出國報告（出國類別：研究）

營業秘密保護之研究-以國家核心關鍵技術保護為中心

服務機關：臺灣臺北地方檢察署

姓名職稱：楊石宇檢察官

派赴國家：美國哈佛大學

出國期間：民國 112 年 9 月 1 日至 113 年 5 月 30 日

報告日期：民國 113 年 6 月 12 日

摘要

首先，我國於 2022 年修正國家安全法，其中提出嶄新的概念「國家核心關鍵技術之營業秘密」，將營業秘密保護提升至國家安全之層級，建立營業秘密層級化的保護體系，目的為保護我國之產業競爭力及國家安全，本研究欲對於此修法之來龍去脈及其內涵一探究竟。

再者，從「防範國家關鍵技術外流」之上位概念觀察，營業秘密保護法制實為「防範國家關鍵技術外流」整體法制之一環。除此之外，外資投資審查法制、出口管制法制，都是世界各國近年來針對「防範國家關鍵技術外流」修法之重點，本研究分別就美國、韓國及我國現有之相關法制予以探討。

最後，本研究針對本次我國修正國安法之立法背景、立法模式選擇、重點內容予以介紹，並嘗試分析其利弊並提出建議，做為未來努力方向。

目次

壹、前言

一、研究動機、目的及過程

(一)、研究動機

我國立法院於 2022 年 5 月 20 日三讀通過國家安全法(簡稱國安法)修正草案，並於同年 6 月 8 日經總統修正公布[1]，新增第 8 條第 1 項之「為外國等侵害國家核心關鍵技術營業秘密罪」(即經濟間諜罪)及同條第 2 項之「國家核心關鍵技術營業秘密域外使用罪」，明定任何人不得為外國、大陸地區、香港、澳門、境外敵對勢力或其所設立或實質控制的各類組織、機構、團體或其派遣之人，為侵害國家核心關鍵技術之營業秘密的行為，以及任何人不得意圖在外國、大陸地區、香港或澳門使用國家核心關鍵技術之營業秘密，而為侵害國家核心關鍵技術之營業秘密的行為，罰則則分別為 5 年以上 12 年以下有期徒刑，得併科新臺幣 500 萬元以上 1 億元以下之罰金及 3 年以上 10 年以下有期徒刑，得併科新臺幣 500 元以上 5 千萬元以下之罰金，科罰金時，如犯罪行為人所得之利益超過罰金最多額，得於所得利益之 2 倍至 10 倍範圍內酌量加重，且均有處罰未遂犯之規定，將符合一定

[1]2022 年 6 月 8 日修正之全文 20條，除第 3 條第 3 項至第 5 項定自 2023 年 4 月 28 日施行外，其餘條文施行日期，另由行政院定之。

條件之營業秘密的保護，提升至國家安全的層級，以因應原本營業秘密法對於侵害國家法益部分之營業秘密犯罪類型部分保護密度不足之處，並建立營業秘密層級化的保護體系[2]，首次將營業秘密之保護提升至國家安全層級，可藉此觀察出我國立法者對於完善我國營業秘密保護法制及之決心，及涉及國家安全、產業競爭力之國家核心關鍵技術營業秘密之重要性。

除了前述之國安法修正外，值得注意的還有 2022 年 5 月 20 日立法院三讀通過，同年 6 月 8 號經總統修正公布，並分別於同年 11 月 18 日、2023 年 4 月 28 日施行[3]之臺灣地區與大陸地區人民關係條例以及 2023 年 1 月 12 號立法院三讀通過，並於同年年 8 月 30 號施行之智慧財產案件審理法當中，關於完善營業秘密保護之相關規定。

臺灣地區與大陸地區人民關係條例部分，是針對受政府機關或政府機構委託、補助或出資達一定基準，從事涉及國家核心關鍵技術業務之人員，建立赴陸審查機制[4]；及針對陸資假藉人頭違法來臺投資，

[2]即「一般侵害營業秘密罪」（營業秘密法第 13 條之 1 第 1 項規定）、「一般營業秘密之域外使用罪」（營業秘密法第 13 條之 2 第 1 項規定）、「國家核心關鍵技術營業秘密之域外使用罪」（國家安全法第 8 條第 2 項規定）、「為外國等侵害國家核心關鍵技術營業秘密罪」（國家安全法第 8 條第 1 項規定）等四個保護層級；立法院網站，https://lis.ly.gov.tw/lglawc/lawsingle?000E6D6F752000000000000000000140000000040000000^0144111105 2000^00000000000（最後瀏覽日：8/27/2023）。

[3]臺灣地區與大陸地區人民關係條例第 40 之 1 條、93 之 1 條、93 之 2 條於 2022 年 11 月 18 日施行；第 9、91 條則於 2023 年 4 月 28 日施行。

[4]臺灣地區與大陸地區人民關係條例第 9 條、第 91 條規定，受政府機關(構)委託、補助或出資達一定基準，從事涉及國家核心關鍵技術業務之個人或法人、團體、其他機構成員，及受委託、補助、出資終止或離職未滿 3 年者，赴陸應經審查會審查許可，違者可處新臺幣 200 萬元以上 1,000 萬元以下罰鍰。

或陸企違法在臺從事業務活動，明確規範人頭為處罰對象，並提高相應之刑責[5]，以健全國家核心關鍵技術之保護，維護國家經濟競爭優勢。

智慧財產案件審理法部分，則是迎來自 2008 年 7 月 1 日施行 15 年以來，最大幅度的修法[6]，新法的 9 大重點如下：完備營業秘密訴訟保護、擴大採行強制律師代理、擴大專家參與審判、智慧財產案件集中審理、訴訟紛爭解決一次性（避免裁判歧異）、促進審理效能、增進科技設備審理（司法Ｅ化升級）、增訂被害人訴訟參與制度及解決實務爭議[7]。其中關於完備營業密密訴訟保護制度部份，新法首先是規定將營業秘密第一審刑事案件從地方法院刑事法庭改由智慧財產及商業法院第一審智慧財產法庭審理，侵害國家核心關鍵技術之營業秘密第一審刑事案件，則由智慧財產及商業法院第二審智慧財產法庭審理[8]，第三審法院則須依法設立專庭或專股辦理智慧財產民事及刑事

[5]臺灣地區與大陸地區人民關係條例第 40 條之 1、第 93 條之 1 及第 93 條之 2，規定中國大陸營利事業於第三地區投資之營利事業，非經主管機關許可，並在臺設立分公司或辦事處，不得在臺從事業務活動，違者可處 3 年以下有期徒刑。而為規避陸資在臺投資應經主管機關許可之規定，將其名義提供或容許他人使用者，得由主管機關處新臺幣 12 萬元以上 2,500 萬元以下罰鍰。

[6]修正前智慧財產案件審理法僅有 41 條，修正後新法增加至 77 條，共計增訂 36 條、修正 41 條，規範密度大幅增加。

[7]司法院網站，https://www.judicial.gov.tw/tw/cp-1887-931280-7e912-1.html（最後瀏覽日：8/31/2023）。

[8]智慧財產案件審理法第 54 條立法理由說明，營業秘密刑事案件具有高度技術與專業特性，侵害營業秘密犯罪，涉及對產業具有獨特競爭優勢之技術、商業性營業秘密侵害，或犯罪所生損害等議題之判斷，為保障產業合法營業權益，鼓勵並保障持續創新研究發展，維護產業倫理與競爭秩序，並避免被害人之營業秘密侵害持續擴大，即有將犯營業秘密法第十三條之一、第十三條之二、第十三條之三第三項及第十三條之四之罪之第一審刑事案件，改由第一審智慧財產法庭審理之必要，以落實營業秘密第一審刑事案件之專業、妥適及迅速審理目標；再者，依國家安全法第十八條第二項規定，違反第八條第一項至第三項之案件，其第一審管轄權屬於智慧財產法院，爰增訂第二項第二款，明定侵害國家核心關鍵技術之營業秘密案件，由第二審智慧財產法庭為第一審之審理。

案件[9]。其餘則有保護營業秘密卷證內容、強化秘密保持命令運用制度、營業秘密卷證去識別化之代稱或代號及提高違反秘密保持命令罪刑責及引進境外違反秘密保持命令罪等措施[10]。智慧財產案件審理法第1條則明文規定:「為建構專業、妥適及迅速審理智慧財產案件之訴訟制度，保障智慧財產及其相關權益，特制定本法。」[11]

我國對於營業秘密之保護，早期對於侵害營業秘密之行為，係分別以民法第184條以下之侵權行為責任及刑法第317條、第318條之洩漏工商秘密罪來處理，於1992年公平交易法施行後，則有公平交易法第19條第5款[12]予以規範，並有相關民、刑事責任。嗣於1996年營業秘密法專法制定，惟制定之初僅有民事責任，在2013年因回應各界對於營業秘密保護之需求及順應國際立法趨勢，方於2013年

