第四章　國防產業安全

吳俊德、蔡榮峰*

壹、前言

在今日專業且分工的生產體系下，一項產品的製造要經歷複雜的流程，各部分的零組件分由位在不同國家的不同廠商製造，最後加以組裝才得以完成。跨國產業鏈已經成為今日工業製造的常態，其中如果有一個環節出了差錯，產品的品質就會受到影響。因此，產業安全成為一項重要的課題，這個問題在國防軍事裝備以及武器系統的生產製造上尤其重要。這些產品應用尖端科技與關鍵技術、其性能攸關一國國力、又有許多民間廠商協力，如何在軍事用品的製造過程中確保品質，又不會讓關鍵技術或機敏資料外洩，成為國防產業的重中之重。本章將由各個面向來探討國防產業安全，由於美國在此議題上的規範較為完備，本章將以介紹美國的機制為主。第貳部分是投資審議與安全評價機制，第參部分是公司安全治理與廠商分級，第肆部分是生產流程與供應鏈安全，第伍部分是終端市場及安全認證，第陸部分為小結。

貳、投資審議與安全評價機制

在經濟活動中，不論是生產商品或提供服務，都必須要使用人力、原料、工具、空間等各項因素，因此在經濟學中，勞動、土地、資本、以及企業才能被稱為是生產要素（factors of production）。當一個國家擁有愈充足的生產要素，其經濟活動就可能愈蓬勃；反之，當一個國家的生產要素不足，經濟活動就會受到限制，因此，生產要素是否能充分供給，成為一國經濟發展的關鍵因素。在這四項生產要素中，除了土地之外，其他三項都可以從國外引入。若是一個國家有著開放的經濟環境，讓生產要素能夠較輕易地跨境流通，將對其經濟發展提供正面及積極的貢獻，並能提升在國際上的競爭力。

雖然勞動、資本、以及企業才能都能從國外引入，在這三者當中，最普遍也最受重視的莫過於外國資本進入本國。這是因為勞動力的進入涉及到人的移動，所造成的問題較多也較複雜；資本流動可能造成的問題比較容易管制，且今日的科技可以很迅速地將非常大量的金額轉移到另一個國家。職是之故，世界上大部分國家對於外國資本進入本國，也就是所謂的「外來直接投資」（Foreign Direct Investment, FDI）大多抱持歡迎態度，以利產業與經濟發展。

然而，FDI 也可能對一國造成負面影響。倘若 FDI 是以「兼併與收購（下稱併購）」（Merge & Acquisition, M&A）的方式，亦即外國公司對本國企業透過購

* 吳俊德，網路作戰與資訊安全研究所助理研究員，負責本章第壹、貳、肆、陸節；蔡榮峰，國防資源與產業研究所政策分析員，負責本章第參、伍節。

買或轉讓股權取得經營權，可能會產生許多問題。首先，企業被外資併購後可能將本國勞工裁員或調職，傷害本國人民權益。其次，外資企業可能從事會造成污染的產業，破壞本國環境。第三，外資企業可能將公司資產移至海外，形同淘空本國資產。第四，原物料或是土地開發產業若是被外資掌握，對本國市場穩定反而不利。第五，外資企業若是進入可做軍事用途的敏感科技或是關鍵技術產業，等於協助其提升技術能力，本國技術領先優勢將不保。最後，某些產業攸關人民日常生活及政府運作，例如能源產業與關鍵基礎設施（critical infrastructure），若是由外國企業掌控，恐將危及國家生存。[1]

由於這些負面影響，各國政府在歡迎 FDI 的同時，也都設立投資審議機制對 FDI 加以審核，尤其是對由外國政府所擁有或是控制的企業所進行的投資，更是格外謹慎。在世界各國當中，美國的投資審議機制可說是最為完備而嚴謹，本節將簡介美國的投資審議機制及其最新發展，以為借鏡。

一、美國外來投資審查委員會

美國政府對於 FDI 的審查，「美國外來投資審查委員會」（Committee on Foreign Investment in the United States, CFIUS）扮演舉足輕重的角色。CFIUS 是在 1975 年由福特（Gerald Ford）總統以行政命令所成立，為一個跨部會的委員會，由內閣中不同部會的首長所組成，主要職掌為審視可能會對美國國家利益有重大影響的外來投資。自成立至今，CFIUS 的成員組成歷經數次立法及修法變革，目前是由財政部長擔任主席，成員包括 9 個常設成員、5 個參與及觀察成員、以及 2 個不具投票權但依法必須參與的成員。

CFIUS 的 9 個常設成員為財政部（Department of the Treasury）、司法部（Department of Justice）、國土安全部（Department of Homeland Security）、商務部（Department of Commerce）、國防部（Department of Defense）、國務院（Department of State）、能源部（Department of Energy）、美國貿易代表辦公室（Office of the U.S. Trade Representative）、科學與技術政策辦公室（Office of Science & Technology Policy）；5 個參與及觀察成員為管理與預算政策辦公室（Office of Management & Budget）、經濟顧問會議（Council of Economic Advisors）、國家安全會議（National Security Council）、國家經濟會議（National Economic Council）、國土安全會議（Homeland Security Council）；2 個不具投票權的成員為國家情報總監（Director of National Intelligence）以及勞工部長。[2]

CFIUS 可以針對任何外國投資人對美國進行跨州投資併購行為時，審查其是否威脅國家安全。CFIUS 以多數決作出對外來投資審查之決議，包括在任何情況

[1] 王震宇，〈外人投資併購與國家安全審查機制之比較研究—以中國大陸國營企業海外併購個案為例〉，《台北大學法學論叢》，第 98 期（2016 年 6 月），頁 248-249。

[2] 關於 CFIUS 的成員組成，請見 https://www.treasury.gov/resource-center/international/foreign-investment/Pages/cfius-members.aspx。

下要求該交易停止，但是該決議並不具有法律強制力，僅為提供總統建議之用，美國總統才是外來投資最後的裁決者。[3]

美國政府對國家安全一詞未曾提出明確定義，這使得 CFIUS 在審查 FDI 時有著相當彈性的空間去詮釋國家安全。然而，在一些重大歷史事件及歷次關於 CFIUS 的立法及修法過程中，某些國家安全的內涵有被提及，此也造成 CFIUS 管轄範圍的演變。2001 年 9 月 11 日發生 911 恐怖攻擊事件，讓美國的國家安全面臨恐怖主義的陰影，時任總統的小布希（George W. Bush）除設立國土安全部，也在 2003 年將該部首長納入 CFIUS 的常設成員。這使得 CFIUS 原來傾向以經濟觀點考量外來投資，開始轉變為以國家安全來考量；對 FDI 的審查焦點，也從較狹隘的國防產業，逐漸轉移到關鍵基礎設施。[4]

