyberwar: How Supporting Ukraine on the Digital Battlefield Can Help Improve the UK's Online Resilience," Henry Jackson Society, 20 February 2024, https://henryjacksonsociety.org/publications/lessons-from-the-first-cyberwar-how-supporting-ukraine-on-the-digital-battlefield-can-help-improve-the-uks-online-resilience/.

Pearl Harbor," but that moment never came. Russian cyberattacks fizzled out, and Ukraine withstood Russia's cyber onslaught with help from both public and private partnerships from the West.[14] Ukraine also acted by going on the cyber offensive. Ukraine's Ministry of Digital Transformation spearheaded an effort to bootstrap an IT army to ensure maximum resistance.[15] Volunteer hackers from around the world joined in on the efforts to wage cyberwar alongside Ukraine's government. This IT Army of Ukraine has contributed extensively to Ukraine's cyber offensive against Russia, executing a diverse and effective range of attacks.[16] These include leaking documents from Russia's central bank, disrupting internet services in Russian-occupied territories, incapacitating one of Moscow's major internet providers, and targeting private corporations to hinder economic activities.[17]

志願軍發起的網路作戰

2022年2月，俄羅斯全面入侵烏克蘭後引發兩國第一次的全面網路戰。[13] 許多人擔心烏克蘭會遭遇「數位珍珠港事變」，但這個時刻並未到來。俄國的網攻並未如預期般發揮作用，烏國在來自西方的公私合作夥伴之協助下，成功抵擋下俄國的網路攻勢。[14] 烏克蘭同樣發動網路攻勢，烏國的數位轉型部率先組建一支網軍，以確保能全力抵抗，[15] 自世界各地的駭客主動加入志願網軍，與烏克蘭並肩發動網路戰。這支烏克蘭網軍在對俄羅斯的網攻中發揮重要作用，執行一系列多樣而高效的攻擊行動，[16] 包含洩漏俄羅斯中央銀行的文件、破壞俄軍占領區的網路服務、癱瘓莫斯科一家主要的網路供應商，以及攻擊民營企業藉以阻礙其經濟活動等。[17]

At its peak, the group had several hundred thousand members, but the overall subscriber

14 Ibid.

15 Matt Burgess, "Ukraine's Volunteer 'IT Army' Is Hacking in Uncharted Territory," Wired, 27 February 2022, https://www. wired.com/story/ukraine-it-army-russia-war-cyberattacks-ddos/.

16 David Kirichenko, "Ukraine's Volunteer IT Army Confronts Tech, Legal Challenges," Center for European Policy Analysis, 27 November 2023, https://cepa.org/article/ ukraine-volunteer-it-army-confronts-tech-legal-challenges/.

17 David Kirichenko, "Ukraine's IT Hacker Army Requires a Non-Technical Solution to Scale," New Eastern Europe (website), 19 July 2024, https://neweasterneurope.eu/2024/07/19/ukraines-it-hacker-army-requires-a-non-technical-solution-to-scale/.

count and the associated impact need to be more accurate. While subscriber counts have decreased on its Telegram channel, the IT Army's attacks have grown in effectiveness and scale. The primary tactic of the IT Army involves executing distributed denial of service (DDoS) attacks as it's easier than targeted cyberattacks. This approach is simple yet effective; it consists of coordinating a large number of computers to launch a concerted attack on a specific network or website. By flooding the target with an overwhelming volume of requests, the strategy aims to overload the system, ultimately causing it to crash.

烏克蘭的網軍在巔峰時，擁有數十萬名成員，但實際網路用戶及其影響力程度仍尚待精確評估，儘管其Telegram 頻道的訂閱人數有所下降，但網軍的攻擊效果與規模依然持續增強。網軍的主要戰術是執行「分散式阻斷服務」(DDoS)攻擊，因為這會比針對性網攻更為容易實施，這種方法雖然簡單，但極為有效，其原理是集結大量電腦對特定網路或網站發動集中攻擊，藉由向目標發動大量請求，進一步讓系統超載，最後導致崩潰。

According to assessments by the IT Army, the group has inflicted economic losses on Russia estimated to be between $1 billion and $2 billion.[18] Consequently, the cyberwarfare conducted by the IT Army represents a novel and innovative form of sanctions against their adversaries. Ted, the spokesperson for the IT Army of Ukraine, shared that cyber warfare can "operate as a form of economic sanction, a tool to strategically weaken an adversary's economy: the faster these digital capabilities are deployed, the more immediate the impact on the enemy's fighting capabilities."[19] In fact, the IT Army even caught the attention of officials from the Security Council of the Russian Federation.[20] One Russian official threatened Western officials,

18 David Kirichenko, "How Ukraine Built a Volunteer Hacker Army from Scratch," Euromaidan Press, 16 January 2024, https://euromaidanpress.com/2024/01/16/ how-ukraine-built-a-volunteer-hacker-army-from-scratch/.