[9]智慧財產案件審理法第48條之立法理由認為，為貫徹智慧財產民事事件審理之專業性，俾達統一法律見解之功能，由具有相關專業知識或審判經驗之法官，透過反覆審理累積經驗，將有助於提升裁判品質、效率及可預測性。基此，第三審法院應設立專庭或專股，以求專業辦理智慧財產民事事件；智慧財產案件審理法第62條之立法理由則明示，智慧財產案件具有高度技術與專業特性，各國為強化其全球經濟力，無不致力於推動相關法令與政策，保護智慧財產權益之創新與發展。其中，犯營業秘密法第13條之1、第13條之2、第13條之3第3項及第13條之4之侵害營業秘密罪案件，或犯國家安全法第8條第1項至第3項之侵害國家核心關鍵技術之營業秘密罪案件，更具審理複雜性與高度經濟價值，為貫徹智慧財產案件審理之專業性，確保產業之國際競爭優勢，及維護國家安全與經濟發展，俾達統一法律見解之功能，由具有相關專業知識或審判經驗之法官透過反覆審理累積經驗，將有助於提升裁判品質、效率及裁判之可預測性。

[10]司法院網站，https://www.judicial.gov.tw/tw/cp-1887-931280-7e912-1.html(最後瀏覽日：9/3/2023)。

[11]智慧財產案件審理法第1條之立法理由提及，在全球化經貿競爭的時代，因科技不斷推陳創新，所衍生之智慧財產保護，成為各國推動經濟發展與貿易自由化之重要課題，更視為國家整體競爭力之指標。為強化競爭優勢，各國無不致力於研修相關法令與政策，以保護智慧財產權益，並發展知識經濟。為建構符合國際趨勢之專業、妥適訴訟制度，迅速解決智慧財產權益紛爭，創造更完善之智慧財產及其相關權益之保護環境，爰增訂本條，揭示本法之立法目的。

[12]修正前公平交易法第19條第5款規定，凡「以脅迫、利誘或其他不正當方法,獲取 他事業之產銷機密、交易相對人資料或其他有關技術秘密之行為」,而有限制競爭或妨礙公平競爭之虞者,事業不得為之。惟該款於2015年修法時遭刪除。

增訂刑事責任[13]，相較於世界各國對於營業秘密保護保護法制之發展進程，起步較晚[14]，在中美貿易戰[15]、科技戰[16]的全球氛圍當下，世界各國無不加緊腳步修正營業秘密保護法制及[17]及保護國家關鍵技術相關之外資投資審查、技術出口管制以求更加妥善保護各營業秘密及國家關鍵技術，我國自然應加緊腳步，針對此領域投入更多研究能量。

根據我國法務部針對侵害智慧財產權案件統計分析統計數據顯示[18]，全國各地方檢察署偵辦營業秘密案件偵查終結人數從開始統計的 2014 年 47 人，到 2020 年 352 人，在短短的幾年內，成長將近 8 倍；而在總共 1,747 件營業秘密案件當中，起訴的比例僅占百分之 25.8，緩起訴占百分之 1.7，不起訴比例則占百分之 64.1，其餘少部

[13] 立法院網站， https://www.ly.gov.tw/Pages/Detail.aspx?nodeid=6590&pid=205760(最後瀏覽日：09/04/2023)。

[14]德國於 1896 年即有不正競爭制止法保護營業秘密，英國、美國則分別於 1822 年、1837 年即有以習慣法(common law)案例保護營業秘密之紀錄，美國並於 1979 年由統一州法全國委員會(National Conference of Commissioners on Uniform State Law)發布統一營業秘密法典(Uniform Trade Secret Act, UTSA)，由各州議會依據該法典調整修正成為各州州法，並以民事救濟為主。見章中信（2013），〈營業秘密之保護與公平交易法之關聯〉，《第 19 屆競爭政策與公平交易法學術研討會論文集》，頁 239 -240。

[15] 維基百科網站，https://zh.wikipedia.org/zh-hant/%E4%B8%AD%E7%BE%8E%E8%B4%B8%E6%98%93%E6%88%98（最後瀏覽日：9/4/2023）。

[16]報導者網站，https://www.twreporter.org/a/interview-cyrus-chu-ultimate-economic-conflict（最後瀏覽日：9/4/2023）。

[17]美國於 2022 年底修正通過 2022 年保護美國智慧財產權法案(Protecting American Intellectual Property Act of 2022)，於 2023 年 1 月 5 日由總統簽署生效，提升對美國營業秘密的保護。見 PWC 網站，https://www.pwc.tw/zh/services/legal/point-view/legal-clouds/legal-clouds-2304.html（最後瀏覽日：9/6/2023）；德國則是原先並獨立的無營業秘密法，於 2018 年 6 月通過營業秘密保護法，2019 年 4 月 26 施行新法；見財團法人資訊工業策進會網站，https://stli.iii.org.tw/article-detail.aspx?no=64&tp=1&d=8362（最後瀏覽日：09/06/2023）；韓國則於 2018 年修正不正競爭防止及營業秘密保護法，放寬營業秘密的成立要件、擴大究責範圍、並加重民事與刑事罰則。見冠群商國際專利商標聯合事務所網站，https://etopteam.com/2019/06/14/korean-trade-secret-amendment/（最後瀏覽日：9/6/2023）。

[18]法務部網站，https://www.rjsd.moj.gov.tw/RJSDWeb/common/WebListFile.ashx?list_id=1737（最後瀏覽日：8/27/2023）。

分則是緩起訴、移送調解、通緝、移轉管轄、移送法院併案審理等，與一般刑案之起訴、聲請簡易判決處刑、緩起訴比例相加有百分之 35 左右[19]相較，明顯偏低；且 2011 年到民國 2020 年間，偵辦侵害智慧財產權案件平均每件結案日數 65.9 日，較全部刑事案之平均日數多 14 日，而其中以違反營業秘密法 154.2 日最長；定罪率部分，依據法務部的統計，我國地方檢察署起訴案件之定罪率，自 2019 年至 2023 年 7 月間，均為百分之 96 左右[20]，惟根據司法院的統計，全國各地方法院近 2018 至 2020 年審理違反營業秘密法刑事案件共有 85 人，審判後有罪 63 人，有罪率僅為百分之 74 上下[21]，顯然也有所落差。從上述的統計數據觀察可以了解到，營業秘密相關的刑事案件近年來呈現穩定增加，並無停止的跡象；而營業秘密相關案件起訴、聲請簡易判決、緩起訴的比例偏低，原因則可能是因為營業秘密之構成要件不符、或是檢、警、調在此類案件上證據蒐集、犯罪事實之舉證有其難度，亦或是告訴人與被告和解撤回告訴[22]，不論是哪一種原因造成，

[19]以 2023 年 1-7 月為計算基礎，全國地方檢察署新收案件 49 萬 1,733 件，起訴及聲請簡易判決處刑共計 153,479 件，緩起訴占 20,726 件，兩者相加所占比例約為百分之 35。法務部網站，https://www.rjsd.moj.gov.tw/RJSDWeb/common/WebList3_Report.aspx?menu=INF_COMMON_P&list_id=779（最後瀏覽日：8/27/2023）。

[20]法務部網站，https://www.rjsd.moj.gov.tw/RJSDWeb/common/WebList3_Report.aspx?menu=INF_COMMON_P&list_id=806（最後瀏覽日：8/27/2023）。

[21]司法院網站，https://www.judicial.gov.tw/tw/cp-1887-477004-a6a73-1.html（最後瀏覽日：8/27/2023）。

[22]營業秘密法第 13 條之 1 第 1 項規定之「一般侵害營業秘密罪」，依同法第 13 條之 3 第 1 項之規定，需告訴乃論。

對於營業秘密之所有人來說，都顯得對其權益保護不足；而營業秘密法案件平均每件結案日數高達154日，則可能有地方檢察署對於此類案件仍不熟稔[23]、辦案人員對於案件中的構成要件認定有困難、蒐集證據及舉證耗費時間較多、辦案資源不足等因素作祟。

筆者於民國2013年起分發至臺灣桃園地方檢察署服務，而於民國2015年至2019年間，因曾經在桃園地方法院擔任公訴檢察官蒞庭時，對應的法官為智慧財產權法專股[24]，以及在偵查組的最後2年兼辦智慧財產權法案件，而有幸曾經辦理數件營業秘密法相關規範之偵查及公訴案件，在案件偵查、審理的過程當中，實際接觸到地方檢察署檢察官在辦理此類型案件時，可能會遇到的上述困難與瓶頸，包括營業秘密構成要件的認定、營業秘密經濟價值的計算、營業秘密的範圍、在偵查過程當中要如何確保營業秘密不致洩漏、偵查保密令的運用、境外使用營業秘密的認定、辦案人員對於營業秘密案件的不熟悉導致平均結案日數較長、法院在審理時如何確保營業秘密不致外流等，也同時在調查程序當中，就營業秘密對於從告訴人本身、到相關產業、甚至國家經濟發展、國家競爭力之關鍵地位有更進一步的認識。