2007 年美國通過《外來投資與國家安全法》（*Foreign Investment and National Security Act*）並在 2008 年 1 月開始實施，該法除了規範 CFIUS 的法定權限及成員組成外，最重要的是將國土安全與關鍵基礎設施作為識別國家安全的成分，且明訂總統在評估外來投資對國家安全的影響時，必須將這兩項因素列入考量。此外，該法也要求 CFIUS，凡外國投資者是由外國政府持有或控制的，無論其交易本質為何，一律進行調查。在《外來投資與國家安全法》實施以後，CFIUS 的運作更為嚴密完整，其管轄範圍也正式擴大到關鍵基礎設施。[5]

二、美國改革投資審議機制以因應中共威脅

近五年來，美國具有高度機敏性的關鍵技術外流嚴重，在全球的科技領先優勢急遽縮小，究其原因，矛頭直指在 2015 年提出「中國製造 2025」，意圖成為世界製造強國的中國。根據 2018 年 1 月美國國防部的研究，中國取得美國技術的管道，雖然有部分是駭客經由網路侵入美國企業竊取資料而得，但大多數仍是透過投資進入美國市場後，藉由取得公司股東身份得以接觸到機密資訊，或是收買公司內部人士取得技術文件。[6]

基於此，美國政府從行政部門到立法部門對 FDI，尤其是來自於中國的投資提升警覺，參眾兩院在 2018 年對此議題分別提出法案，對 CFIUS 的審查機制進行改革，最後協調出《外來投資風險審查現代化法》（*Foreign Investment Risk Review Modernization Act*, FIRRMA），該法合併於《2019 財政年度國防授權法》（*National Defense Authorization Act for Fiscal Year 2019*, NDAA 2019）之下提出，並於 2018 年 8 月 13 日經川普（Donald Trump）總統簽署通過。FIRRMA 的大部

[3] 王震宇，〈外人投資併購與國家安全審查機制之比較研究—以中國大陸國營企業海外併購個案為例〉，頁 290。

[4] Edward M. Graham and David Marchick, *US National Security and Foreign Direct Investment* (Washington D.C., Peterson Institute Press, 2006).

[5] 邱奕宏，〈美國外來投資審查及「外來投資與國家安全法」之發展〉，《貿易政策論叢》，第 21 期（2014 年 7 月），頁 22-25。

[6] Michael Brown and Pavneet Singh, *China's Technology Transfer Strategy: How Chinese Investments in Emerging Technology Enable A Strategic Competitor to Access the Crown Jewels of U.S. Innovation* (Washington D.C.: Defense Innovation Unit Experimental, 2018), https://admin.govexec.com/media/diux_chinatechnologytransferstudy_jan_2018_(1).pdf.

分條款要等到施行細則公布後才生效，在此之前，美國政府在 FIRRMA 授權下，對關鍵技術領域的 FDI 實施「新前導方案」（New Pilot Program）。該方案於 11 月 10 日正式開始實施，預計試行到 2020 年 3 月 5 日。[7]

「新前導方案」公布 27 項產業為關鍵技術領域，較受矚目者包括先進製造（含飛機及發動機）、機器人、半導體及晶片、人工智慧、生物醫藥技術、無線通信設備、以及奈米技術等。只要是與此 27 項產業當中任何一個環節相關，不論是設計、開發、生產乃至於組裝之 FDI 交易，都必須在交易完成日前 45 天向 CFIUS 履行通報。值得一提的是，FIRRMA 並非針對特定國家，普遍適用於所有外資，但 FIRRMA 仍有具體的防堵中資規定，要求美國商務部必須針對中國 FDI，每兩年向國會及 CFIUS 提出報告，以確切掌握中資對美國整體投資情況。[8]可以說，FIRRMA 對美國投資審議機制的改革，是為了因應中共威脅而來。

過去 FDI 投資審議僅在交易方自願通報 CFIUS 後才啟動審查，且僅限於外國投資人對美國企業取得控制權的投資。FIRRMA 的亮點在於不僅擴充 CFIUS 可審查的交易型態，且有若干類型的交易強制在事前必須向 CFIUS 通報，即便是該項投資並不足以取得美國企業的控制權，即「非控制性投資」（non-controlling investment）。這些必須事前通報的交易包括：第一、涉及國家安全的敏感性不動產交易；第二、使外國投資人得以取得基礎關鍵設施、非公開的關鍵技術、或個人敏感資訊的「非控制性投資」，如取得董事會席次、觀察員、或其他得以介入公司決策的權利；第三、變更既有投資下外國投資人的權利，而該變更可使外國投資人獲得上述關鍵技術資訊或個人敏感資訊。[9]

美國財政部於 2019 年 9 月 17 日公布 FIRRMA 施行細則的草案，並以 1 個月的時間徵求大眾意見。此草案對投資國設有例外條款，來自例外國家之 FDI 只要不違反美國法律，可以不受 CFIUS 擴大之管轄限制。例外國家之認定是由 CFIUS 主席及成員以三分之二多數決投票決定，美國財政部至本年報出版前尚未確認任何國家為例外國。[10]

參、公司安全治理與廠商分級

隨著國防領域所涉及的各類尖端科技發展資本門檻越來越高與私部門於軍民通用科技之創新速度逐漸超越公部門的情況下，各國政府需要民間創新技術，企業則需政策鼓勵才有能力持續研發。受到國際經濟自由化潮流影響，包括台灣在內，先進國家的製造工業於過去 30 年間快速全球化，致使跨國產業鏈成為工

[7] 顏慧欣，〈美國外人投資審查機制之改革方向與影響〉，中華經濟研究院 WTO 及 RTA 中心，2019 年 1 月 17 日，https://web.wtocenter.org.tw/mobile/page.aspx?pid=318503&nid=126。

[8] 顏慧欣，〈美國外人投資審查機制之改革方向與影響〉。

[9] 孫欣、洪唯真，〈美中角力關係下，跨境商務和投資如何管理法律風險〉，安侯法律事務所，2019 年 9 月 9 日，https://home.kpmg/tw/zh/home/insights/2019/09/tw-american-china-trade-war-investment-cross-border-law-risk-management.html。

[10] 李宜靜，〈美國盟友之企業團體要求暫緩投資審查〉，《WTO 及 RTA 電子報》，第 667 期，2019 年 10 月 24 日，https://web.wtocenter.org.tw/Page.aspx?pid=331027&nid=120。

業製造之常態。然而，全球分工對於保護智慧財產權帶來新的挑戰。該如何透過政府機制保持商業彈性而又同時有效管控國安風險，已是國家發展國防工業重要課題。

一、公司安全治理

根據 2001 年美國國防部報告《智慧財產權：航渡商務之海》（*Intellectual Property: Navigating through Commercial Waters*）的概念，國防科技涉及專利、著作權、商標、營業秘密（trade secrets）、技術資料（technical data）與電腦軟體。其中，只有營業秘密這一項無專用期限，只要不公開就可以永久專用；除了保護範圍較廣，它也有專利替代效果，為國防與科技產業之基礎，因而備受重視。[11]

營業秘密必須符合「秘密性」、「具經濟價值」、「採取合理保密措施」三大元素，可概分為「商業性營業秘密」及「技術性營業秘密」兩大類。商業性營業秘密指涉與經營相關之資訊，如客戶名單、定價策略、交易底價、人事管理等。技術性營業秘密則指特定領域的創新技術，如技術、製程等。而營業秘密與企業內部安全管理機制息息相關。