19 Ibid.

20 Ivan Egorov, "Russian Security Council: Ukrainian Hackers from the 'IT Army' Are Recruited and Trained in the Baltic Countries [in Russian]," Rossiyskaya Gazeta (website), 5 March 2024, https://rg.ru/2024/03/05/sovbez-rf-ukrainskih-hakerov-iz-it-armii-verbuiut-i-gotoviat-v-stranah-baltii.html.

saying that by "supporting the IT ARMY, they are opening Pandora's box which will eventually turn against its masters."[21]

根據烏克蘭網軍的評估，其對俄羅斯造成的經濟損失估計在10～20億美元之間。[18] 由此可見，該軍對敵人發起的網路戰，代表了一種新穎又創新的制裁形式。烏克蘭網軍發言人泰德表示，網路戰可以「作為一種經濟制裁的形式，一種削弱敵方經濟的戰略工具：這些數位能力愈快完成部署，就愈能直接影響敵人作戰能力。」[19] 事實上，該軍甚至引起俄羅斯聯邦安全會議的關注。[20] 一名俄國官員向西方官員警告道：「支持網軍等於是打開潘朵拉的盒子，最終將反噬其主。」[21]

The IT Army's campaign against Russian internet providers led to a disruption of 40 percent of its resources at one point, leading to extensive disruptions in service.[22] Kommersant, a Russian daily newspaper, wrote that the "number of DDoS attacks on Russian companies doubled year on year in the first quarter. Mostly companies from critical industries ... Roskomnadzor speaks of repelling almost three times more attacks in the first quarter alone than in the entire 2023."[23] Furthermore, while Russia has invested billions of dollars in its building out its own satellite internet network, Ukraine's IT Army launched an attack in April 2024 that took out "two of the largest providers, Astra and Allegrosky," for several days.[24]

烏克蘭網軍向俄羅斯網路供應商發動的攻擊，曾一度導致其四成資源的損失，引發大範圍的服務中斷。[22] 俄國《生意人報》報導指出「當年第一季對俄羅斯企業的DDoS攻擊次數就比去年同期增加一倍，受害者大多是重要產業的公司……，俄羅斯聯邦通訊、

21 Ibid.

22 Roman Rozhkov, "DDoS to Every Home: How Hackers Attack Operators and Energy Sales Companies in the Regions [in Russian]," Forbes (website), 12 February 2024, https://www.forbes.ru/tekhnologii/505933-ddos-v-kazdyj-dom-kak-hakery-atakuut-operatorov-i-energosbytovye-kompanii-v-regionah.

23 "Hackers Went According to Distribution [in Russian]," Kommersant (website), April 2024, https://www.kommersant.ru/doc/6649341.

24 Anna Ustinova, "Putin Promised to Allocate 116 Billion Rubles for Satellite Internet [in Russian]," Vedomosti (website), 1 March 2024, https://www.vedomosti.ru/technology/articles/2024/03/01/1023124-putin-poobeschal-videlit-na-sputnikovii-internet-116-mlrd-rublei.

資訊科技和大眾傳媒監督局也表示，僅在第一季，他們所防禦的攻擊次數幾乎就是整個2023年的三倍。」[23] 此外，雖然俄羅斯已投入數十億美元建設自身的衛星網路系統，但面對烏克蘭網軍在2024年4月的一次攻擊中，兩家最大網路供應商Astra 與Allegrosky的服務仍不免遭致癱瘓而中斷數日。[24]