[23]以民國2020年為例，全國地方檢察署偵查案件終結人數為619,134人，營業秘密法案件偵查案件終結人數僅為352人，全國地方檢察署實際上能接觸到營業秘密法案件的檢察官並不多，以致於檢察官在初次接觸此類型之案件時，可能會耗費更多的時間在研究如何辦理此類刑的案件。

[24]見臺灣桃園地方法院網站，https://tyd.judicial.gov.tw/tw/cp-6780-215785-38e4f-181.html（最後瀏覽日：8/27/2023）。針對各種專業案件類別，由相對應的特定法官股別審理，藉由其反覆審理專業案件累積經驗，有助於提升裁判品質、效率及裁判之可預測性。

基於包含以上所述之諸多原因如各國相關法制修法動作頻仍、對於各產業科技技術發展的競逐、我國營業秘密案件件數之快速增長、營業秘密案件偵查審理的困境，以及營業秘密案件所涉賠償、罰金金額龐大[25]，對於國家安全、產業經爭力影響巨大等因素，凝聚成為本研究欲針對營業秘密保護法制、國家核心關鍵技術保護法制之研究動機。

(二)、研究目的

若從「防範國家關鍵技術外流」之上位概念俯瞰，營業秘密法制屬於保護關鍵技術外流整體法制之一環，主要功能在於防止國家關鍵技術遭到不法方式竊取之外流。除此之外，關鍵技術直接外流之出口管制、間接外流之外資投資審查，在其他國家之法律制度上都受到相當程度之重視，近年來也持續補強，成為世界各國關鍵技術的綿密保護網。

我國此次國安法修正，將「國家核心關鍵技術之營業秘密」之相關規定，在國安法當中處理，結合了「營業秘密」及「國家核心關鍵

[25]大立光控告先進光案，法院曾判決先進光須賠償新臺幣 15.2 億元。見中時新聞網，https://tw.stock.yahoo.com/news/%E5%A4%A7%E7%AB%8B%E5%85%89-%E5%85%A7%E9%AC%BC%E5%B7%A5%E7%A8%8B%E5%B8%AB-%E7%AB%8A%E6%A9%9F%E5%AF%86-%E4%B8%8B%E5%A0%B4%E8%B6%85%E6%85%98-%E5%85%AC%E5%8F%B8%E7%94%A81%E6%8B%9B%E9%80%9A%E6%AE%BA-031735140.html（最後瀏覽日：09/11/2023）。美國政府控告聯電違反聯邦營業祕密保護法一案中，聯電以認罪協商之方式，支付美金 6000 萬元罰金，並承諾配合美國政府針對共同被告福建晉華進行調查和起訴。見美國司法部網站，https://www.justice.gov/opa/pr/taiwan-company-pleads-guilty-trade-secret-theft-criminal-case-involving-prc-state-owned（最後瀏覽日：9/11/2023）。

技術」，但是此種結合兩者之立法模式，卻是我國所獨有。因此，其他國家在防範關鍵技術外流之法制，是如何處理「營業秘密」及「國家關鍵技術」之保護？其他國家在外資審查、出口管制法制方面如何防止關鍵技術之外流？各有哪些最新的法律制度來防範關鍵技術外流？其成效如何？我國在相關現行防範關鍵技術外流法制層面，有哪些現有規範可以利用？現行規範有沒有需要補強之處？此次修正國安法是否妥適？未來努力方向？嘗試回答上開問題即為本研究之研究目的。

(三)、研究過程

由於本身在大學及研究所時期就對智慧財產權法制有濃厚研究興趣，碩士論文也是選擇與智慧財產權法相關主題，營業秘密法又是其中相當新而且對於我國國家安全、產業競爭力影響重大之領域。觀察前人的研究成果，雖然對於營業秘密法制之研究已經有許多文獻，但是對於「國家核心關鍵技術之保護」(或是敏感科技保護)整體法制部分，文獻之數量較少。此次出國擔任訪問學者，恰巧適逢我國國安法新增「國家關鍵核心技術之營業秘密」之相關規定，不但符合研究興趣，也是法務部所認可之研究領域，在國際上，也是各國當前修法保護重點，因此選定「營業秘密保護之研究-以國家核心關鍵技術保護為中心」作為研究題目。

「國家核心關鍵技術之保護」之法律制度，要一窺其完整之輪廓，除了營業秘密法制外，也涉及外資投資審查、出口管制等法律制度，我國此次僅針對竊取外流部分，在國安法處理「國家核心關鍵技術之營業秘密」遭不法竊取外流之相關議題，而在外資投資審查、出口管制部分，則並無配套措施，在研究之過程中，其他國家之作法便引起我的興趣。

本研究挑選美國及韓國作為我國法制之研究、參考對象，原因在於美國營業秘密法、經濟間諜法發展已有一定之時間，且在保護國家關鍵技術之外資投資審查、出口管制法制發展上，都有許多新動態值得研究。而韓國則是世界上唯一以一部專法統一處理國家關鍵技術之防止竊取、外資投資審查、出口管制等規範之國家，且其國家產業發展狀況與我國雷同，可供我國作為未來修法參考之用。

研究方向之選擇，其實也是在研究過程當中慢慢浮現，起初只是一個起心動念，後來慢慢經由大量的蒐集、閱讀國內外相關文獻並且內化後，才逐漸對於細部之研究方向有更深刻的想法，甚至再一次次地回頭來充新審視本研究整體的架構，試圖聚焦本研究之核心議題。

二、研究方法、範圍及限制

(一)、研究方法

本研究將結合歷史、案例、文獻分析及比較研究等研究方法，蒐集的文獻包含各國立法機關、行政機關制定或公布之法律及司法機關之判決等主要法源與法律百科全書、論文、專書及期刊文章、網頁資料、網路法律資料庫等次要法源[26]。

(二)、研究範圍

本研究範圍將以美國、韓國、我國之營業秘密法制、外資投資審查法制、出口管制法制等關於「防範國家關鍵技術外流」之整體法律制度。

(三)、研究限制

1. 語言限制

受限於筆者本身之語言能力以及從事研究時身處美國哈佛大學，且為了確保研究內容之精確，本研究主要以英文、中文文獻作為研究材料，未能兼顧其他語言之文獻，而使本研究在文獻引用上有所侷限。

[26]Harvard Law School Library Website, https://guides.library.harvard.edu/law/researchstrategy/primarysources#s-lg-page-section-2497248（last visited：9/11/2023）.

2. 時間範圍限制

本研究之研究期間為 2023 年 9 月 1 日至 2024 年 5 月 30 日，故研究所引用之資料都是發生在 2024 年 5 月 30 日前，為本研究在時間範圍上之限制。

3. 地理範圍限制

本研究之主要研究對象為美國、韓國、我國之相關法制，此為本研究在地理範圍區域上之限制。

4. 資料完整性限制

本研究之撰寫期間，筆者均身處美國哈佛大學，故主要以在美國能蒐集到的文獻為主。而在美國哈佛大學因為有訪問學者的身分，可以在哈佛大學法學院之圖書館現場使用圖書館內附設電腦，運用哈佛大學法學院所訂閱之付費法學資料庫，故能查閱之付費資料庫資源較為豐富，因為使用付費法學資料庫查閱相關資料之效率較高，因此也大量使用線上資料庫中所能蒐集的資料。此為本研究之資料完整性之限制。

5. 時間資源限制

在美國哈佛大學柏克曼網路暨社會研究中心[27]研究期間，因實際研究時間約為 9 個月，在研究工作之外，到哈佛大學法學院旁聽兩門課程及平時閱讀課程指定資料，及每周參加前開研究中心舉辦之各國學者研討會，探討各種科技、網路、社會公益相關法律研究，均影響實際能投注在本研究之時間資源，此為本研究之時間資源限制。

貳、美國防範國家關鍵技術外流法制

世界各國防範關鍵技術外流之法制，在制度設計上大多採取防止技術竊取、外資投資審查及出口管制，而防止竊取通常就是透過營業秘密保護，美國也不是例外。傳統上美國擁有強大的技術實力，並藉以維持其經濟發展、軍事上之領導地位，然而，隨著新興科技之發展與擴散，其優勢逐漸減弱，對於其國家安全及經濟發展有所影響。因而在防範國家關鍵技術外流之法制上，近年來都有所變革。本文以下將針對美國以上三種面向予以探討美國防範技術外流法制之最新發展。

[27] Berkman Klein Center for Internet & Society at Harvard University.

