# 俄烏戰爭下的軟體供應鏈安全

吳宗翰

網路安全與決策推演所

## 壹、前言

2022 年的俄羅斯—烏克蘭戰爭是一混合戰爭（hybrid warfare）。除了實體戰事對抗外，外界最為關注的焦點無疑是雙方的網路攻防。據報導，戰爭爆發前後，烏克蘭多個政府部門與關鍵基礎設施遭到大規模的分散式阻斷服務（Distributed Denial-of-Service，DDoS）攻擊，並傳出遭到惡意軟體 Wiper 刪除政府機構與基礎設施的資料；烏國政府亦號召國內外「資訊科技（Information Technology，IT）大軍」，在網路空間展開反擊。[1]在戰事的脈絡下，軟體供應鏈（software supply chain）的安全受到重視。實際上，相關議題近年來在資安領域已廣被討論，著名案例如 2020 年牽連美國政府與科技公司甚廣的太陽風（SolarWinds）事件、2021 年中旬的殖民油管（Colonial Pipeline）事件、軟體測試服務業者 Codecov 被駭、託管軟體業者 Kaseya 遭襲與同年底的 Log4j 漏洞事件。然而，隨著俄烏戰爭的爆發，議題本質從資安的角度被轉置於更為嚴峻而複雜的國家安全與戰略的視角。各國政府與產業界擔心對手利用軟體開發特性入侵供應鏈並從事惡意行為，反思傳統軟體供應鏈流程中的「信任」（trust）以及開源軟體（open source）安全議題。本文回顧美國、歐盟以及產業界近年來對相關議題的應對措施；在未能擺脫安全不確定性的情況下，總體趨勢呈現供應鏈重組集團化、安全手段複雜化，以及軟體開發封閉化。

[1] Lauren Feiner, "Cyberattack Hits Ukrainian Banks and Government Websites," *CNBC*, February 23, 2022, https://www.cnbc.com/2022/02/23/cyberattack-hits-ukrainian-banks-and-government-websites.html; Joe Tidy, "Ukraine Crisis: 'Wiper' Discovered in Latest Cyber-attacks," *BBC NEWS*, February 24, 2022, https://www.bbc.com/news/technology-60500618; Ukraine War: Ukrainians Announce the Launch of an 'IT Army' to Fight off Russian Cyberattacks," *euronews*, February 27, 2022, https://www.euronews.com/next/2022/02/26/ukraine-war-ukrainians-announce-the-launch-of-an-it-army-to-fight-off-russian-cyberattacks.

## 貳、軟體供應鏈定義與威脅來源

根據 ISO28000 系列條文的定義，供應鏈指涉產品從生產到最終消費者之間的相關活動過程，其中包括最上游的原料供應來源，到中下游的製造、運輸物流、商店銷售與服務。[2]作為一個整體來看，供應鏈宛如一個生態系（ecosystem）。基於產品的差異，供應鏈可粗分成硬體與軟體的供應鏈。在硬體供應鏈的環節中，內部上下游呈現出接力賽或階段式的單向過程。然而，與前者不同，軟體供應鏈的上下游關係較為複雜。由於軟體開發生命週期（Software Development Life Cycle）的特性，軟體開發過程間，概念架構與程式碼往往會彼此參照與引用，這使得產品的生產上下游界線變得模糊。

就此而言，軟體供應鏈的攻擊存在大量管道。攻擊者藉由入侵產品的生產環節後，經由複雜的網絡，橫向或縱向朝目標單位的相關軟體廠商、委外廠商或合作夥伴展開攻擊。此外，由於軟體是由受信任的廠商建置與發行，一旦使用者安裝或執行受到感染的程式，惡意程式碼也會再進一步擴散。[3]研究顯示，由於比起攻擊高價值目標的成本相對低，效果佳，近年來網路犯罪者逐漸偏好這類型的攻擊行動。根據以色列資安公司 Argon Security 的報告，2021 年的軟體供應鏈攻擊比起 2020 年增加了 3 倍。[4]

不論硬體或軟體供應鏈，「信任」都是推動整體環節順利運作的重要關鍵。但供應鏈的攻擊也是藉由「信任圈」途徑發動。與此同時，為縮短產品的開發週期，現代的程式開發人員時常運用開源軟體和既有的元件和組件（components and packages），然此一現象從資安的

[2] "ISO 28000:2022(en) Security and Resilience — Security Management Systems — Requirements," *ISO*, https://www.iso.org/obp/ui/#iso:std:iso:28000:ed-2:v1:en; "ISO 28001:2007(en) Security Management Systems for the Supply Chain — Best Practices for Implementing Supply Chain Security, Assessments and Plans — Requirements and Guidance," *ISO*, https://www.iso.org/obp/ui/#iso:std:iso:28001:ed-1:v1:en.