However, assembling a volunteer IT army presents a significant challenge because it introduces civilians to uncharted waters. As the world continues to digitize, there are increasing opportunities for ordinary individuals to participate in cyberwarfare when their nation's needs become apparent. This involvement helps to decentralize key aspects of warfare, showing how wars will increasingly be fought in the digital age. Ukraine has been attempting to draft legislation to provide a more formal legal structure to the fairly informal IT Army.[25] If the Ukrainian legislation in formalizing the "IT Army" is enacted, foreign volunteers seeking legal protection for participating in hacking on Ukraine's behalf would need to join Ukraine's cyber reserves. Vasileios Karagiannopoulos, an associate professor in cybercrime and cybersecurity at the University of Portsmouth, believes that if the IT Army were incorporated into Ukraine's cyber reserves, it could help offer legal protections for civilians participating in cyberwar by offering "legal protection as combatants and potentially shield them from prosecution for their actions during the war."[26]

然而，組建一支志願的網軍是一項重大挑戰，因為這需要讓平民踏入前所未有的領域。隨著世界持續數位化，當國家有需要時，普羅百姓也愈來愈有機會參與網路戰。這種參與有助於使戰爭的關鍵面向去中心化，展現戰爭在數位時代將逐漸以新的方式進行。烏克蘭一直在嘗試起草立法，以提供相對非正式網軍一個較正式的法律架構。[25] 但若烏國正式立法將網軍合法化，則代表烏國參與駭客行動的外國志願者想要獲得法律保護，就需要加入烏軍的網路後備部隊。樸茨茅斯大學網路犯罪與網路安全副教授瓦西里歐斯・卡拉吉安諾普洛斯認為，若網軍被納入烏國的後備部隊，將有助於為參與網路戰

25 Shaun Waterman, "Ukraine Scrambles to Draft Cyber Law, Legalizing Its Volunteer Hacker Army," Newsweek (website), 14 March 2023, https://www.newsweek.com/ukraine-drafting-new-law-legalizing-volunteer-hacker-cyber-army-red-cross-1786814.

26 Kirichenko, "How Ukraine Built a Volunteer Hacker Army from Scratch."

的平民提供法律保障，也就是藉由提供「戰鬥人員法律保護，就有可能讓他們免於因戰爭期間的行動而遭到起訴。」[26]

Importantly, not all preparations will need to be technical. One limitation that the IT Army has faced is engaging with nontechnical audiences. To scale the work of effective botnets and DDoS attacks, more people are needed to join the attacks. The average civilian citizen, though, does not consider themselves capable of conducting cyberattacks against an enemy. The reality is that anyone can follow simple instructions to download a tool and allow their computer's processing power and internet access to be added to the botnet and help flood an enemy's networks to bring them down. The IT Army also said that their cyber operations were conducted in support of bringing down Russian CCTV cameras to reduce visibility on Ukrainian drones bombing Russian oil refineries inside Russia demonstrating the ability of volunteer forces to bolster the regular military in cyberspace.[27] If there is a battlefield objective and the military needs some target to be shut down, they can relay the request to the hacker army to initiate an attack to help provide support. An easy example would be Ukraine's hacker army attacking Russian satellite systems or attacking Russian telecom providers in occupied territories, which they have previously done.

重要的是，並非所有準備工作都需要技術背景。烏克蘭網軍面臨的一項限制是難以吸引非技術背景的大眾參與。要擴大殭屍網路與DDoS的攻擊效果，就需要更多的人力加入攻擊。雖然一般平民並不認為自己有能力對敵人發動網路攻擊。事實上，任何人都可以依照簡單的指示來下載工具，並讓自己的電腦運算能力透過網路連線加入殭屍網路的行列，協同攻擊以淹沒敵方網路並使之癱瘓。網軍表示，網路協同行動是為了破壞俄羅斯中央電視台(CCTV)的攝影機，以降低烏克蘭無人機在執行轟炸俄國境內煉油廠時被發現的可能性，這也顯示志願者部隊有能力在網路空間中支援正規軍。[27] 若戰場作戰目標是中斷某些系統，軍方可以向駭客部隊發出請求，由其協助支援並發動攻擊。舉個

27 David Kirichenko, "Ukraine's IT Army Now Aids Drone Strikes on Russian Oil Refineries," Euromaidan Press, 29 June 2024, https://euromaidanpress.com/2024/06/29/ukraines-it-army-now-aids-drone-strikes-on-russian-oil-refineries/.