一、美國營業秘密法制發展

(一)、民事法律規範

1. 州法[28]

營業秘密作為智慧財產權最原始的型態，已經存在了數千年。收成蠶絲的秘密方法讓中國的特定區域獲利了數個世紀；而一個亞美尼亞人家族在管絃樂鈸片製作領域保有 400 年的領先，正因為其小心守護其營業秘密。這些早期的營業秘密並無法律規定要求所有人細緻的保護營業秘密，此時，營業秘密的佔有包含了其所有權的一切[29]。

美國現代營業秘密法源自美國馬薩諸塞州(MASSACHUSETTS)19 世紀早期的普通法(COMMON LAW)[30][31]，自契約法與侵權法的原理原則演化

[28]聯邦法與州法各司其職，聯邦法律使用於全體美國人民，州法則適用於特定州(領地)之人民；聯邦法例如移民法、破產法、專利法、聯邦刑法、社會安全和補充保障收入法、聯邦反歧視與民權法等，州法則處理特定州(領地)的刑事案件、婚姻和家事案件、遺囑及遺產事件、房地產和其他財產案件、商業契約案件、人身傷害案件等。
See LawHelp Website, https://www.lawhelp.org/resource/the-differences-between-federal-state-and-loc（last visited：9/24/2023）.

[29]Daniel G. Mackrides, *Trade Secret Law in the Wake of Defend Trade Secrets Act of 2016*, 47 DEL. J. CORP. L. 65(2022),at 67.

[30]普通法系，或稱英美法系、英國法系或海洋法系，是與歐陸法系（又稱大陸法系或羅馬法系）齊名的兩大法系之一，起源於中世紀的英格蘭，目前世界人口的三分之一（約 24 億人）生活在英美法司法管轄區或混合民法系統內，其中大部分來自大英國協國家。從法律淵源來看，英美法系的特點就是判例法，即反覆參考判決先例，最終產生類似道德觀念一般的普遍的、約定俗成的法律。維基百科網站，https://zh.wikipedia.org/zh-tw/%E8%8B%B1%E7%BE%8E%E6%B3%95%E7%B3%BB（最後瀏覽日：9/15/2023）。

[31]在 1837 年的 Vickery v. Welch 案件當中，法院認為被告有營業秘密的不當取用(misappropriation)，故需賠償原告；而在 1866 年的 Taylor v. Blanchard 當中，法院對於潛在的營業祕密不當取用，核發禁制令(injunctive relief)。See Vickery v. Welch, 36 Mass. (19 Pick.) 523(1837)、Taylor v. Blanchard, 95 Mass. (13 Allen) 370 (1866).

而來，因為當時的衝突大多牽涉到雇主與雇員間或是營業秘密所有人與惡意第三人之間之違反保密關係[32]。

隨著工業從普遍的農耕主義當中興起，營業秘密需要法律保護的需求持續增加，起初源自美國各州普通法的營業秘密，後來於 1939 年正式出現在當年出版的第一版侵權行為法彙編(Restatement of Torts)[33]當中的 757 條到 759 條當中。在第一版侵權行為法彙編當中，第 757 條對於營業秘密的定義為：「營業秘密可以由任何公式、圖案、裝置、資訊彙編所組成，被使用在個人的商業中，並且可以給予個人針對不知道或沒有使用前開營業秘密之競爭者優勢之機會。它可能是一個化合物的公式、一個製造、處理或保存材料的過程、一個機器或其他裝置的圖案、或是一個客戶名單。」[34]營業秘密必須是秘密，不能是公開地所能取得之知識，營業秘密也不需具備新穎性，它可以是對現有技術的改進，或是透過檢查現有技術後的發現[35]。這些條文反

[32]Steven Miller, *Repeal the Defend Trade Secret Act: Why Congress Can't Rely on Trade Secret Law to Protect America's Trade Secrets*, 28 J. INTELL. PROP. L. 213, 217-218 (2020).

[33]法律彙編是一系列由美國法律協會(American Law Institute)出版的法學論文，目標是將英美法的一班原理原則傳達給法官及律師，目前該協會已出版四個系列的法律彙編，該協會是由法官、學者及法律從業人員於 1923 年所組成。在 1923 年到 1944 年間，該協會出版了第一版法律彙編，包含侵權行為法彙編等之一系列法律彙編。See Wikipedia website, https://en.wikipedia.org/wiki/Restatements_of_the_Law（last visited：9/16/2023）.

[34]原文如下：「A trade secret may consist of any formula, pattern, device or compilation of information which is used in one's business, and which gives him an opportunity to obtain an advantage over competitors who do not know or use it. It may be a formula for a chemical compound, a process of manufacturing, treating or preserving materials, a pattern for a machine or other device, or a list of customers.」; See RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (AM. L. INST. 1934).

[35]Mackrides, *supra* note 29.

映了美國法院針對營業秘密的基本原則所做的決定[36]。

雖然第一版侵權行為法彙編闡明了法院所闡明的應業秘密法基本原則，營業秘密法在美國各州的發展卻是不均勻的，在擁有大型許多商業中心的州比較發達，而在農業較多的州則比較稀疏。事實上，隨著時間的推移，營業秘密法的變化很大，以致於 1979 年出版的第二版侵權行為法彙編，並未囊括營業秘密法的部分[37]。

為了統一全國的營業秘密法，並且嘗試在秘密持有人之權利及科技之需求之間獲得折衷，統一州法委員會(Uniform Law Commission, 簡稱 ULC)[38]創造了統一營業秘密法(Uniform Trade Secrets Act, 簡稱 UTSA)[39]，儘管 UTSA 在許多方面都與英美法不同，卻很快得到各州的批准，到了 2014 年 UTSA 已經在全美 48 個州、哥倫比亞特區、波多黎各、美屬維京群島均獲得某種形式的通過。雖然與 UTSA 有些許細微出入，1994 年出版的第三版不公平競爭法律彙編也對於營業秘密法保護提供概述。有些州仍然遵循第一版侵權行為法彙編第 757 條

[36] *Id*, at 68.
[37] *Id.*
[38]統一州法委員會於 1892 年成立，為各州提供無黨派、構思周密及起草良好的立法，使各州成文法的關鍵領域獲得清晰和穩定。委員會成員必須是擁有律師執業資格的律師，他們是被州政府、哥倫比亞特區、波多黎各、美屬維京群島任命的執業律師、法官、立法者、立法人員和法學教授，在統一州法是理想且實際的領域中，負責研究、起草、推動統一州法的頒布。See Uniform Law Commission website, https://www.uniformlaws.org/aboutulc/overview（last visited：9/17/2023）.
[39]於 1979 年出版。See Uniform Law Commission website, https://www.uniformlaws.org/committees/community-home?communitykey=3a2538fb-e030-4e2d-a9e2-90373dc05792（last visited：9/17/2023）.

到 759 條之英美法原則，有另外一些州則實施自身獨立的營業秘密法規[40]。

2.聯邦法

就營業秘密法的民事規範而言，直到 20 世紀末仍然維持在州法的範圍，儘管國會在 1996 年通過了經濟間諜法(Economic Espionage Act of 1996, 簡稱 EEA)[41]，將侵害營業秘密之行為，在聯邦法律的層級上刑罰化，惟若營業密密持有人只希望尋求民事救濟，則仍然使用州法的民事救濟。由於各州在 UTSA 的執行上有所差異，造成營業秘密所有人難以制定全國性的保密政策。為了解決這些差異，國會開始著手制定聯邦層級的營業秘密法，參議院跟眾議院[42]在 2014 年分別提出自己版本的營業秘密法，但是兩者皆未能通過。僅管如此，建立一個聯邦層級的民事營業秘密法案的想法，獲得兩黨廣泛的支持，最終，國會在 2016 年通過了營業秘密防護法案(Defend Trade Secret Act of 2016, 簡稱 DTSA)[43]。

儘管營業秘密法的來源隨著國家歷史的演化上多有不同，一個營

[40]Mackrides, *supra* note 29, at 68.
[41]Economic Espionage Act of 1996, P. L. 104-294(October 11, 1996), 110 Stat. 3489, codified at 18 U.S.C. §1831 et seq.
[42]美國國會是一個兩院制的立法機構，分為兩個平等的機構，眾議院和參議院，每個州選出代表和參議院進入國會，儘管兩院的結構不同，擁有各自的腳色及責任，但兩院共同合作並通過立法。任何法案皆須經過兩院批准才能成為法律。See U.S. CAPITOL visitor center website, https://www.visitthecapitol.gov/explore/about-congress（last visited：9/23/2023）.
[43]Mackrides, *supra* note 29, at 68-69；Defend Trade Secrets Act of 2016, P. L. 114-153(May 11, 2016), 130 Stat. 376, codified at 18 U.S.C. §1836 et seq.