公司安全治理機制可用「管理標的」來區分為「物件管理」、「人員管理」、「組織管理」三大區塊。首先，「物件管理」的核心要旨在於如何依照資訊生命週期來保護記載營業秘密的實體與數位載體，諸如網路資訊安全、機密卷宗歸檔等。其次，「人員管理」強調錄取前的安全查核，以及錄用後員工對於保密責任的認知與遵守。最後，「組織管理」則是指以設計安全機制來宏觀管控前述的物件與人員互動所產生的安全風險，可說是安全管理的成敗關鍵。其兩大核心分別為「機敏資訊管理」與「存取權限管理」。資訊可依其特性、可被利用的方式以及經濟價值等來制定機密等級，且包括標示方式皆屬機敏資訊之管理範疇。而判定需保密之資料，就按照「需知原則」（Need-to-Know Principle），讓只有業務上需要知道的人員才能取得。因此，公司內的成員須依其職務給予差異化的資訊存取權限，藉此避免單一人員掌握完整業務資訊。

[11] 技術資料包括任何涉及研製、後勤過程或訓練等技術相關的圖像與文字記錄，例如圖紙或操作手冊等，但是不包括數位程式碼，因此電腦軟體單獨成類，見 U.S. Government, *Intellectual Property: Navigating through Commercial Waters Appendix B* (Washington D.C.: Department of Defense, 2001), https://www.acq.osd.mil/dpap/specificpolicy/intelprop.pdf。

表 4-1、公司安全治理機制

物件管理	門禁管制、卷宗/數位檔案管理、網路資訊安全、內外網實體隔離
人員管理	背景安全查核、身分識別系統、資安訓練、保密協定、外部合作規範
組織管理	機敏資訊分類/儲存/傳輸制度、實體/數位存取權限設定

資料來源：蔡榮峰整理自公開資料。

除了公司企業內部規範之外，政府為鼓勵創新與扶植包括國防在內的國內產業，也會透過立法保護境內廠商，以遏止非法竊用智慧財產之惡性競爭，尤其涉外商業間諜案之襲擾。

美國為彌補各州政府僅以民事責任追訴之不足，遂於 1996 年通過聯邦層級的《經濟間諜法》（*Economic Espionage Act 1996*）正式追訴侵害營業秘密者之刑事責任，將企圖使外國代理人獲益之行為、無須經過物理移轉之侵害行為，如非法洩漏前雇主營業秘密之離職員工等犯罪納入法。[12]2016 年 5 月 11 日則通過《營業秘密防護法》（*The Defend Trade Secrets Act of 2016,* DTSA），把原本屬於州法層級的民事法律適用範圍提升至聯邦層級一體適用，並加入吹哨者保護條款。[13]類似條款也同樣出現在 2016 年 6 月 8 日歐盟通過的《歐盟營業秘密規程 2016/943》，該規程整合了歐盟成員國營業秘密保護法，就民法範圍內給予法律保護，2018 年 6 月 9 日正式生效。[14]我國《營業秘密法》也參考美國《經濟間諜法》，於 2013 年增訂刑事規範第 13 條之 1 項至第 4 項。

二、廠商分級

發展國防產業涉及一個國家的工業基礎與科技發展。單一國防工業產品之產業鏈往往涉及不計其數的上下游承包商。因此，管理相關市場機制的規範，除了經濟考量之外，還必須兼顧國家安全與國防需求，涵蓋的專業領域十分廣泛。為了在管控風險的同時避免阻礙技術創新，國防產業先進國家就會按照國家現有需求的急迫性、須因應的情勢，以及廠商的技術能力與專業領域等面向來制定分級管理制度，藉此避免其國防供應鏈產生薄弱環節，例如台灣軍購的主要來源國—美國就是最標準的例子。

根據美國《聯邦法規》（*Code of Federal Regulations,* CFR）第 7 章第 700 節，以及《國防生產法》（*Defense Production Act,* DPA）所建立的「國防等級與配置系統」（Defense Priorities & Allocations System, DPAS），擇定國防出口由美國商務

[12] Thierry Olivier Desmet, "The Economic Espionage Act of 1996: Are We Finally Taking Corporate Spies Seriously?" *Houston Journal of International Law*, Vol. 22, No. 1 (1999), pp.105-106.

[13] "Senate Bill 1890-Defend Trade Secrets Act of 2016," 114th Congress of United States, May 11, 2016, Section 7, https://www.congress.gov/bill/114th-congress/senate-bill/1890.

[14] 該規程正式全稱為《歐盟保護技能知識與商業資訊（營業秘密）防止非法取得、使用與公開之規程 2016/943》（*Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure*）, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L0943.

部為業管單位，國防採購項目則由美國國防部提供準則來制定廠商分級制度。採購計畫與廠商人員分成三級制，分別為：國防急迫需求等級的「DX」、國防關鍵等級「DO」以及無等級，個別計畫的分級還會加上分類標號（見表 4-2），例如 DX-A1 為最高等級的航空器製造類別、DO-A3 則為中階等級的船舶製造類別。人員方面，例如持有 DO-A3 的製造商採購人員要採購半導體設備來製造產品時，就必須依照 DO-A3 規定來向下游廠商採購。[15]

事實上，美國的國防採購還將就業機會、新創潛力與社會正義納入考量。根據美國《小型企業法》（*Small Business Act*）第 15 條 g 項，包括美國國防部在內的聯邦政府各部門於招標時，小型企業的「得標主約」（prime contract）以及「轉包」（subcontract）金額加總，不得低於採購總額的 23%。美國國防部的「小型企業計畫辦公室」（Office of Small Business Programs）為業管單位，負責政策協調與相關作業。[16]

表 4-2、美國 DPAS 計畫標號分類表

標號	計畫類型	業管單位
國防採購計畫		
A1	航空器 Aircraft	美國國防部
A2	飛彈 Missiles	美國國防部
A3	船舶 Ships	美國國防部
A4	戰車—汽車 Tank-Automotive	美國國防部
A5	武器 Weapons	美國國防部
A6	彈藥 Ammunition	美國國防部
A7	電子通訊設備 Electronic and communications equipment	美國國防部
B1	軍用建築之供應 Military building supplies	美國國防部
B8	廠商國防生產設備	美國國防部

[15] "Defense Priorities & Allocations System (DPAS)," Defense Contract Management Agency, https://www.dcma.mil/DPAS/.