簡單的例子，就是烏克蘭駭客部隊攻擊俄羅斯衛星系統，又或是攻擊俄羅斯在占領區的電信供應商，都是曾執行過的行動。

As society moves deeper into the digital age, the involvement of ordinary people in warfare will increasingly expand. Also, as economies and vital services become more integrated with the digital realm, vulnerabilities will multiply, presenting new opportunities for attacks. Countries like Taiwan and other democracies under threat should accept this reality and will need to prepare for how its citizenry will engage in cyberwar. Some military theorists have developed the idea of "cyber militias" in which private citizens could be called up or be prepared during a major cyberattack.[28] There will be a number of ways that governments can organize citizens to volunteer for service without having to join the military to contribute to the war effort.

隨著社會日漸進入數位化時代，普通民眾參與戰爭的情況會愈來愈常見。此外，經濟與關鍵服務也逐漸與數位系統整合，脆弱性因此大增，帶來更多讓人攻擊的機會。鑑此，像臺灣及其他受威脅的民主國家，應該認清這樣的事實，需要為公民如何參與網路戰做好準備。一些軍事理論家已經提出建立「網路義勇軍」的概念，即在重大網路攻擊發生時，可以召集或預先規劃好民間公民參與網路攻擊，[28] 所以政府可以透過各種方式組織公民自動自發參與軍事行動，讓他們無須正式加入軍隊也能對戰爭做出貢獻。

Comparably to other aspects of democratization, there are risks from this occurring. Cyberattacks cannot always be contained, even when performed by highly professional hackers. For example, the NotPetya attack committed by a Russian threat actor spread far beyond Ukraine and devastated companies like Maersk.[29] That connection to the corporate world raises a separate issue. The democratization of cyberwar will not just involve hacktivists and citizens.

28 Dan Jerker B. Svantesson, "Regulating a 'Cyber Militia' - Some Lessons from Ukraine, and Thoughts about the Future," The Scandinavian Journal of Military Studies (website), accessed 28 October 2024, https://sjms.nu/articles/10.31374/sjms.195.

29 Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," Wired (website), 22 August 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

Within the Russo-Ukrainian War, major technology companies have also directly participated, such as Microsoft providing intelligence on cyber incidents and SpaceX providing internet access.[30] Democratization of cyberwar means that organizations, some even powerful and well-funded, can also directly intervene in the conflict based on economic, security, or ideological interests. That will further change the nature of warfare and complicate the democratization of conflict as companies could stop hacktivists or oppose government interests as well.

與大眾化的其他面向相比，這種情況也存在風險，也就是即使是由高度專業的駭客執行行動，也難保就一定能控制住網路攻擊範圍。例如俄羅斯的威脅行為者所發動的NotPetya 攻擊就蔓延到烏克蘭以外地區，重創像馬士基這樣的公司。[29] 另一個引發的問題是，網路戰大眾化不僅涉及駭客主義與一般公民，更涉及企業界的影響力，在烏俄戰爭中，主要的科技公司也參與其中，如微軟公司提供有關網路事件的情報，SpaceX公司則提供網路連線服務。[30] 網路戰大眾化意味著一些組織，其中有些甚至擁有強大資源與充足資金，也可能基於經濟、安全或意識形態利益而直接介入衝突。這將進一步改變戰爭本質，並讓衝突大眾化的情況變得更為複雜，因為企業可以阻止駭客主義行動者，也可以抵制政府的作為。

Influence Operations and Social Media

When pundits think about the weaponization of social media, they usually refer to the use of social media to drive political change like the Arab Spring or how Russia used it to try and influence U.S. elections. However, use of social media and open-source intelligence can be used by nation-states to try to influence outcomes on the battlefield itself. Such information operations have been a critical part of warfare for some time, but social media now allows average citizens (even those not party to the conflict) to impact operational capabilities. The purpose of information operations is to gather relevant information on the enemy along with

30 Treston Wheat, "A State in Disguise of a Merchant": Multinational Tech Corporations and Reconfiguration of the Balance of Power in Asia (Jaffrey, NH: Andrew W. Marshall Foundation, October 2022), https://www.andrewwmarshallfoundation.org/library/a-state-in-disguise-of-a-merchant-multinational-tech-corporations-and-the-reconfiguration-of-the-balance-of-power-in-asia/.

disseminating propaganda (white, black, and gray) to create an advantage in the war. White propaganda is truthful information shared to counter opposing narratives, black propaganda is false, distorted, or exaggerated information (i.e., disinformation), and gray propaganda is a combination of white and black.[31]