[3] "Supply Chain Attacks," *Microsoft*, June 4, 2022, https://docs.microsoft.com/en-us/microsoft-365/security/intelligence/supply-chain-malware?view=o365-worldwide.

[4] Eran Orzel, "Software Supply Chain Attacks: 2021 in Review," *Aqua*, January 25, 2022, https://blog.aquasec.com/software-supply-chain-attacks-2021.

角度言並非沒有疑慮。開源軟體的原旨核心概念在「自由、開放、公開」，目的在於透過大眾的集體知識不斷促進系統的完善，創造良性循環。新思科技（Synopsys）2022 年的《開源軟體安全與風險分析報告》（*Open Source Security and Risk Analysis*）指出，在其調查的 2,409 個代碼庫中，使用開源軟體的佔有高達 9 成以上。[5]換言之，在多數情況下應用程式少有百分之百獨立開發，而是在現成的軟體包基礎上再設計與編輯，軟體之間因此往往呈現高度的相依性（dependence）。然而，這種相依性亦可能成為惡意行為者的施力點。

如同前述，設若攻擊者利用開源軟體開放的特性植入惡意程式或後門，即能網絡擴散造成大範圍影響；此外，攻擊者也可以藉由公開漏洞與暴露（Common Vulnerabilities and Exposures，CVE）[6]或尚未存在修補方式的零日漏洞（Zero-day Vulnerability）達到此一效果。新思科技的《開源軟體安全與風險分析報告》指出，在其調查的對象中，有 85%的代碼庫含有超過 4 年未更新的元件；有 88%的代碼庫中的元件並非最新版本。這些都隱藏極大的安全疑慮。美國軟體分析業者 Sonatype 發布的《2021 軟體供應鏈狀態》（2021 State of the Software Supply Chain）調查指出，自 2015 年 7 月到 2021 年底為止，利用開源軟體的攻擊情況已經成長了 6 倍以上。[7]

## 參、俄烏戰爭與態度分歧的開源軟體社群

從目前對俄烏戰爭的觀察，已知交戰雙方或其支持者都利用軟體供應鏈與開源軟體的特性從式攻擊行為。多起資安報告與報導指出俄國駭客集團利用漏洞、惡意程式、釣魚信件等對烏克蘭政府網站或個人展開攻擊。[8]另一方面，支持烏克蘭的一方也展開反擊。戰爭爆發以

---

5 "2022 Open Source Security and Risk Analysis Report," *Synopsys*, https://www.synopsys.com/software-integrity/resources/analyst-reports/open-source-security-risk-analysis.html.

6 指的是公開已知的安全漏洞列表。

7 "2021 State of the Software Supply Chain," *Sonatype*, https://www.sonatype.com/hubfs/SSSC-Report-2021_0913_PM_2.pdf?hsLang=en-us.

8 Bill Goodwin, "'Russian-backed' Hackers Defaced Ukrainian Websites as Cover for Dangerous

後，一位工程師為抗議俄國的入侵行動，利用開源程式 npm 撰寫了名為 peacenotwar 的程式碼，並將其發布到開源社群論壇。他原先的設計是使電腦系統一旦偵測到具有俄羅斯或白俄羅斯的 IP 位址，電腦系統就會自動刪除檔案。然而，由於 npm 與 node-ipc 套件以及 JavaScript 框架的相依性，而後兩者又各自被廣泛用於支持 Linux、Mac、Windows 系統以及建立網頁介面，結果使得大量用戶受到影響。儘管工程師的「反戰行為」受到部分人的讚揚，但也引發部分軟體開發者的憂慮，認為其行為逾越開源軟體的底線，可能會使人們失去對開源軟體的信任。[9]