[16] 保留額內部可細分為 3%為「因公致殘退伍軍人持有之小型企業」（Service Disabled Veteran Owned Small Businesses, SDVOSB）、3%保留給位於「歷史上發展落後地區」（historically underutilized business zones，簡稱 HUBZones）之小型企業、5%「社經弱勢族群持有之小型企業」（Small Business Concerns Owned and Controlled by Socially and Economically Disadvantaged Individuals）、5%為「女性持有之小型企業」（The Woman-Owned Small Business, WOSB），見"Small Business Act," U.S. Small Business Administration, https://www.sba.gov/document/policy-guidance--small-business-act。

	Production equipment (for defense contractor's account)	
B9	政府國防生產設備 Production equipment (Government owned)	美國國防部
C1	戰備糧食 Food resources (combat rations)	美國國防部
C2	國防部建築 Department of Defense construction	美國國防部
C3	國防部設施保養、維修、運作之供應 Maintenance, repair, and operating supplies (MRO) for Department of Defense facilities	美國國防部
C9	雜項 Miscellaneous	美國國防部
針對加拿大的之軍事協助		
D1	加拿大軍事計畫 Canadian military programs	美國商務部
D2	加拿大生產與建造 Canadian production and construction	美國商務部
D3	加拿大原子能計畫 Canadian atomic energy program	美國商務部
針對其他外國之軍事協助		
G1	外國政府所採購經美國國內商業管道出口之特定彈藥項目 Certain munitions items purchased by foreign governments through domestic commercial channels for export	美國商務部
G2	來自加拿大以外的外國政府之特定直接國防需求 Certain direct defense needs of foreign governments other than Canada	美國商務部
G3	除加拿大以外的其他外國製造與建造 Foreign nations (other than Canada) production and construction	美國商務部
針對外國關鍵基礎設施之協助		
G4	外國關鍵基礎設施計畫 Foreign critical infrastructure programs	美國商務部
合作生產		
J1	F-16 合作生產計劃 F-16 Co-Production Program	美國商務部 美國國防部
原子能計畫		
E1	建築 Construction	美國能源部

E2	運轉-包括保養、維修、運作之供應 Operations-including maintenance, repair, and operating supplies (MRO)	美國能源部
E3	私人擁有設施 Privately owned facilities	美國能源部
國內能源計畫		
F1	探勘、製造、提煉與運輸 Exploration, production, refining, and transportation	美國能源部
F2	儲存 Conservation	美國能源部
F3	建築、維修與保養 Construction, repair, and maintenance	美國能源部
其他國防、能源及相關計畫		
H1	其他綜合 Certain combined orders (see section 700.17(c))	美國商務部
H5	國內私人製造 Private domestic production	美國商務部
H6	國內私人建築 Private domestic construction	美國商務部
H7	保養、維修、運作之供應 Maintenance, repair, and operating supplies (MRO)	美國商務部
H8	指定計畫 Designated Programs	美國商務部
K1	聯邦供應項目 Federal supply items	美國總務署
國土安全計畫		
N1	聯邦緊急事態準備、減緩、因應及重建 Federal emergency preparedness, mitigation, response, and recovery	美國國土安全部
N2	州、地方、部落政府緊急事態準備、減緩、因應及重建 State, local, tribal government emergency preparedness, mitigation, response, and recovery	美國國土安全部
N3	情報及預警系統 Intelligence and warning systems	美國國土安全部
N4	邊境與運輸安全 Border and transportation security	美國國土安全部
N5	國內反恐，包括強制執法 Domestic counter-terrorism, including law enforcement	美國國土安全部
N6	化學、生物、放射線及核能應變措施 Chemical, biological, radiological, and nuclear countermeasures	美國國土安全部

N7	關鍵基礎設施保護與重建 Critical infrastructure protection and restoration	美國國土安全部
N8	雜項 Miscellaneous	美國國土安全部

資料來源：蔡榮峰翻譯自“Code of Federal Regulations Part 700-Defense Priorities and Allocations System,” Electronic Code of Federal Regulations, https://reurl.cc/6gq3vZ。

肆、生產流程與供應鏈安全

在今日的工業生產體系下，軍事裝備或武器系統並不是由獲得合約的主承包商（prime contractor）獨力製造，而是由下游眾多協力廠商層層轉包，每一家廠商負責一部份零組件，最後再組裝成最終產品。美國武器製造大廠洛克希德馬丁（Lockheed Martin）宣稱與大約 1 萬 6,000 家供應商合作，而美國國防部總共大約有 30 萬家供應商。[17]這麼多的協力廠商加上層層轉包，很容易造成供應鏈的安全漏洞。從 2017 年起，美國有為數不少的國防承包商（contractor）與轉包商（subcontractor）被中國駭客入侵並竊走重要資料，例如中國駭客於 2018 年 1 月及 2 月入侵一家為海軍水下戰中心（Naval Undersea Warfare Center）進行研發的承包商，竊取了 614GB 的資料，包括由潛艦發射的超音速反艦飛彈、感測器及訊號資料、潛艦無線電室密碼系統、以及海軍潛艦發展單位的電子戰資料庫。[18]

這個事件對美國來說非常嚴重，在軍事力量上，中國與美國最大的差距在於水下作戰能力，如果這些先進科技為中國所用，將會削弱美軍在水下作戰的優勢，一旦未來與中國發生戰爭，整個局勢將可能改觀。因此，加強供應鏈安全（supply chain security）成為美國國防部自 2018 年以來的重點工作。[19]本節將介紹美國目前正在建立的兩項供應鏈安全規範，一是「無侵入交付」（Deliver Uncompromised, DU）；另一是「網路安全完善模式認證」（Cybersecurity Maturity Model Certification, CMMC），最後再介紹美國當前對於供應鏈及網路安全的新思維—「零信任架構」（Zero Trust Architecture, ZTA）。

[17] Nicole Ogrysko, “DoD unveils new cybersecurity certification model for contractors,” *Federal News Network*, September 5, 2019, https://federalnewsnetwork.com/defense-main/2019/09/dod-unveils-new-cybersecurity-certification-model-for-contractors.

[18] Ellen Nakashima and Paul Sonne, “China hacked a Navy contractor and secured a trove of highly sensitive data on submarine warfare,” *Washington Post*, June 8, 2018, https://www.washingtonpost.com/world/national-security/china-hacked-a-navy-contractor-and-secured-a-trove-of-highly-sensitive-data-on-submarine-warfare/2018/06/08/6cc396fa-68e6-11e8-bea7-c8eb28bc52b1_story.html.

[19] Gordon Lubold and Dustin Volz, “Chinese Hackers Breach U.S. Navy Contractors,” *Wall Street Journal*, December 14, 2018, https://www.wsj.com/articles/u-s-navy-is-struggling-to-fend-off-chinese-hackers-officials-say-11544783401.