影響力作戰與社群媒體

當自命的專家談論到社群媒體武器化時，他們通常指的是利用社群媒體來推動政治變革，例如「阿拉伯之春」，或是俄羅斯如何用來試圖影響美國大選。然而，國家也可以運用社群媒體與公開來源情報，以試圖影響戰場上的結果。這類資訊作戰早已是戰爭中關鍵的一環，但如今社群媒體讓一般公民(即使他們並非是衝突的其中一方)也能對作戰行動產生影響力。資訊作戰目的是蒐集敵人相關情資，並散播消息(白色、黑色及灰色宣傳)，以利在戰爭中取得優勢。白色宣傳為反駁對方敘事而傳播的真實資訊，黑色宣傳為虛假、扭曲或誇大的資訊(亦即假訊息)，灰色宣傳則是白色與黑色宣傳的混合體。[31]

Social media is now quintessential to information operations for gathering intelligence and spreading propaganda. For example, militaries and intelligence agencies scout and extract as much information from social media and open-source intelligence to try and direct battlefield strikes. Ukrainian citizens in particular have been prolific at leveraging these tools to gather intelligence and direct attacks. For example, Russian soldiers have been tricked into revealing sensitive information via Tinder.[32] Some disclosed their tactical locations through profile images while searching for companionship. One clever woman used dual Tinder accounts with varied border locations to pinpoint and report over seventy such profiles to Ukrainian authorities. Ukrainian hackers also created fake profiles on platforms like Telegram to lure

31 Loch K. Johnson, The Third Option: Covert Action and American Foreign Policy (New York: Oxford University Press, 2022), 23-24.

32 Jesse O'Neill, "'Sleeping with the Enemy' Russian Troops Try to Pick Up Ukrainian Women on Tinder," New York Post (website), 24 February 2022, https://nypost.com/2022/02/24/ukrainian-women-say-russian-troops-are-flirting-with-them-on-tinder/.

Russian soldiers near Melitopol into sharing on-duty photos.[33] These images helped locate a Russian military base, leading to a targeted Ukrainian military strike days later. In August 2022, a local pro-Russian journalist shared photos online and unintentionally compromised the location of their base.[34] Shortly after, Ukraine struck the base with rockets. The journalist had shared images on Telegram that included visible details sufficient to pinpoint the Wagner base's precise location.

社群媒體如今已是資訊戰中用來蒐集情報與從事宣傳不可或缺的一部分。例如，軍方與情報機構會從社群媒體與公開來源情報中，不斷觀察並儘可能擷取多一些資訊，以試圖引導戰場上的攻擊行動。烏克蘭公民尤其擅長運用這些工具來蒐集情報並引導攻擊。例如俄羅斯士兵曾被誘騙在Tinder交友軟體上透露敏感資訊。[32] 有些士兵在尋求伴侶時，上傳至Tinder的個人檔案照片洩漏了他們所在的戰術位置。某位精明的女性利用兩個設定在不同所在地的Tinder帳號，成功鎖定並回報超過70個俄軍士兵帳號給烏克蘭當局。烏克蘭駭客也在Telegram等社群媒體平台建立假帳號，誘使鄰近烏國梅利托波爾城市的俄軍士兵分享他們在值勤時的照片。[33] 這些照片協助烏軍鎖定一處俄軍基地並在幾天後進行精準打擊。在2022年8月一位親俄的當地記者於網路上分享照片時，無意間暴露了他們的基地位置，[34] 不久之後，烏軍就以火箭彈襲擊了該基地，該名記者上傳至Telegram的照片中包含了足以精準定位瓦格納基地的明顯細節。

Similarly, messaging apps have allowed Ukrainians to spread malicious software under the guise of support. On Russian Navy Day in July 2023, Ukrainian hackers targeted Russian sailors by sending videos with deceptive "good wishes" via messaging apps. These videos, which showed Ukrainian attacks on Russian ships, contained malware that breached the sailors' phones, extracting confidential data for Ukrainian use. Many sailors thanked the senders before realizing the videos' true intent.