業秘密的法律上主張，有 3 個共同要素：1.原告的資訊必須符合營業秘密的要件、2.獲取營業秘密的行為某種程度上是不當的，屬於「不當取用」、3.原告保護營業秘密的行為必須是「依具體情況下是合理的」或適當的[44]。

在聯邦層級的營業秘密法民事救濟途徑還沒出現之前，德拉瓦州的衡平法院[45]曾是提起此類訴訟的著名地點。該法院長期享有「世界上主要解決公司內部治理事務法院」的名聲，也在 1950 年代以來在許多著名的營業秘密法案件中作出判決。尋求營業秘密保護的企業，在考慮選擇法院時，會青睞「與不當取用營業秘密者解決爭議的速度及運用禁制令救濟之專業知識」，在數十年來，該法院證明其為符合上述兩者需求的首選法院。除了速度與經驗之外，該法院在授予懲罰性賠償金之能力、通常會維持契約中的協議管轄條款、在各種不同的案件當中適用他轄法律的廣泛經驗，對於營業秘密之擁有者也具有吸引力。基於以上種種優勢，部分論者認為該法院是 DTSA 出現，執行營業秘密權利之首要法院[46]。

---

[44]Mackrides, *supra* note 29, at 69.

[45]衡平法院是一種具有授予非金錢賠償權力之法院類型，這些賠償包括禁制令、書面命令及特定履行。傳統上，英國法院區分可以授予金錢賠償的普通法法院跟不能授予金錢賠償的衡平法法院。Court of Chancery 就是英國早期衡平法院的例子。此兩種類型法院的區別在現在基本已經被消除。在美國，1938 年採行的「聯邦民事訴訟程序規則」給予法院針對普通法及衡平法事項之合併管轄權。破產法院跟某些特定之州法院(德拉瓦州、密西西比州、紐澤西州、田納西州)可以被視為衡平法院的僅存例子。See Cornell Law School Website, https://www.law.cornell.edu/wex/court_of_equity（last visited：9/23/2023）.

[46]Mackrides, *supra* note 29, at 69-70.

(二)、刑事法律規範

1. 州法

在州法部分，僅有 23 州對於營業秘密採取刑事規範保護[47]，這些州對於營業秘密的保護，主要分成兩種。少數州是將營業秘密法獨立成一章來規範，而多數州則是將營業秘密之規定放置於財產權或智慧財產權之規範下，而處罰竊盜、重製等行為[48]。這些州法在範圍跟刑度上都有很大的差異[49]。有學者認為，由於多數州都並未將營業秘密犯罪獨立成章，而是將營業秘密是為財產權之內容而為保護，犯罪態樣甚多，各州對於營業秘密之定義也有過於廣泛的現象，對於打擊營業秘密犯罪，恐有困難[50]。且 UTSA 本身並無法律效力，僅為各州參考範本，需要各州自行立法規範，故對於跨州或聯邦層級的竊取營業秘密案件仍然無法規範[51]。綜上所述，在 EEA 制定之前，州刑事法對於營業秘密之保護，不是法律效力不足，就是構成要件無法涵蓋所有行為主體及行為態樣，由於商業逐漸發達，營業秘密侵害行為也並不限

[47]林志潔（2016），〈美國聯邦經濟間諜法之回顧與展望-兼論我國營業秘密法之刑罰化〉，《科技法學評論》，13 卷 1 期，頁 10。
[48]多數州的做法，又可區分有無將竊取營業秘密罪獨立成罪，而非僅為財產權下之一種犯罪態樣。見林志潔，前揭註 47，頁 10。
[49]Todd Kowalski, Caitlyn Coffey, Christina Danberg, Jessica Tsibidis-Goldberg, *INTELLECTUAL PROPERTY CRIMES,* 60 Am. Crim. L. Rev. 1003(2023), at 1020.
[50]林志潔，前揭註 47，頁 11。
[51]林志潔，前揭註 47，頁 11。

於州內，聯邦層級的 EEA 方才因此產生[52]。

2.聯邦法

(1)1934 年國內贓物法(National Stolen Property Act of 1934,簡稱 NSPA)

NSPA[53]針對任何人「在跨州或國際貿易中，運輸、傳輸或轉移價值 5000 美元以上的商品、器具、貨物、證券或貨幣，且明知前開商品、器具、貨物、證券或貨幣為竊取、侵占、詐欺所生」之行為，提供刑事制裁[54]。NSPA 原先並非為了適用於營業秘密竊取案件，事實上，法院普遍認為單純竊取無體財產[55]之行為並非犯罪行為[56]；然而，當有體財產被竊取時，NSPA 確實有保護智慧財產。儘管如此，最高法院對於 NSPA 是否可以適用於營業秘密，並無明確的裁決[57]。

在 EEA 立法以前，聯邦法上對於侵害營業秘密之行為，主要是以 NSPA 來規範[58]，該法之目的是為了跨州運送贓物而迴避州管轄權的問

---

[52]林志潔，前揭註 47，頁 11。
[53]See 18 U.S.C. § 2314 et seq.；美國法典是美國通用及永久法律，按照主題整合及編纂的成果。美國法典是由美國眾議院法律修訂委員會辦公室所出版。See U.S. House of Representatives website, https://uscode.house.gov/（last visited：9/29/2023）.
[54]Todd Kowalski, Caitlyn Coffey, Christina Danberg, Jessica Tsibidis-Goldberg, *supra* note 49, at 1013-1014.
[55]無體財產是指沒有實體存在的財產，無體財產的例子像是專利、專利申請、商標、商業名稱、服務標誌、著作權、營業秘密。See Cornell Law School website, https://www.law.cornell.edu/wex/intangible_property（last visited：9/29/2023）.
[56]Todd Kowalski, Caitlyn Coffey, Christina Danberg, Jessica Tsibidis-Goldberg, *supra* note 49, at 1014.
[57]*Id.*
[58]林志潔，前揭註 47，頁 7。

題[59]。在資訊時代，無體智慧財產權可能比有體財產具有更高價值，並且在科技進步的同時，竊取營業秘密的客體也不在限於有體財產，NSPA 顯然不足以規範竊取營業秘密行為[60]。

(2)營業秘密法(Trade Secret Act, 簡稱 TSA)

在 EEA 之前，聯邦法唯一特別處理營業秘密竊取行為的只有 TSA[61]，TSA 將政府員工未經授權而洩漏機密訊息之行為定為犯罪行為[62]。因為 TSA 無法適用於私人部門，且只有提供輕罪(misdemeanor)[63]的刑事制裁，聯邦檢察官傳統上使用 EEA、NSPA、郵件和電信詐欺法(Mail and Wire Fraud Statutes)[64]來追究不當取用營業秘密的指控[65]。

(3)郵件和電信詐欺法(Mail and Wire Fraud Statutes)

美國法典第 18 編第 1341、1343 條之規範，提供了對於使用或使他人使用郵件和電信服務進行詐欺行為之刑事制裁[66]。與 NSPA 不同，郵件和電信詐欺法已經廣泛適用在竊取無形財產，包含營業秘密[67]。

---

[59]林志潔，前揭註 47，頁 7。
[60]林志潔，前揭註 47，頁 7。
[61]See 18 U.S.C. § 1905.
[62]Todd Kowalski, Caitlyn Coffey, Christina Danberg, Jessica Tsibidis-Goldberg, *supra* note 49, at 1017.
[63]輕罪是刑法下可以處罰的一種犯罪類型。輕罪通常是一種刑罰不超過 12 個月監禁的犯罪。對於輕罪，通常會施以社會服務、緩刑、罰款及少於 1 年之監禁等處罰。更嚴重的犯罪則稱為重罪(felony)，伴隨更嚴厲的刑罰，包含超過 12 個月的監禁。許多州將輕罪根據犯罪嚴重程度及刑罰分成不同的類型。See Cornell Law School website, https://www.law.cornell.edu/wex/misdemeanor（last visited：9/29/2023）.
[64]See 18 U.S.C. §1341, 1343.
[65]Todd Kowalski, Caitlyn Coffey, Christina Danberg, Jessica Tsibidis-Goldberg, supra note 49, at 1017.
[66]*Id.* at 1018.
[67]*Id.*

郵件和電信詐欺法雖然因此受到聯邦檢察官的青睞，對於不當取用營業秘密之行為之刑事訴追，並無太大的幫助[68]。因為營業秘密可以用網路、磁片或是以人類單純記憶之方式快速傳輸，在這些情況下都不會使用法條規定要件的郵件、電話或資料傳輸，而不會構成犯罪，新科技的進展與法規之間仍有落差[69]。

(4)1986 年電腦詐欺及濫用法(Computer Fraud and Abuse Act of 1986，簡稱 CFAA)

CFAA[70]針對儲存在受保護電腦上之營業秘密不當取用，提供刑事制裁及民事救濟[71]，違反 CFAA 的態樣可能是外部人未經授權而為或是內部人超過被授予的權限而為[72]。雖然 CFAA 並非專門針對營業秘密的不當竊取而設，當電子型態之營業秘密被從電腦系統上取走時，CFAA 就會被使用於刑事起訴[73]。根據 CFAA 而來之罰金或處罰各有不同，在「犯罪目的為商業優勢或私人經濟利益」之情況下，個人可能會面臨

[68]益思科技法律事務所(2003)，〈營業秘密法制之研究〉，頁 53，經濟部智慧財產局 92 年度委託學術機構研究案期末報告書。
[69]益思科技法律事務所，前揭註 68，頁 53。
[70]Computer Fraud and Abuse Act of 1986, P. L. 99-474(October 16, 1986), 100 Stat. 1213, codified at 18 U.S.C. § 1030.
[71]Todd Kowalski, Caitlyn Coffey, Christina Danberg, Jessica Tsibidis-Goldberg, *supra* note 49, at 1019.
[72]*Id.*
[73]Paul D. Ackerman, Esq., Aimee N. Soucie, Esq., Hunton Andrews Kurth(2020), *An Overview of Trade Secrets Law*, at 4, https://www.huntonak.com/images/content/6/5/v2/65081/an-overview-of-trade-secrets-law.pdf（last visited：9/29/2023）.