一、無侵入交付

供應鏈通常會在兩個方面出現安全漏洞。首先，轉包商的規模有大有小。在供應鏈下游的轉包商通常都是小型企業，比較不注意網路安全，也比較沒有財力建立完善的資訊安全系統。因此，這些小型廠商很容易被駭客鎖定並入侵，成為軍事科技被竊取的管道。其次，在層層轉包的機制下，上游廠商往往不知道最後是轉包給哪一家下游廠商。若是最下游廠商發生資安事件，最上游的主承包商無法掌握。這兩項因素會造成關鍵技術在供應鏈的某個環節外洩，或是軍事裝備在生產、組裝流程中被植入後門，而主承包商在完成最終產品交貨時一無所知。

為了增進供應鏈安全，美國國防部現正大力推動「無侵入交付」。DU 的概念最早出現於美國米崔公司（MITRE Corporation）接受國防部委託在 2018 年 8 月提出的報告，該報告強調，民間廠商要承接國防部合約，除了成本、製造時程、產品性能外，安全是第四項考量因素，未能達到安全標準的廠商無法獲得合約。[20]DU 的精神在於供應鏈安全由上游廠商負責，上游廠商要知道每一項零組件是由哪一家下游廠商生產，第一層和第二層的承包商要監督其下的所有轉包商，並且負責管理整個供應鏈，確保每一層廠商往上一層交付的商品沒有受到侵入。[21]

在 DU 的概念下，每一家承包商必須做到兩件事。第一、其自身要符合美國國家標準暨技術研究院（National Institute of Standards and Technology, NIST）所頒布的工業標準規範，例如 NIST SP 800-171。第二、確認其下游所有轉包商也符合工業標準規範，若是一家承包商的下游轉包商不符合安全標準，該承包商就無法承接國防部合約。[22]DU 的具體辦法和時程至本年報出版前尚在制訂中，但美國國防部官員已經數次在公開場合倡導，未來必定會具體落實，我國廠商若是有意成為美國國防產業轉包商，必須特別注意 NIST 的工業標準規範。

二、網路安全完善模式認證

美國國防部於 2019 年 8 月公布「網路安全完善模式認證」（CMMC）草案、9 月 4 日公布修正版草案、11 月 8 日再公布第 0.6 版草案。CMMC 是對於國防承包商與轉包商在網路安全上新的標準及規範，以確保供應鏈安全。根據 CMMC 草案，美國國防部將廠商分為 5 級，第 1 級最低，第 5 級最高，要獲得國防部的合約成為承包商，該廠商的網路安全防護至少要達到第 3 級；要成為轉包商，網

[20] Christopher A. Nissen, John E. Gronager, Robert S. Metzger, and Harvey Rishikof, "Deliver Uncompromised: A Strategy for Supply Chain Security and Resilience in Response to the Changing Character of War," MITRE Corporation, August 2018, https://www.mitre.org/publications/technical-papers/deliver-uncompromised-a-strategy-for-supply-chain-security.

[21] Justin Doubleday, "New DOD contracts language will hold companies 'accountable' for cyber, supply chain security," *Inside Defense*, May 15, 2019, https://insidedefense.com/daily-news/new-dod-contracts-language-will-hold-companies-accountable-cyber-supply-chain-security.

[22] "Deliver Uncompromised: The Department of Defense's Latest Security Initiative," Aronson LLC, August 27, 2018, https://aronsonllc.com/deliver-uncompromised-the-department-of-defenses-latest-security.

路安全防護也至少要達到第 1 級。而要被評定為第 3 級，一家廠商必須符合 NIST SP 800-171 所規定的 110 項安全管制措施。[23]

具體而言，要成為 CMMC 第 3 級以上的廠商，必須達成的幾項重要安全措施包括：第一、建立與維持由專職人員運作的安全行動中心；第二、建立與維持 24 小時待命的網路安全應變小組；第三、使用自動化機制偵測電腦系統中是否有未獲授權軟體、硬體、或是檔案；第四、當資訊從一個系統轉移到另一個系統時，必須以安全的方式進行控制資訊流，例如資料加密。此外，美國國防部也要求所有承包商與轉包商建立資安事件通報機制，有任何網路入侵事件，都必須在發現後的 72 小時之內通報。[24]

CMMC 的第 0.6 版草案主要是對第 1 級到第 3 級的廠商提出規範，美國國防部要求第 3 級廠商要做到：員工只能接觸到或使用完成其工作所必須的資料與服務。另外，第 3 級廠商也要能夠控制與管理與外部網路相連的公司內部網路，並且控制與限制能夠連接公司網路並獲取資訊的個人通訊裝置，如筆記型電腦、平板電腦、以及手機。[25]

CMMC 按照規劃已經有比較明確的時程，美國國防部預計在 2019 年 11 月底提出第 0.7 版草案，將對第 4 級與第 5 級廠商制訂較明確的規定，然後在 12 月完成最後修訂；美國國防部同時計劃於 12 月建立評鑑機構，並於 2020 年 1 月開始試行 CMMC。[26]因此，想要進入美國國防產業供應鏈的廠商，必須深入瞭解美國的工業標準規範，並加強在網路安全防護機制的投資，才有可能通過認證。

三、零信任架構

在網路安全與供應鏈安全的思維上，美國現今正在進入「典範轉移」（paradigm shift）的時期。最早的安全思維是個別防禦（individual defense），也就是在個別終端設備安裝防毒軟體，掃描並移除電腦病毒。後來個別終端設備彼此相連，系統漸趨複雜，安全思維轉變為「邊緣防禦」（perimeter defense），也就是在系統的對外連接的出入端點設立防火牆，將電腦病毒與入侵者擋在系統外面，系統內部就是安全的。然而，今日的系統太過複雜，可以和外部相連的端點太多，如果還是以設立防火牆的方式來防禦，防火牆的數量將一直增加，造成成本過高且效率不彰。兼以5G通訊技術以及物聯網（Internet of Things, IoT）的發

[23] Nicole Ogrysko, "DoD unveils new cybersecurity certification model for contractors," *Federal News Network*, September 5, 2019, https://federalnewsnetwork.com/defense-main/2019/09/dod-unveils-new-cybersecurity-certification-model-for-contractors.

[24] Kristen Soles and Bhavesh Vadhani, "New DOD requirements – supply chain, risk management, and Cybersecurity Maturity Model Certification," CohnReznick LLP, August 15, 2019, https://www.cohnreznick.com/insights/achieve-compliance-with-new-dod-supply-chain-cybersecurity-rules-and-maturity-model.

[25] Rick Weber, "Pentagon issues draft cyber certification plan, delays input on controls for 'advanced' threats," *Inside Defense*, November 8, 2019, https://insidedefense.com/daily-news/pentagon-issues-draft-cyber-certification-plan-delays-input-controls-advanced-threats.

[26] Rick Weber, "CISA supply-chain task force briefed by DOD on aggressive schedule for contractor certification," *Inside Defense*, October 28, 2019, https://insidedefense.com/daily-news/cisa-supply-chain-task-force-briefed-dod-aggressive-schedule-contractor-certification.