同樣地，即時通訊軟體也讓烏克蘭人可以假借支持軍方之名來散播惡意軟體。在

33 Mehul Srivastava, "Ukraine's Hackers: An Ex-Spook, a Starlink and 'Owning' Russia," Financial Times (website), 3 September 2022, https://www.ft.com/content/f4d25ba0-545f-4fad-9d91-5564b4a31d77.

34 Matt Burgess, "Their Photos Were Posted Online. Then They Were Bombed," Wired (website), 26 August 2022, https://www.wired.com/story/wagner-group-osint-russia-ukraine/.

2023年7月俄羅斯海軍節當天，烏克蘭駭客針對俄羅斯海軍官兵發動攻擊，透過即時通訊軟體傳送假「祝福」的影片。這些影片展示了烏軍對俄軍軍艦的攻擊，其中內含惡意程式，可以侵入俄軍官兵手機並竊取機密資料供烏克蘭使用。許多俄軍官兵在不明所以的情況下，甚至還向發送者表示感謝。

When it comes to propaganda, the Russo-Ukrainian War has been called the world's first TikTok war.[35] It is important to point out that Russia has used social media at a high level to try to direct the outcome of the entire war, but Ukrainians have fought back with their own information operations. Social media helps Ukraine in "crowdsourcing people to fight, materials, donations through cryptocurrencies, and more."[36] Part of that is those in the Ukrainian diaspora sharing their own perspectives, videos, and memes about the atrocities Russia is committing. There is no clear evidence if this democratized propaganda is impactful, but that it is still occurring with regular frequency.

談到宣傳戰，烏俄戰爭被稱為是世界上第一場「抖音戰爭」。[35] 值得注意的是俄羅斯大量運用社群媒體，試圖左右整場戰爭結果，但烏克蘭也透過發動資訊戰來加以反制。社群媒體協助烏克蘭「招募人力來參與作戰、集資物資、使用加密貨幣進行捐款等」。[36] 還有一部分是烏克蘭流離失所民眾貼文發表自身觀點、發布影片，以及指責俄羅斯暴行並在一夕之間透過網路散播而爆紅的內容。雖然目前沒有明確證據顯示這種大眾化宣傳是否真的會產生影響，但這類行為仍然持續頻繁地發生。

Then there is the issue of artificial intelligence (AI) employed in information operations. Large language models are still nascent in this area, and it remains unclear how they can effectively be utilized to gather information or spread propaganda. While North Korean hackers have been using AI tools like ChatGPT to conduct sophisticated attacks, there is no doubt

35 Kyle Chayka, "Watching the World's 'First TikTok War,'" New Yorker (website), 3 March 2022, https://www.newyorker.com/culture/infinite-scroll/watching-the-worlds-first-tiktok-war.

36 Sara Brown, "In Russia-Ukraine War, Social Media Stokes Ingenuity, Disinformation," MIT Sloan School of Management, 6 April 2022, https://mitsloan.mit.edu/ideas-made-to-matter/russia-ukraine-war-social-media-stokes-ingenuity-disinformation.

that nation-states will use a tool like ChatGPT to influence the battlefield. For example, like in the case of fake Tinder women reaching out to Russian soldiers and extracting important intelligence, if either side can identify low-level soldiers on the battlefield, they can use AI to build a dossier or a profile on an individual and more easily trick them into revealing information. Researchers from the Alan Turing Institute used AI agents to collect open-source intelligence on a specified target, and then the system was able to build a "dossier on an individual and permit users to ask questions about them."[37]

接下來就是人工智慧在資訊戰中運用的課題了，大型語言模型的發展雖然還處於初期階段，目前也尚不清楚其能否有效用來蒐集資訊或從事宣傳。即使是北韓的駭客都已經開始使用像ChatGPT 這種人工智慧工具來發動精密攻擊，毫無疑問地也有國家會利用類似ChatGPT的工具來影響戰場。如同在Tinder交友軟體上的假冒女子，藉由認識俄軍士兵取得重要情資的案例一樣，敵我任何一方若能夠識別戰場上的基層官兵，就可以利用人工智慧為這些人建立一份檔案或個人資料。英國艾倫・圖靈研究所的研究人員使用人工智慧代理人，用以蒐集某個特定目標的公開來源情報，然後該系統就可以建立一份「檔案或個人資料，並允許使用者提出關於某人的問題」。[37]