戰爭陰影嚴重衝擊開源軟體開發與使用社群。為響應西方對俄羅斯的制裁，開源軟體入口網站 Scarf 在 2022 年 5 月初宣布禁止俄國政府或軍事單位從其網站下載資料。支持這類行動的意見主張，限制用戶的目的在於喚起對戰爭的重視，從而達到伸張自由；然而，部分平台如 GitHub 與 GitLab 則持反對看法。贊同此一立場者多認為，自由、開放與非歧視的原則不應該因為戰爭和用戶的來源處而有所打折。[10]這些爭議顯示，戰爭陰影分裂了開源軟體社群，後者對於戰爭的立場目前仍然頗分歧。

## 肆、美歐近年來從法規政策強化供應鏈安全

Malware Attack," *ComputerWeekly.com*, January 17, 2022, https://www.computerweekly.com/news/252512087/Russian-backed-hackers-defaced-Ukrainian-websites-as-cover-for-dangerous-malware-attack;〈俄烏衝突升高，網路攻擊也如火如荼〉，《資安趨勢部落格》，2022 年 3 月 10 日，https://blog.trendmicro.com.tw/?p=71548；陳曉莉，〈烏克蘭統計自開戰以來已遭到近 800 次網路攻擊〉，《iThome》，2022 年 7 月 1 日，https://www.ithome.com.tw/news/151719。

[9] Steven Vaughan-Nichols, "Corrupted Open-source Software Enters the Russian Battlefield," *ZDNet*, March 21, 2022, https://www.zdnet.com/article/corrupted-open-source-software-enters-the-russian-battlefield/; Joseph Marks and Aaron Schaffer, "Ukraine Hacktivism Fights Threaten Open-source Software," *The Washington Post*, March 21, 2022, https://www.washingtonpost.com/politics/2022/03/21/ukraine-hacktivism-fights-threaten-open-source-software/; Flashpoint Team, "The Promise of Open Source Code and the Paradox of 'ProtestWare,'" *Flashpoint*, March 28, 2022, https://flashpoint.io/blog/the-promise-of-open-source-code-and-the-paradox-of-protestware/.

[10] Mike Melanson, "Where Does Open Source Fit into Russia's War with Ukraine?," *THENEWSTACK*, March 4, 2022, https://thenewstack.io/where-does-open-source-fit-into-russias-war-with-ukraine/.

## 一、美國

隨著美中之間的貿易戰與科技戰開打，美國在川普政府時期即透過一連串的行政命令與政策逐步加大對整體供應鏈的管理。2018 年 4 月，「國家標準與技術研究院」（National Institute of Standards and Technology，NIST）發布了《資安框架》（Cybersecurity Framework，CSF）1.1 版，將「供應鏈風險管理」列入核心類別，要求關鍵基礎設施與相關單位評估供應商的資安狀況。同年 11 月，國土安全部成立「資通訊供應鏈風險管理小組」（ICT Supply Chain Risk Management Task Force），力圖促進公私協力的供應鏈管理。2019 年 5 月，川普總統簽署「保護資通訊技術與服務供應鏈安全」（Executive Order on Securing the Information and Communications Technology and Services Supply Chain）的行政命令，禁止美國境內單位與具有競爭關係的外國政府或機構的資通訊科技技術或服務有所來往。2020 年 1 月，美國國防部公布「供應鏈網路安全成熟度認證」（Cybersecurity Maturity Model Certification，CMMC）1.0 版，作為對國防部供應商的資安規範。[11]而後在 4 月時，時任國務卿的蓬佩奧（Mike Pompeo）宣布「5G 乾淨路徑」，要求進出美國的端點傳輸路徑僅能透過受信賴的設備商。8 月時，該計畫進一步擴大為「5G 乾淨網路」，範圍涵蓋營運商、商店、應用程式、雲端與電纜等。透過這些政策，川普政府使中國的華為、中興等公司退出美國市場。

拜登就任總統以後，延續了川普的路線，並持續頒布一系列命令措施，用以強化美國國家網路安全。就背景而言，2021 年以來，美中關係依然緊張，而俄羅斯也因為在烏克蘭議題上的強硬態度，而構成對美國和其盟國在國際上的挑戰。此外，在短時間內接連爆發的幾起

[11] 2021 年 11 月，美國國防部已重新提出 CMMC2.0 版。雖然認證制度與若干細節有變，但核心目標與精神與 1.0 版一致。可見羅正漢，〈美國防部 CMMC 認證計畫推 2.0 版，建立國防供應鏈網路安全成熟度新標準〉，《iThome》，2022 年 3 月 3 日，https://www.ithome.com.tw/news/149664。