展，未來一個系統可能有成千上萬的設備互相連接，「邊緣防禦」將無法滿足網路與供應鏈的安全需求，因此必須要有新的安全思維。

2019年7月，美國國防部的諮詢機構「國防創新理事會」（Defense Innovation Board）提出一份白皮書，建議美國國防部以「零信任架構」（ZTA）取代「邊緣防禦」，成為物聯網時代的安全思維。簡單地說，ZTA把系統本身當作是不安全的，對進入系統的每位使用者都不信任，因此，每位使用者都只給予「最低限度存取權限」（least-privilege access），也就是只給予每位使用者及其終端裝置要完成其工作所必須的資料及系統服務，其他不相關的資料及系統服務，該位使用者及其終端裝置沒有權限接觸。[27]此概念就如同一棟公寓有多位住戶，一位特定住戶只會拿到公寓大門鑰匙和自己房間的鑰匙，不會拿到其他住戶房間的鑰匙；因此該名住戶進入公寓後只能進入自己的房間，無法進入其他住戶的房間，如此可以保護整棟公寓的安全。[28]

ZTA是以使用者的「角色」做為核心概念，依據每位使用者的不同角色而給予不同權限。[29]ZTA有三個基本步驟：第一、辨識使用者；第二、辨識其所使用的裝置；第三、根據使用者的任務給予權限。ZTA的重點在於，當同一位使用者的角色發生變化，他在系統內的權限也會隨之擴張或限縮，因此，實施ZTA的先決條件是建立身份及權限的管理機制。ZTA的概念在提出之後，已經受到美國國防部的重視，2019年10月12日，美國國防部下轄的國防資訊系統局（Defense Information Systems Agency, DISA）發布徵求建立身份辨識機制的白皮書；[30]前述在11月8日公布的CMMC第0.6版草案中，對第3級廠商的要求即是ZTA的概念。可以預期，ZTA在未來將會在美國的供應鏈安全規範中逐步落實。

伍、終端市場及安全認證

國防產業的銷售市場端通常以國家為單位，因此從製造到銷售，皆涉及國家利益之維護。發展國防產業所投入的公共預算、產出的經濟溢出效益，又與民生經濟和研發資金息息相關，因此形成了私人資本與公共利益之匯流的循環經濟。然而也正是因為國防產業在資訊、資金、人員的流動上，具有公私混合之特性，且商品規格也異於民用標準，因此在整個國防產業經濟循環末端的「交易對象」以及「交易品項」就成了一國國防工業能力能否持續獲得動能的重要關鍵，特別是有關敏感科技轉移的終端使用者控管與安全認證管理。

---

[27] Justin Doubleday, “DOD seeks white papers on identity technologies foundational to ‘zero-trust’ initiative,” *Inside Defense*, October 16, 2019, https://insidedefense.com/daily-news/dod-seeks-white-papers-identity-technologies-foundational-zero-trust-initiative.

[28] Kurt DelBene, Milo Medin, and Richard Murray, The Road to Zero Trust (Security), *Defense Innovation Board*, July 9, 2019, https://media.defense.gov/2019/Jul/09/2002155219/-1/-1/0/DIB_THE_ROAD_TO_ZERO_TRUST_(SECURITY)_07.08.2019.PDF.

[29] Justin Doubleday, “DOD research and engineering lead pushing ‘zero trust’ approach to cyber, 5G developments,” *Inside Defense*, September 23, 2019, https://insidedefense.com/daily-news/dod-research-and-engineering-lead-pushing-zero-trust-approach-cyber-5g-developments.

[30] Justin Doubleday, “DOD seeks white papers on identity technologies foundational to 'zero-trust' initiative,” *Inside Defense*, October 16, 2019, https://insidedefense.com/daily-news/dod-seeks-white-papers-identity-technologies-foundational-zero-trust-initiative.

一、終端市場風險管理

一國政府通常以頒發「出口許可」（export license）作為管控終端市場風險的方式，管制途徑主要分成「軍民兩用產品」以及「軍用產品」兩大類。凡是被列在管制清單上的類別，都需要依照一些判斷標準加以評估，例如技術特徵（technical characteristics）、目的地（destination）、終端使用者（end user）及最終用途（end use）等。

管制清單依循的國際規範來自包括澳洲集團（Australia Group）、《禁止化學武器公約》（*Chemical Weapons Convention*）、核子供應國集團（Nuclear Suppliers Group）、《飛彈技術管制協議》（*Missile Technology Control Regime*）、《瓦聖納協定》（*Wassenaar Arrangement*）等國際出口管制組織。

在獲得「出口許可」前，出口國政府通常還會要求出口商向國家有關單位出示具有公信力的「終端用戶證明書」（End User Certificate, EUC），證明買方有資格承擔隨交易行為而來之義務。「終端用戶證明書」往往是由進口國政府的經貿或國防單位作為第三方擔保核發，用以證明在國際轉讓行為完成後，國籍買家將是貨品的最終使用者，藉此限制貨品流動性、避免重要軍品或高科技零組件落入敵對國家、禁運國家、迫害反人權之政府或恐怖份子之手，有時也出於保護本國智慧財產與商業利益。

一份較詳盡的「終端用戶證明書」內容除了買賣雙方資訊以外，通常還包括：交易目的與用途、交易內容、交易背景、對現行法規之影響、內文名詞定義、相關政策、交易責任、交易程序等。然而，此類機制需仰賴進出口國政府落實管制機制，甚至是國際監督制衡，才能真正管控風險，否則即使終端使用者為一國之政府，有時也難以保證該義務能確實履行。

我國1994年於《貿易法》中納入相關條文，另訂定《戰略性高科技貨品輸出入管理辦法》以及《戰略性高科技貨品種類、特定戰略性高科技貨品種類及管制地區》等管制措施，由經濟部國際貿易局執行「軍民兩用產品」輸出入管理，參照「歐盟管制清單」（*EU Consolidated List*）作為管制名單主要參考，列管10大類產品，包括核能物質與設施、特殊材料與相關設備、材料加工程序、電子、電腦、電信及資訊安全、感應器與雷射、導航與航空電子、海事、航太與推進系統，廠商皆須申請輸出許可才能出口。[31]2016年我國進一步建立經濟部戰略性高科技貨品管理策略推動小組，納入國防部、外交部等共15個部會局處，組成跨部會的機制推動平台。

在美國，「軍民兩用產品」則由美國商務部工業暨安全局（Bureau of Industry and Security, BIS）依照《出口管理規則》（*Export Administration Regulations*, EAR）管制，[32]該規則下的「商品管制清單」（*Commerce Control List*）當中每種品項均

[31] 《高科技貨品管理》，經濟部國際貿易局，2019 年 10 月 25 日，https://www.trade.gov.tw/Pages/Detail.aspx?nodeID=242&pid=662639。

[32] 主要法源為《出口管制法》(*Export Administration Act*, EAA)。

有一組「出口管制分類編碼」（The Export Control Classification Number, ECCN），由5碼代號所組成，分別代表「商品管制清單種類」、「商品種類」、「管制類型」、「瓦聖納協定軍品管制清單」4種內涵，例如「9A610」代表「軍用航空器及相關商品」，而「9D610」則代表「軍用航空軟體」。部分不在「商品管制清單」上的低技術含量之商品項目，則會被列為「EAR99」，也就是除非輸出對象是被列為禁運名單的終端使用者，否則無須出口許可。