罰金及最多 5 年的監禁[74]。

(5)1996 年經濟間諜法(Economic Espionage Act of 1996，簡稱 EEA)

美國在 EEA 立法之前，能夠涵蓋侵害營業秘密行為之法律，若非法律效力不足，就是構成要件無法涵蓋所有行為主體及行為態樣，在商業越來越發達，而侵害營業秘密之行為也不僅限於州內時，EEA 因此而生[75]。

作為對於逐漸增加的外國政府、機構及代理人對於不當取用美國公司營業秘密努力之回應，美國國會在 1996 年頒布了 EEA，對於營業秘密竊取行為，提供刑事及民事處罰[76]。2016 年國會通過了 DTSA，該法案補充了 EEA，針對營業秘密不當竊取，創造了私人民事訴訟程序[77]。EEA 建立了兩種關於竊取營業秘密可起訴的犯罪，第 1 種是第 1831[78]條的「經濟間諜罪」(economic espionage)，只有在竊取行為有利於外國政府、機構或其代理人之情況才適用，且其處罰較第 2 種犯罪更嚴重[79]。第 2 種則是 1832[80]條規定的「竊取營業秘密罪(theft

[74] *Id.*
[75] 林志潔，前揭註 47，頁 11。
[76] Todd Kowalski, Caitlyn Coffey, Christina Danberg, Jessica Tsibidis-Goldberg, *supra* note 49, at 1005-1006.
[77] Todd Kowalski, Caitlyn Coffey, Christina Danberg, Jessica Tsibidis-Goldberg, *supra* note 49, at 1006.
[78] See 18 U.S.C. §1831.
[79] Todd Kowalski, Caitlyn Coffey, Christina Danberg, Jessica Tsibidis-Goldberg, *supra* note 49, at 1006.
[80] See 18 U.S.C. §1832.

of trade secrets)，攸關任何有利於非真正營業秘密擁有者的竊取行為，適用於國內外之營業秘密爭議[81]。

(三)、1996 年經濟間諜法介紹

1.營業秘密的定義

EEA 保護「所有形式和類型的財務、商業、科學、技術、經濟或工程資訊...無論是有體還是無體，無論是否或如何以物理、電子、圖形、照片或書面形式儲存、編輯或記憶....」[82]。根據 EEA 之規定，前開資訊若符合下列條件，則可以做為營業秘密而受到保護：（I）擁有者已採取合理措施來保密該訊息、（II）該資訊由於不被他人普遍知曉，且他人無法通過適當手段輕易確定，而具有實際或潛在的獨立經濟價值，而他人可從該資訊的揭露或使用獲得經濟價值[83]。

2.罪名種類

(1).經濟間諜罪

根據 EEA 第 1831 條規定，「經濟間諜」是指意圖或知情將裨益外國政府、機構或其代理人，而不當取用營業秘密之行為[84]。營業秘

[81] *Id.*
[82] See 18 U.S.C. §1839(3).
[83] See 18 U.S.C. §1839(3)(B).
[84] See 18 U.S.C. § 1831(a).

密之不當取用包含單純竊盜[85]、未經授權複製[86]、販入及持有竊取而來之營業秘密[87]，以及試圖[88]或共謀[89]為這些犯行。為了符合知情之要件，政府必須證明被告知道其所持有的資訊是營業秘密[90]。政府毋庸證明外國政府實際受益於營業秘密，證明竊取營業秘密是為了裨益外國政府即足[91]。

違反此條而被判決有罪的個人被告，將面臨最高 15 年之監禁或罰金美金 500 萬元，或兩者兼具[92]。組織違反本條而判決有罪者，將面臨最高美金 1,000 萬元或被竊取之營業秘密價值之 3 倍，包含該組因此避免的相關研發費用[93]。

2012 年的外國及經濟間諜罪刑加重法案(The Foreign and Economic Espionage Penalty Enhancement Act of 2012)[94]，將個人犯罪之罰金從美金 50 萬元提高至美金 500 萬元[95]。對於組織而言，則是將罰金數額修正為美金 1,000 萬元或被竊取之營業秘密價值之 3 倍兩者中較高者[96]。此法案還要求美國量刑委員會(United States

[85]See 18 U.S.C. § 1831(a)(1).
[86]See 18 U.S.C. § 1831(a)(2).
[87]See 18 U.S.C. § 1831(a)(3).
[88]See 18 U.S.C. § 1831(a)(4).
[89]See 18 U.S.C. § 1831(a)(5).
[90]Todd Kowalski, Caitlyn Coffey, Christina Danberg, Jessica Tsibidis-Goldberg, *supra* note 49, at 1008.
[91]*Id.*
[92]See 18 U.S.C. § 1831(a).
[93]See 18 U.S.C. § 1831(b).
[94]The Foreign and Economic Espionage Penalty Enhancement Act of 2012, P.L. 112-269(January 14, 2013), 126 Stat. 2442.
[95]See 18 U.S.C. § 1831(a).
[96]See 18 U.S.C. § 1831(b).修正前之版本是僅有罰金 1000 萬美元。

Sentencing Commission)[97]修改關於經濟間諜及竊取營業秘密部分之美國量刑準則[98](United States Sentencing Guidelines)。美國量刑委員會因此在 2013 年做出回應而修改相關的準則[99]。

本條規定係針對外國政府介入經濟間諜之犯罪而做規定，且為經濟間諜行為做了具體定義[100]。若無法證明涉案之人背後有外國政府支持或指使，或意圖有利於外國政府或相關組織，及無法適用本條，而應援用第 1832 條進行偵查[101]。關於有利於外國政府或其關係組織者，並不僅限於「經濟上」之利益，尚包括「名譽上、策略上或戰略上」之利益[102]。

本條之處罰之所以偏重，係因經濟間諜行為除了損害營業秘密所有人之商機外，還會裨益其他國家，在現今全球經濟競爭之年代，若國內的重要經濟資訊不斷被竊取，將會壯大其他國家而削弱自身國家競爭力，受害人除了營業秘密所有人外，也包含國家整體[103]。

---

[97]美國量刑委員會是美國政府司法單位中的獨立機構，由 1984 年的量刑法案所創立，國會通過此法案來做為對於聯邦法院判決量刑中廣泛存在的不一致性之回應，透過創建該委員會及制定量刑準則，開啟了聯邦法院判決量刑的新時代。See United States Sentencing Commission website, https://www.ussc.gov/about-page（last visited：10/3/2023）.

[98]由美國量刑委員會頒布，法官在針對聯邦罪犯判決量刑時，會參考此準則，當準則有被修正時，會出版後續的準則手冊。See United States Sentencing Commission website, https://www.ussc.gov/about-page（last visited：10/3/2023）.

[99]Todd Kowalski, Caitlyn Coffey, Christina Danberg, Jessica Tsibidis-Goldberg, *supra* note 49, at 1008.

[100]林志潔，前揭註 47，頁 13。

[101]林志潔，前揭註 47，頁 13。

[102]章中信(2011)，經濟間諜法案簡介，著作權筆記網站，經濟間諜法案簡介 - 著作權筆記 (copyrightnote.org) （最後瀏覽日：10/6/2023）。

[103]林志潔，前揭註 47，頁 14。

(2).竊取營業秘密罪

根據 EEA 第 1832 條之規定，「竊取營業秘密」是為了營業秘密所有者之外之任何人的利益，而不當取用營業秘密[104]。此罪名「經濟間諜」罪有三種起訴條件的區別：（I）預期的利益必須是本質上經濟性的[105]、（II）被告必須故意或知情該罪行將傷害合法擁有者[106]、(III)此處的資訊必須與用於或意圖用於跨州或國外商務的產品或服務有關[107]。

違反第 1832 條之個人被告，將會面臨最高 10 年的監禁，或是依該法所定之罰金，或兩者兼具[108]。被判決有罪的組織則是面臨最高美金 500 萬元之罰金或被竊取之營業秘密價值之 3 倍[109]。

本條乃係針對美國國內傳統一般營業秘密竊取案件，與第 1831 條不同之處在於本條之行為人必須是將營業秘密轉化營業秘密所有人之外之「經濟上」利益，而不包括「名譽上、策略上或戰略上」利益[110]。因為美國國會當初立法目的係為了遏止外國政府之經濟間諜行為，因為其可能影響美國經濟及危害美國國安，而傳統的營業祕密竊