重大資安事件例如太陽風、殖民油管等事件，更促使拜登政府意識到相關議題的嚴峻情形。

2021 年 5 月，拜登簽署 14028 號行政命令，提及「零信任網路安全策略」以及「強化軟體供應鏈安全」兩大焦點。接著，在同一年的 8 月，拜登於白宮舉行資安高峰會，宣布「國家標準與技術研究院」將與產業界合作，共同開發一個新框架來提高技術供應鏈的安全與完整性，該倡議獲得微軟（Microsoft）、谷歌（Google）、蘋果（Apple）、亞馬遜（Amazon）及 IBM 等業者的響應。2022 年 1 月底，白宮再次邀集產業界，共同討論開源軟體議題。一般認為，這場會議與前一年底的 Loj4j 事件密切相關。[12]

俄烏戰爭爆發以後，有鑑於俄國可能報復西方國家對烏克蘭的支持與對俄國的制裁行動而採取網攻，拜登於 3 月 21 日發布緊急聲明，呼籲美國企業加強網路防禦並改善網路安全。鑒於美國許多重要關鍵基礎設施均由私部門營運，他要求企業有必要加強管理其數位大門。[13]

而在國際方面，拜登也持續加強與盟國的聯合行動，減輕圍堵中俄造成的壓力。5 月 23 日，拜登宣布其「印太經濟架構」（Indo-Pacific Economic Framework，IPEF）計畫。雖然其中細節尚未明朗，但數位經濟與供應鏈已確定將是箇中重點。

綜觀美國近兩任政府的作為，可明顯看到美國正透過國內外政策以及結合友盟方式，逐步建構以自身為核心的供應鏈體系。

## 二、歐盟

相比於美國，歐盟近幾年亦透過制定法規與發布報告的形式於境

[12] 羅正漢，〈【攜手產業需解決關鍵資安議題，推動企業加速資安強化】強化國家資安，美國白宮推動多項新世代防護對策〉，《iThome》，2022 年 4 月 2 日，https://www.ithome.com.tw/news/150237。

[13] Maegan Vazquez, Donald Judd, Sean Lyngaas and Zachary Cohen, “Biden Warns Business Leaders to Prepare for Russian Cyber Attacks,” *CNN*, March 21, 2022, https://edition.cnn.com/2022/03/21/politics/biden-russia-cyber-activity/index.html.

內建構出一致的標準。此一作為也與歐盟為達成數位單一市場的目標相符。2017 年 9 月，歐盟提出《網路安全法》（Cybersecurity Act）草案，並於 2019 年 4 月獲得通過，同年 6 月開始實施。據此，歐盟建立了資安驗證框架（cybersecurity certification framework），透過歐盟網路安全局（The European Union Agency for Cybersecurity，ENISA）設定規範，針對資安產品、服務與流程所能處理的風險等級做出區別。2019 年 10 月，歐盟會員國代表組成的網路安全組織發布《歐盟 5G 網路安全統合風險評估》（*EU Coordinated Risk Assessment of the Cybersecurity of 5G Networks*），列出 5G 時代可能面臨的挑戰。報告指出，5G 網路吃重軟體的角色，網路漏洞的影響因此變得非常重要。此外，各國的行動網路營運商對供應商的依賴程度也可能與其可能遭受的攻擊相關。2020 年 11 月，歐盟網路安全局發布有關物聯網的安全指南，指出解決物聯網供應鏈安全的關鍵，需要利害關係人建立彼此的信任關係。[14]

2021 年 7 月，網路安全局再發布報告，指出超過 6 成的供應鏈攻擊企圖從程式碼下手，同時也有超過 6 成比例的攻擊依賴惡意程式達到目的。該報告亦對供應商與消費者提出建議，其中，有關軟體元件、相依性以及弱點的狀況應予以掌握。[15]

俄烏戰爭爆發以來，供應鏈危機對於歐盟構成極大挑戰。歐美在達成制裁俄羅斯的共識同時也擴大雙方在供應鏈環節的合作。

## 伍、產業界強化安全的多元化策略

不同於國家採取的法規制定途徑或協同整體公私部門的全社會

[14] 陳曉莉，〈歐盟 5G 網路風險評估報告：對供應商的依賴將擴大駭客攻擊表面〉，《iThome》，201910 月 10 日，https://www.ithome.com.tw/news/133566；“IoT Security: ENISA Publishes Guidelines on Securing the IoT Supply Chain,” *enisa*, November 9, 2020, https://www.enisa.europa.eu/news/enisa-news/iot-security-enisa-publishes-guidelines-on-securing-the-iot-supply-chain.