表 4-3、美國出口管制分類編碼表

I、商品管制清單種類 Commerce Control List Categories	
0	核子原料、設施、設備（及相關雜項）
1	材料、化學、微生物與有毒物質
2	材料處理
3	電子用品
4	電腦
5	遠端通訊及資訊安全
6	感應器與雷射
7	導航與航空電子技術
8	海事
9	推進系統、太空載具及有關設備
II、商品種類 Product Groups	
A	系統、設備、零組件
B	測試、檢查、製造設備
C	材料
D	軟體
E	技術
III、管制類型 Type of Control	
0	《瓦聖納協定》之國安管制* 核子供應集團之軍民兩用管制及觸發清單（trigger list）
1	飛彈技術管制
2	核不擴散管制
3	生化武器管制
6	美國國家軍品轉移至商品管制清單之管制
9	非國家及單邊管制（反恐、犯罪管制、區域穩定、短期供應、聯合國制裁等）
IV、《瓦聖納協定》軍品管制清單 Wassenaar Arrangement Munitions List (WAML)	

資料來源：蔡榮峰整理自公開資訊。

*說明：該清單包括核子轉移規範，例如實體保護、保護措施、對敏感技術出口的特別管制、核子材料濃縮設施出口特別安排、對可用於核武器的材料進行管制、對二次轉移之管制以及支援，見“Guidelines for nuclear Transfers,” Nuclear Suppliers Group, https://www.nuclearsuppliersgroup.org/en/guidelines。

「軍用產品」則由美國國務院國防貿易管制處（Directorate of Defense Trade Controls, DDTC）依照《武器貿易管制條例》（*International Traffic in Arms Regulations*, ITAR）、《武器出口管制法》（*Arms Export Control Act*, AECA）及《外國援助法》（*Foreign Assistance Act*, FAA）管理。

美國國防部下轄的國防技術安全局（Defense Technology Security Administration, DTSA）專責檢視國安與科技管制技術規範，協助前述的BIS與DDTC判定出口許可之發放；若遇有部門意見相左時，DTSA也會代表美國國防部進行跨部門協商。當相關法規需要修改時，也是由DTSA協調美國國防部有關單位進行評估。[33]值得注意的是，美國國會於2018年8月13日通過之《出口管制改革法》（*Export Control Reform Act of 2018*, ECRA）第1758條，將由BIS後續公布14項新興科技管制細節後進行審查，以防止關鍵技術流失。此一改變可說對台灣乃至世界科技產業鏈影響深遠，未來發展值得觀察。[34]

除了來自境外的採購，一國國防本身的軍需市場的獨占性特質，對其經濟與科技同樣具有重要影響力。因此如何善用政府採購來扶植國防產業，相當受到各國重視。例如我國於2019年5月31日三讀通過的《國防產業發展條例》，其第11-18條特別列出了獎勵捐助補助、資金技術投資或授權、優先採購、提供融資及優惠利率等獎勵方式，以及外購前應先以「技術轉移」、「研發產製」、「後勤支援」評估國內能量。而考慮到軍用科技的特殊性，戰機、戰車、船艦等一等列管軍品的採購，未來也不再受《政府採購法》及其施行細則內「有關規劃、設計服務的廠商不得參與後續投標、作為決標對象或分包廠商或協助投標廠商」等相關規定的限制，以有利我國重要軍備之全壽期規劃。更重要的是，《國防產業發展條例》第19條將技術輸出入的潛在風險納入考量，管制重要零組件與原物料來源非經許可不得來自中國大陸、香港或澳門背景之法人機構。以法規限制來降低供應鏈風險，除了能夠減少製造或技術依賴性，也能夠透過替代效果扶植我國國內的國防產業。

事實上類似的風險管制，也可見於2018年9月美國國防產業評估報告—《評估與強化美國製造與國防產業基礎與供應鏈韌性》（*Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States*）。該報告提出超過280項可能影響美軍軍品與零組件供應的漏洞，並一再點出「中國製造」因素對於美國國防產業基礎（defense industrial base）的

[33] DDTC 負責管制 ITAR，BIS 則負責管制 EAR，見"The U.S. Export Control System and the Export Control Reform Initiative," Congressional Research Service, April 5, 2019, p6, https://fas.org/sgp/crs/natsec/R41916.pdf。

[34] (1)生物奈米與合成技術；(2)人工智慧與機器學習技術；(3) 定位、導航和定時技術；(4)微處理器技術；(5)先進計算技術；(6)大數據分析技術；(7)量子資訊和感應傳輸技術；(8)物流技術；(9)積層製造技術；(10)機器人；(11)腦機介面；(12)極音速；(13)先進材料；(14)先進監控技術，見"Review of Controls for Certain Emerging Technologies," *Federal Register*, November 19, 2018, https://www.federalregister.gov/documents/2018/11/19/2018-25221/review-of-controls-for-certain-emerging-technologies。

侵蝕性影響。[35]美國《聯邦採購條例》（*Federal Acquisition Regulation,* FAR）規定任何國防與能源的採購案，都必須按照「國防等級與配置系統」分級制度進行。[36]而美國政府也能透過修改該法之下的《國防部補充條例》（*Department of Defense FAR Supplement,* DFARS），來防堵其境內國防產業鏈遭受外國勢力滲透。[37]此外，在美國法律中，被定義為美國國防產業廣義來源地的「國家科技和產業基礎」（National Technology and Industrial Base, NTIB）除美國本身以外，還包括後來納入的3個盟國：加拿大（1994納入）、澳洲（2016納入）和英國（2016納入）。NTIB的擴張、新的威脅和技術環境、私部門逐漸在技術創新上超越公部門，這些新的變化預料將對美國未來國防產業的發展計畫和風險管理帶來新的挑戰。[38]

二、軍規產品安全認證

重要軍用設備的設計與製造往往能夠反映一國的戰略意圖，或是反映其先進工業能力，因此由製造商或第三方來驗證產品安全性，多半視機敏性而定；等級越高的重要軍品例如軍用飛行器製造，就越仰賴掌握獨家技術的製造商提供原廠認證。軍規產品適用之環境條件較民用產品嚴苛，因此其安全認證的標準自然也有所不同，因此除了「製成品」之外，「製程標準」的安全認證更是維繫整個產業鏈上下游的關鍵，而這也是公部門或第三方安全認證能夠在整個國防產業發展過程當中扮演的角色。

拿國防產業技術門檻較高的航太領域來說，波音（Boeing）、空中巴士（Air Bus）、奇異（General Electric）、賽考斯基航空（Sikorsky Aircraft）及龐巴迪（Bombardier）等主要航太製造龍頭，都有針對其下游代工廠商所授予的原廠認證，用以認證一架飛機各階段所需要的上百萬件零組件。當然，一些國家的國防

---

[35] "Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States," U.S. Department of Defense, September 2018, https://media.defense.gov/2018/Oct/05/2002048904/-1/-1/1/ASSESSING-AND-STRENGTHENING-THE-MANUFACTURING-AND%20DEFENSE-INDUSTRIAL-BASE-AND-SUPPLY-CHAIN-RESILIENCY.PDF.

[36] "Federal Acquisition Regulation 52.211-14&15," Aquisition.gov, https://www.acquisition.gov/content/part-52-solicitation-provisions-and-contract-clauses#i1063085.