[104]See 18 U.S.C. § 1832(a).
[105]*Id.*
[106]*Id.*
[107]*Id.*
[108]*Id.*
[109]See 18 U.S.C. § 1832(b).
[110]林志潔，前揭註 47，頁 16。

取行為，對於國家經濟影響較不具威脅性，故構成要件較為嚴苛[111]。

3.實施情況

根據 EEA 產生的大部分刑事訴訟都涉及內部人對於營業秘密的竊取，而在 2001 年之前，所有根據 EEA 提起的訴訟都是根據第 1832 條提起的[112]。

在 EEA 施行的前 5 年，所有根據 EEA 起訴的案件，均需要美國司法部[113](U.S. Department of Justice)司法部長[114](Attorney General)、副司法部長(Deputy Attorney General)或刑事司[115]助理司法部長(Assistant Attorney General of Criminal Division)之明確批准[116]。儘管對於第 1832 條之起訴批准要求後來已經取消，但根據第 1831 條進行的經濟間諜起訴仍然需要國家安全司[117]助理司法部長(Assistant Attorney General of National Security

[111]林志潔，前揭註 47，頁 16。
[112]Todd Kowalski, Caitlyn Coffey, Christina Danberg, Jessica Tsibidis-Goldberg, *supra* note 49, at 1010.
[113]美國司法部的使命是維護法治、保障國家安全，以及保護公民的民權。See U.S. Department of Justice website, https://www.justice.gov/about（last visited：10/7/2023）.
[114]司法部長亦有翻譯為總檢察長，其為司法部的首腦，也是聯邦政府的首席執行官，在一般的法律事務中代表美國政府，並在總統和政府部門需要時提供意見。See U.S. Department of Justice website, https://www.justice.gov/ag（last visited：10/7/2023）.
[115]刑事司為美國司法部所屬單位，除了那些明確分配給其他司法部門的法律外，負責發展、執行和監督所有聯邦刑事法律的適用。See U.S. Department of Justice website, https://www.justice.gov/criminal/about-criminal-division（last visited：10/7/2023）.
[116]Todd Kowalski, Caitlyn Coffey, Christina Danberg, Jessica Tsibidis-Goldberg, *supra* note 49, at 1010-1011.
[117]國家安全司為美國司法部所屬單位，使命是通過法律追求正義，以保護美國不受到對於國家安全的威脅。國家安全司的組織結構旨在確保檢察官和執法機構以及情報律師和情報社區之間有更好的合作和相同目標，從而增強聯邦政府國家安全工作的效率。See U.S. Department of Justice website, https://www.justice.gov/nsd（last visited：10/7/2023）.

Division)的批准[118]。

除了前述的批准規定外，由於國會擔心過於嚴格的限制行為，將會限制美國的經濟發展，甚至會影響員工選擇工作的權利，使得案件量不如預期[119]。前開批准規定雖於 2001 年取消，惟於 2002 年又重行採用，且僅適用於第 1831 條之經濟間諜罪，原因在於經濟間諜罪之影響非限於美國國內而會延伸到外國政府，若起訴標準過於寬鬆，將對於國與國之關係有負面影響[120]。第 1832 條之批准規定刪除後，起訴案件逐年上升，1996 年到 2012 年就有上百件，同期間第 1831 條卻只有 9 件案件[121][122]。有學者認為，除了前開批准規定之外，條文本身之疑義，也可能是造成此結果之原因之一[123]。

政府在決定是否根據 EEA 進行起訴方面具有廣泛的自由裁量權，根據美國聯邦檢察官手冊[124](Justice Manual，2018 年前稱為 United

[118]Todd Kowalski, Caitlyn Coffey, Christina Danberg, Jessica Tsibidis-Goldberg, *supra* note 49, at 1011.
[119]林志潔，前揭註 47，頁 17。
[120]林志潔，前揭註 47，頁 18。
[121]林志潔，前揭註 47，頁 18。
[122]根據美國智慧財產權執法協調機構(U.S. Intellectual Property Enforcement Coordinator，IPEC)向美國國會每年提出的年度智慧財權報告(ANNUAL INTELLECTUAL PROPERTY REPORT TO CONGRESS)所統計之數據，2017 年第 1831 條起訴 2 件、第 1832 條 9 件；2018 年第 1831 條起訴 1 件、第 1832 條 10 件；2019 年第 1831 條起訴 2 件、第 1832 條 14 件；2020 年第 1831 條起訴 2 件，第 1832 條 6 件。1996 年到 2008 年，根據 EEA 起訴之案件共 96 件，平均 1 年 7.2 件，而 2009 到 2016 年，起訴的案件有 69 件，平均一年則是 8.6 件。See Rebecca Guiterman(2023), *DOJ'S INCREASED FOCUS ON CRIMINAL TRADE SECRET CASES*, Kropf Moseley website, https://kmlawfirm.com/2023/09/07/dojs-increased-focus-on-criminal-trade-secrets-cases/（last visited：10/12/2023）.
[123]林志潔，前揭註 47，頁 18。
[124]聯邦檢察官手冊包含了美國司法部公開的政策及程序，在美國司法部長之監督及副司法部長之指導下所準備的。美國聯邦檢察官辦公室(The Executive Office for United States Attorneys)負責協調司法部內各單位及領導階層來完成前開手冊的修訂。該手冊提供司法部內部準則之用，其目的並非、也不能被用創立任何程序或實質上的權利，或是在民、刑事訴訟中被任何一方依法執

States Attorneys' Manual)解釋到，EEA 並非要將所有在州法下可能有民事救濟途徑之竊取營業秘密案件都定罪。相反地，應該要裁量5 個適當的自由裁量因素[125]。

檢察官在決定是否以 EEA 第 1831、1832 條之罪名來起訴時，會考慮下列的因素：(1)犯罪的活動範圍，包括是否有外國政府、機構或其代理人涉入之證據、(2)對於營業密所有人之經濟上損害程度、(3)被不當取用之營業秘密類型、(4)可用之民事救濟措施之有效性、(5)起訴帶來的潛在威嚇價值[126]。對於潛在的被告公司，檢察官可能會考量額外之因素：(1)公司內部不正行為之普遍性、(2)公司是否願意在調查其代理人之過程中合作、(3)公司現存的法令遵循計畫之存在及有效性、(4)公司是否及時且自願揭露其不當行為[127]。

4. 實務上面臨之困境

美國當初立法就是希望可以打擊裨益外國政府之營業秘密竊取行為，以保護美國國內智慧財產之經濟發展以及國家安全，當時美國眾議院估計在 EEA 立法之 6 年內，將可以起訴 50 件經濟間諜案件，惟從 1996 年以來，該目標似乎僅在第 1832 條部分適用，多數案件係

行。此外，也不會對司法部在其他訴訟權利產生任何限制。See The United States Department of Justice website, https://www.justice.gov/jm/jm-1-1000-introduction （last visited：10/12/2023）.

[125]Guiterman, *supra* note 122.

[126]Todd Kowalski, Caitlyn Coffey, Christina Danberg, Jessica Tsibidis-Goldberg, *supra* note 49, at 1011.

[127]*Id.*

以竊取營業秘密罪起訴，而第 1831 條部分，計算至 2012 年為止，起訴的案件僅有 9 件，其中 5 件為認罪協商，剩下的僅有 1 件為有罪判決[128]。論者認為，實際執行與立法目的之落差，可能原因為：法院認定構成要件過於狹隘、國會積極修法卻未擊中要害[129]。

(1).法院認定要件過於狹隘

承前所述，由於從 EEA 施行以來，遭到司法部以經濟間諜罪調查的案件不多，而最後能進入法院審理程序的案件更少，所以使法院鮮有機會解釋構成要件，亦無重要判例可以遵循[130]。

立法者當時在制定經濟間諜法時，有意要擴張刑罰範圍，故將法條文字設計的較過去法律為廣，卻反而造成構成要件不明確，而必須要靠法院在個案的解釋，來決定是否個案符合處罰要件[131]。而目前法院對於各要件的解釋都過於狹隘，也會因舉證困難而削弱檢察官起訴之意願，而成為一個惡性循環，對於打擊外國經濟間諜行為將窒礙難行[132]。

(2).國會修法卻未擊中要害

美國國會在 2012 年雖以外國及經濟間諜罪刑加重法案，將第

[128]林志潔，前揭註 47，頁 19。
[129]林志潔，前揭註 47，頁 20-26。
[130]林志潔，前揭註 47，頁 20。
[131]林志潔，前揭註 47，頁 20。
[132]林志潔，前揭註 47，頁 20。