[15] “Understanding the increase in Supply Chain Security Attacks,” *enisa,* July, 29, 2021, https://www.enisa.europa.eu/news/enisa-news/understanding-the-increase-in-supply-chain-security-attacks.

途徑來提升軟體供應鏈安全，產業界的相對應措施可歸納出兩大趨勢。需要強調的是，這兩大趨勢之間並非互斥關係。首先，因應威脅無處不在，許多企業把安全防護的概念整合進自身產品的開發過程之中。亦即，許多企業將焦點轉向改善提升開發過程中的安全度，依照設計階段、開發測試階段、作業部署等不同項目而有區別；許多方案（solution）與資安產品也應運而生，以下列舉幾項。

第一，部分方案著重在開發過程中的安全測試。這類似於事前預防的概念，透過早期測試找出系統中的漏洞而改善之。第二，建立「軟體物件清單」（Software Bill of Materials，SBOM），揭露使用的開源軟體資訊、第三方元件、授權與漏洞補丁等；這目的在於透明化資訊，使必要時能迅速掌握所需情報。第三，有些方案重視軟體組成分析工具，用以辨識開源程式碼與安全漏洞。第四，軟體開發過程中開發人員的帳號安全。雙因素認證或多因素認證成為重點項目。[16]

另一方面，部分業者應對威脅的策略則是走向封閉化。為避免使用開源軟體可能產生的風險，以及出於保護自身產品的智慧財產權心態，不少廠商在開發過程中盡可能要求開發人員降低使用開源軟體比例，朝自行開發原始碼，建立屬於自身的封閉系統努力。看起來，這似乎是對電腦系統從早期的封閉式架構走向開放式架構發展的逆流，但實際上卻存在不同的脈絡；過去是受限於技術以及對市場排他性的目的，如今則是基於安全需求的考量。

## 陸、結語

俄烏戰爭的爆發，致使軟體供應鏈的安全議題在國家安全的脈絡下較以往更形重要。實際上，針對戰爭行動結合資訊攻擊的反制作為、韌性與防範已是當前顯學，而對軟體供應鏈安全議題的相關討論則可

[16] 鍾銘輝，〈從供應鏈威脅看全球科技產品資安市場趨勢〉，《電腦與通訊》，2021 年 6 月 25，https://ictjournal.itri.org.tw/Content/Messagess/contents.aspx?&MmmID=654304432122064271&MSID=1126502366544734441；羅正漢，〈提升軟體供應鏈安全，提升開發者帳號保護將是不可或缺的關鍵〉，《iThome》，2022 年 6 月 6 日，https://www.ithome.com.tw/news/151263。

提供更細緻的面向。總體言之，疫情（COVID-19）以來的全球供應鏈斷鏈危機由於戰爭緣故雪上加霜，加之戰爭深刻地影響全球地緣政治與國際秩序，更是催化了逆全球化的潮流，導致供應鏈重組；網路空間的裂解情況有增無減，中立者立場近乎難以維持。這點從開源軟體社群對戰爭的分歧態度可見一斑。

隨著美國和其友盟與中俄的對抗態勢趨於明顯，在難以擺脫安全的不確定性（sense of uncertainty）的情況下，為保障供應鏈的安全，全球供應鏈的脫鉤也獲得更強勁的理由背書。觀察美歐與科技廠商的作為，目前出現的趨勢有三。首先是供應鏈出現重組並呈現集團化。這點從美國領頭的乾淨網路、印太經濟架構以及對比中俄結合可見之。第二，為保護軟體供應鏈的安全，相關手段趨於多元化與精緻化，近幾年資安方案大量出現是一明顯現象。最後，針對開源軟體的使用問題，由於使用開源軟體程式碼須公開，對於企業保護機敏資訊與安全的角度言，整體產業趨勢可能逐步走向使用自主封閉軟體（close source）。但這將可能造成技術進入門檻的提升與開發成本增加，長遠來看，可能不利於後進者加入與自由市場發展。

本文作者吳宗翰為倫敦大學國王學院中國研究院博士，現為國防安全研究院網路安全與決策推演研究所助理研究員。他的研究領域為網路主權、認知作戰、國際衝突與安全困境。