The battlefield has expanded beyond the physical landscape to encompass the extensive, interconnected domain of the internet, where every click or post can have as much impact as a conventional military operation. Western military planners should understand that the next compromised service member could be a NATO soldier who accidentally leaks vital information on social media to our adversaries or falls prey to virtual "honey traps."[38] With the

37 Ardi Janjeva et al., The Rapid Rise of Generative AI: Assessing Risks to Safety and Security (London: Centre for Emerging Technology and Security, December 2023), https://cetas.turing.ac.uk/sites/default/files/2023-12/cetas_research_report_-_the_rapid_rise_of_generative_ai_-_2023.pdf. 譯者註：人工智慧代理人係指由人工智慧代表人類，與環境互動後自行做出決策、執行任務，幾乎不需要人為干預的程式，其最重要的特點就是能獨立完成任務，無需人類逐步引導。至於生成式人工智慧則是生成內容，可以生成文本、影音，但是仍要依賴人類一步步指揮，無法自主行動。

38 David Kirichenko, "The Growing Use of Scamming Techniques and Social Media on the Battlefield," Irregular Warfare Center, 18 October 2023, https://irregularwarfarecenter.org/publications/perspectives/the-growing-use-of-scamming-techniques-and-social-media-on-the-battlefield/.

growing digitization of societies, these types of social media attacks will only increase in the future.

戰場範圍已不再局限於實體空間，而是擴展至廣大且相互連結的網際網路領域，在這個領域中，每一次點擊或發文都可能帶來與傳統軍事行動同等的影響力。西方軍事規劃人員必須理解，下一位遭到危害的軍人，可能會是某位在社群媒體上不小心洩露重要資訊的北約官兵，或是誤中虛擬「美人計」的受害者。[38] 隨著社會日益走向數位化，這類社群媒體攻擊只會愈來愈頻繁而已。

There are risks that come with the democratization of propaganda, though, and countries will have to be considerate of how supporters might cause reputational risks. Governments cannot control the kind of memes and videos that will be shared online, and it is entirely plausible that citizens will spread misinformation, disinformation, and ideologically extreme statements. Should that happen, this could harm the overall war effort by reducing broader support for the conflict. In addition, citizens participating in propaganda can plausibly lead to the spread of conspiracy theories that similarly harm support for particular operations. Social media now allows average citizens to contribute to the war effort by encouraging support, but that support can be a double-edged sword if they stray too far from the messaging or cause false beliefs to spread that turn away public support.

宣傳手段的大眾化也帶來一些風險，各國必須留意支持者可能帶來的聲譽風險。各國政府無法掌控一夕之間透過網路散播而爆紅的人、事、物或網路流傳影片，民眾散播錯誤資訊、假消息，甚至是意識形態的極端言論，這完全是可能發生的情況。如果出現這種情形，有可能會削弱整體戰爭行動，因為這會降低大眾對衝突的支持度。此外，民眾參與宣傳活動也可能會導致陰謀論的傳播，同樣會傷害對特定軍事行動的支持度。社群媒體如今讓普通公民也能透過參與來為戰爭行動貢獻己力，但這種群眾參與支持可能是一把雙面刃，一旦偏離官方立場或散播令人誤解的不實觀念，反而可能會失去大眾對戰爭的支持度。

Conclusion

The Russo-Ukrainian War is the best-case study of modern warfare in a number of areas,

and one area that will need serious analysis and scholarship is the further democratization of conflict. This article looked at the three major areas that is happening: drones, cyberattacks, and information operations. Drones are incredibly cheap to produce and purchase, and supporters of Ukraine fund them to bring them into the conflict with exceptional ease. In the cyber domain, Ukraine was able to raise a cyber militia to support attacks against Russia and bolster the defense of the homeland. Then on social media, netizens and global supporters help shape the narrative of the conflict while also gathering critical information on Russian soldiers and operations. Each of these areas shows how regular citizens can far more easily participate in warfare to support their countries, but the war is ongoing. Further scholarship will be needed to explore this phenomenon more fully.