[37] 1984 年生效、1995 年修正的美國《聯邦採購條例》，其內容闡述該條例希望透過政府採購案達到四個主要目標：（1）在適當的性價比、交件期限下，滿足公部門對特定商品與服務的需求；（2）降低部門行政成本；（3）維護美國國內商務環境的公平、開放、完整性；（4）達成政府公共政策目標。然而，依照美國國防部的採購經驗來看，多半時候「維持對中小企業的採購比例」與「最理想的性價比」往往是兩個互不相容的選項，顯示即便是身為國防產業先發國家，美國為了扶植國內產業，也必須仰賴政策的介入。不過，涉及新創企業的創新科技產品採購案時，較不會發生前述情況，見 Moshe Schwartz, "Social and Economic Public Policy Goals and Their Impacts on Defense Acquisition-A 2019 Update," *Defense Acquisition Research Journal*, July 2019, Vol. 26, No.3, pp.208-228, https://www.dau.edu/training/career-development/logistics/blog/New-Issue-of-Defense-Acquisition-Research-Journal.

[38] William Greenwalt, Leveraging the National Technology Industrial Base to Address Great Power Competition: The Imperative to Integrate Industrial Capabilities of Close Allies, *Atlantic Council*, April 2019, https://www.atlanticcouncil.org/wp-content/uploads/2019/04/Leveraging_the_National_Technology_Industrial_Base_to_Address_Great-Power_Competition.pdf.

部也會以作戰需求與後勤狀況來訂定特有的軍用標準以作驗收之用，例如美國、歐盟、澳洲就有自己的適航認證（airworthiness）標準。

用於後勤維修的零組件，有時會碰到消失性商源的情況，因此需要使用非原廠或非原廠授權代工廠之零組件，這也是「製程標準」發揮功能的主要階段，此時由國家機構所頒定的製程標準認證，可用來檢驗備用商源是否達到堪用標準門檻，例如美國聯邦航空總署（Federal Aviation Administration, FAA）所頒發的技術標準規定認證（*Technical Standard Orders*, TSOs），不過這類認證屬於「製造許可」類的認證，能否使用於特定的飛行器，則需要視廠商合約、相關適航認證許可而定。[39]例如在扣件供應，主要是由美國國防後勤局（Defense Logistics Agency, DLA）核發合格供應商認證，其「合格製造商名單」（*Qualified Suppliers List for Manufacturers*, QSLMs）以及「合格經銷商名單」（*Qualified Suppliers List for Distributors*, QSLDs）兩個主要名單上，就標示了屬於第3級的航太扣件，以及屬於第2級的陸海軍用扣件。[40]

此外，與製造業品質管理息息相關的國際組織「國際標準化組織」（International Organization for Standardization, ISO）也扮演了重要角色，例如航太領域就有ISO9001、AS9100、AS9120。而從產業聯盟演進而來的認證體系，認證範圍更廣，例如致力於規格標準化的美國「汽車工程師學會」（Society of Automobile Engineers, SAE）於1990年創立的「國際航太與國防工業承包商認證體系」（National Aerospace and Defense Contractors Accreditation Program，NADCAP）就涉及品管、製程、產品、相關實驗。近年戮力發展航太產業的台灣，也於2019年8月15日，由國家中山科學研究院、經濟部航空產業發展推動小組、台灣經濟研究院邀集11個單位成立「國機國造檢量測聯盟」，希望能夠藉此協助國內廠商降低嵌入國際供應鏈的門檻，並強化我國國防領域之安全。[41]

不僅軍規產品需要安全認證，就科技創新的先進國家來說，只要有關國防的敏感科技，其轉移過程也需要安全查核。例如美國為了維持20世紀以來的技術優勢，特別針對軍民兩用科技的技術移轉設置了「安全閥」，即1993年頒布實行的《國家工業安全計畫》（*National Industrial Security Program*, NISP）。該計畫主要針對有關國安與國防的敏感科技之技術轉移進行保密管理，由美國國防部長負責、另由資訊安全監督辦公室（The Information Security Oversight Office, ISOO）代表美國國家安全會議監管。[42]根據該計畫所制定的美國《國家工業安全計畫守則》（*National Industrial Security Program Operating Manual*, NISPOM），成為美國政

---

[39] "Technical Standard Orders," *Federal Aviation Administration*, October 11, 2018, https://www.faa.gov/aircraft/air_cert/design_approvals/tso/.

[40] "Engineering and Technical Services - Qualified Suppliers List," *Defense Logistics Agency*, https://www.dla.mil/TroopSupport/IndustrialHardware/Engineering-and-Technical-services/Qualified-Suppliers-List/.

[41] 11 個共同成立的單位包括國家中山科學研究院、台灣區航太工業同業公會、台灣機械工業同業公會、台灣區電機電子工業同業公會、台灣經濟研究院、國家實驗研究院、金屬工業研究發展中心、工業技術研究院、台灣電子檢驗中心、資訊工業策進會、車輛研究測試中心。

[42] ISOO 為美國檔案紀錄管理局（National Archives and Records Administration, NARA）下轄單位。

府跨部會有關單位辦理業務之依循。在執行層面，由美國反情報與安全局（Defense Counterintelligence and Security Agency, DCSA）協調與聯邦政府33個單位的行政作業，並負責美國國防產業鏈上下游國防廠商之招標管理、頒發執照與安全查核。[43]

陸、小結

工業全球化使得產業鏈跨國分工常態化，而這個趨勢同樣也影響到國防產業，甚至先進國家的民用技術創新科技，部分發展速度已超越以往領銜發展的國防機構。該如何透過政府機制來管控技術溢散風險，並於軍民領域間轉換創新動能，逐漸成為各國發展國防工業的重要課題。

從本章的說明可以發現，基於近幾年來外資併購、網路竊取事件頻頻發生，造成美國關鍵科技外流嚴重，因此美國在產業安全的各個面向都在進行改革，制訂新的機制與規範。首先對於外來投資作更嚴謹的審查，不以獲得控制權為前提，而是以投資領域為管制目標，避免外國政府或企業藉由併購獲取關鍵技術。其次是依據廠商的技術能力與專業領域將其分類分級管理，並加強公司內控機制，避免機敏資料由內部流出。更重要的是，因為國防產品之需求與一般商業用途有所不同，所以必須建立國家認證標準來保證國防工業產品的品質，並藉此消弭消失性商源可能帶來的負面影響。最後，國家權責機構依專業機制，建立管理出口許可協同機制來管控終端使用者、保障一國之智慧財產權。

現今的安全思維也面臨典範轉移，從「邊緣防禦」轉變為「零信任架構」。美國新的規範例如「無侵入交付」與「網路安全完善模式認證」的具體措施都正在研擬當中，「網路安全完善模式認證」也已經融入了「零信任架構」的安全思維。我國相關單位應密切注意，這些規範必定有我國可以效法之處，也可以提醒國內廠商注意，以助其打入美國國防供應鏈。

（責任校對：吳宗翰、盧屏淵）

[43] "New to DCSA?" Defense Counterintelligence and Security Agency, https://www.dcsa.mil/; National Industrial Security Program Operating Manual (NISOPM 2006), U.S. government, May 18, 2016, https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/522022M.pdf.