結　　論

烏俄戰爭是現代戰爭中體現許多領域的最佳研究案例，其中一個需要深入分析與學術探討的部分就是衝突走向全民國防。本文探討這種正在發生中情況的三個主要領域：無人機、網路攻擊及資訊作戰。無人機生產與購買成本極低，讓烏克蘭的支持者可以輕易地買進並投入戰場；在網路領域，烏克蘭成功動員一支網路義勇軍來對抗俄軍攻擊，以及強化本土的防禦；在社群媒體領域，網民與全球支持者不僅協助形塑這場衝突，而且也蒐集關於俄羅斯官兵與軍事行動的重要情報。這些領域都顯示出一般公民如今能以更簡單方式參與戰爭，為自己國家提供支援，但由於烏俄戰爭仍在持續進行中，未來還需要更多的學術研究，才能更全面地探討這種現象。

However, governments and military strategists can already learn a tremendous amount from the information currently available. In bygone decades, militias would serve the purpose of bringing regular citizens into war. The American Revolution was only successful because of the many militias that supported the regular military. Now, military leaders will need to strategize on how to incorporate regular citizens in new and different ways. Could they create a coordinated propaganda campaign using netizens to spread videos and memes to turn a population against its government? Can they create “cyber militias” where patriotic hackers become part of the reserves and called up to attack foreign enemies? Are drones and other

cheap technology the new "war bonds" that would allow people to give resources to the war effort? These are only the start of the questions military and government leaders will need to ask when creating strategies for the future of war.

然而，各國政府與軍事戰略家已經可以從目前既有的資訊中學到大量寶貴經驗。在過去年代，義勇軍存在正是為了讓普通公民能夠參與戰爭，像是美國獨立戰爭之所以能夠成功，就是因為有眾多民兵部隊支援正規軍隊。如今，軍事領導人必須思考如何以全新不同方式將普通公民納入戰略規劃之中，這些人能否齊力策劃一場宣傳活動，利用網民散播影片與迷因，以煽動某個國家的民眾反對其政府？這些人能否組建「網路義勇軍」，讓愛國駭客成為後備力量，並在需要時出動去攻擊外國敵人？無人機及其他平價科技，是否會成為新一代的「戰爭債券」，讓民眾能夠籌募這些資源來支援戰爭行動？以上這些問題都只是軍事與政府領導人在制定未來戰爭策略時需要思考的起點而已。

The great war theorist Carl von Clausewitz articulated in his writings the nature of "small wars." For Clausewitz, a small war included irregular units that supported the regular army in the field by gathering intelligence and guerilla attacks on the enemy (what was then called partisan warfare). In On War, Clausewitz spends time on this concept while discussing general uprisings, and he notes that the system of conscription and militias "run in the same direction when viewed from the standpoint of the older, narrower military system, and that also leads to the calling out of the home guard and arming the people."[39] Of course, he was referring to physically arming the people to support the military through irregular operations, but his concept remains valid for the new democratization efforts that are far more extensive. Rather than armed citizens attacking foreign militaries on the battlefield, "armed" citizens are fighting with propaganda on social media, using cheap drones, and engaging in cyberattacks against the enemy's critical infrastructure. The democratization of warfare is not a new concept and

39 Carl von Clausewitz, On War, trans. Michael Howard and Peter Paret (New York: Oxford University Press, 2007), 184.

has been part of the broader trends of conflict for centuries, but the Russo- Ukrainian War shows how technology has furthered that democratization and how it will differ in wars of the future.

西方兵聖克勞塞維茨在其《戰爭論》中說明「小型戰爭」的本質，他認為小規模戰爭的參與者也包含支援正規軍的非正規單位，而且這些單位的人會在戰場上蒐集情報，並對敵人發動游擊攻擊(當時稱之為庶民戰爭)。在《戰爭論》中，克氏在討論全民起義時特別提到這個的概念，他指出從舊有且較狹隘的軍事體系觀點來看，徵兵制度與民兵制度是朝著相同的方向發展，這也導致了動員國民警衛隊和武裝人民的結果。[39] 當然，克氏所指的是實際去武裝人民，以支援軍隊進行非正規作戰，他的概念淵遠流長，甚至在如今非正規戰的大眾化現象中依然適用。與其說武裝公民在戰場上攻擊外國軍隊，還不如說現在的「武裝」公民是在社群媒體上進行宣傳戰、使用平價無人機，以及對敵重要基礎設施發動網路攻擊。戰爭大眾化並不是一個新概念，幾個世紀以來它一直是衝突發展的廣泛趨勢之一，如今烏俄戰爭顯示科技如何進一步推動這種非正規戰的大眾化，以及未來戰爭型態將有所不同。

(114年4月24日收件，114年6月18日接受)