1831 條之個人及組織犯罪之罰金加重，希望能夠透過加重刑罰來達到嚇阻之效果，然而因為沒有對症下藥，對於構成要件並未修正，而無法將行為人入之於罪[133]。

(四)、2016 年營業秘密防護法介紹

1. 立法背景

原先美國國會在制定 EEA 時，實際上曾經考慮在原本的 EEA 當中，加入一個私人的請求權，但是部分立法者對於將私人民事救濟納入刑事法案當中一事表達憂慮，原本國會預計任內稍後再來討論此想法，結果過了 20 年，國會才實現這個打算[134]。雖然 EEA 被賦予崇高的期望，EEA 從施行至今，只產生了 125 個起訴及 10 個有罪判決[135]。同時，在 2012 年，國家安全局[136]局長 Keith Alexander[137]將軍，宣稱「透過網路間諜活動造成的工業資訊及智慧財產損失…是歷史上最大的財富移轉[138]」。在 2013 年，一個獨立、跨黨派的委員會[139]估計，美國

[133]林志潔，前揭註 47，頁 20。
[134]Miller, *supra* note 32, at 223.
[135]*Id.*經過筆者搜尋本篇論文作者所引用的數據資料，其統計之時間點應為 2013、2014 年左右。根據本文前開所提出的研究數據顯示，EEA 從制定以來至今，被起訴的案件雖然有逐漸增加的趨勢，整體而言，每年被起訴的案件數量都還是只有 10 到 20 件左右。
[136]國家安全局(National Security Agency)隸屬於美國國防部(U.S. Department of Defense)，任務為在密碼學領域引領美國政府，包括信號情報洞察和網絡安全產品與服務，並使電腦網絡操作為國家和其盟友贏得決定性優勢。See National Security Agency website, https://www.nsa.gov/About/Mission-Combat-Support/（last visited：10/15/2023）.
[137]於 2005/8/1 到 2014/3/28 間擔任國家安全局局長。
[138]Miller, *supra* note 32, at 223.
[139]美國智慧財產權盜竊委員會(Commission on the Theft of American Intellectual Property)，於 2012 年在國家亞洲研究局(The National Bureau of Asian Research)成立，旨在研究智慧財產權竊盜之規

企業每年因智慧財產遭竊而損失超過美金 3 千億元[140]。4 年後，相同的委員會估計，遭竊的營業祕密價值可能高達美金 6 千億元[141]。EEA 未能嚇阻、懲罰甚至減緩產業間諜的活動，而國會也注意到此點[142]。

DTSA 的起源可以追溯到 2012 年，參議員 Orrin Hatch 及 Christopher Coons 領導最初的改革，但是該法案並未通過，而眾議院在 2014 年重新推動了此法案，並且成為參議院制定 DTSA 之基礎。自 2012 年到 2020 年 11 月，在被提出的法案當中，只有百分之 1 到百分之 3 最終成為法律，DTSA 不但在國會中獲得通過，而且在主要的立法當中，也算是比較快速獲得通過的。由於有兩黨的支持以及私人產業美金 125 萬的遊說，DTSA 在 2016 年 5 月 11 日成為法律，自其在參議院被提出僅 287 天[143]。DTSA 在眾議院以 410-2 的票數獲得通過，而在參議院則是獲得一致通過，其之所以受到歡迎似乎是源於其保護美國智慧財產不受外國干預以及在聯邦層級將現有州法法規化的目標[144]。

模、範圍及後果。國家亞洲研究局則為一個非營利的獨立研究機構。See National Bureau of Asian Research website, https://www.nbr.org/about/（last visited：10/15/2023）.

[140]Miller, *supra* note 32, at 223.

[141]Miller, *supra* note 32, at 224.

[142]*Id.*

[143]*Id.*

[144]Mackrides, *supra* note 29, at 71.

2.立法目標

國會在設想一個全美國通用的營業秘密法時，在創建 DTSA 時有些特定之目標，諸如：(1)提供清楚的原則及可預測性、(2)仔細的劃定聯邦民事請求權、(3)建立快而有效的營業祕密訴訟及鼓勵創新、(4)促進營業秘密求償的統一性[145]。

首先,如果在 DTSA 及聯邦層級尋求營業秘密賠償,國會希望 DTSA 在如何適用法律方面有足夠一致的原則及結果會是如何方面上有可預測性。其次，透過針對特定營業秘密提供特定的請求權，營業秘密案件可以用相似及可預測之方式處理，可以提供一致性及穩定性。此種可預測性將有助於一個有效率且有效之系統，來保護營業秘密。第三,DTSA 特定具體之限制級明確的原則,希望可以提供快速的救濟及保護，並且減少商業交易及業務往來中的干擾。如此一來，公司及企業在營業秘密受到侵害時不會受到影響，而能夠有效的恢復工作。透過不干擾商業運作,DTSA 鼓勵企業持續創新，持續生產。最後，DTSA 之主要目標為促進更統一的法律體系以監督營業秘密求償訴訟。DTSA 提供條文、定義、條件來達到這個目的[146]。

[145]Victoria Hanson, *Improving the Defend Trade Secrets Act of 2016: Against Preempting State Trade Secret Law*, 2 NOTRE DAME J. oN EMERGING TECH. 164 (2021), at 168.
[146]*Id.*

3.重要條文內容簡介

除了創建一個聯邦層級的營業祕密民事訴訟外，DTSA 也創建了幾個有用的新規定，諸如管轄權要求(Jurisdiction requirement)、單方扣押(Ex parte seizure)及吹哨者豁免(Whistleblower immunity)[147]。這些規定都是在限縮 DTSA 之範圍及適用，使 DTSA 不至於超過其界限[148]。

(1).管轄權要求

DTSA 運用其管轄權要件來平衡聯邦與州間之營業秘密法，其提供聯邦的保護給特定種類的營業秘密，而其他營業秘密則交由州法保護。國會打算僅對被用於或預定被用於跨州或國際貿易的產品或服務相關的營業祕密提供保護[149]。這些 DTSA 的管轄要件要求和限制有助於降低濫訴行為及控制實際進入訴訟之案件。此外，透過要求營業秘密符合管轄權要件，這些要件將創造 DTSA 下營業秘密訴訟更大的一致性[150]。

自從 DTSA 施行以來，其管轄要求已限制了 DTSA 下營業秘密訴訟的數量。然而，營業秘密的範圍獨厚技術性的營業祕密，像是製造過

[147] *Id.*
[148] *Id.*
[149] See Defend Trade Secrets Act of 2016, §2(b)(1), 130 Stat. 376, at 376.
[150] Hanson, *supra* note 145, at 168-169.

程或是配方等，因為這些營業秘密最有可能將價值導向商品或服務，並且實際參與交易。其他類性的營業秘密像是商業性資訊，包含財務、策略、顧客方面的資訊，便無法達到 DTSA 的標準，除非跟前開要件有所關連[151]。

(2).單方扣押條款

在當事人之一方要求法院從違規者處扣押遭竊之營業秘密財產時，就是根據美國刑法典第 18 編第 1836 條(b)(2)[152]之單方扣押規定進行。法院只會在必要且特殊情況下，才會核發扣押財產之命令，來防止營業祕密被散布給他人或公眾[153]。國會深知此規定的威力，所以對於設定了特定條件，原告必須達到條件才能獲得扣押命令[154]。

原告為了要獲得單方扣押命令，原告必須證明初步禁制令[155]（preliminary injunction）及臨時禁止令[156]（temporary restraining order)不足以提供救濟[157]。更甚者，原告必須在其案件

[151]Hanson, *supra* note 145, at 169-170.
[152]See 18 U.S.C. § 1836(b)(2).
[153]See 18 U.S.C. § 1836(b)(2)(A)(i)；See also Defend Trade Secrets Act of 2016, § 2(a)(2)(A), 130 Stat. 376, at 376.
[154]Hanson, *supra* note 145, at 171.
[155]初步禁制令是一個可能在審判前或審判中獲發的禁制令，其目的在於在終局判決前保持現狀。See Cornell Law School website, https://www.law.cornell.edu/wex/preliminary_injunction（last visited：10/21/2023）.
[156]暫時禁止令是一個短期、審判前、暫時的禁止令，為了獲得暫時禁止令，一方必須說服法官，若不核發該命令，其將會立即受到不可彌補的損害。若法官認為必要，可以不經舉行聽審(hearing)就核發暫時禁止令。暫時禁止令之功能係作為臨時性措施，只在法院針對是否核發初步禁制令而舉行之聽審前有效。See Cornell Law School website, https://www.law.cornell.edu/wex/temporary_restraining_order (last visited：10/21/2023）.
[157]See 18 U.S.C. § 1836(b)(2)(A)(ii)；See also Defend Trade Secrets Act of 2016, § 2(a)(2)(A), 130 Stat.

上，提供足夠的證據給法院，來讓法院作出相關裁決，因此在訴訟的初步階段就帶給當事人很大的負擔。由於這些方面必須達到要求，國會試圖不讓此命令輕率的被授予，以此規定遭濫用及對被告造成負擔[158]。

(3).吹哨者豁免條款

根據美國刑法典第 18 編第 1833 條(b)之規定，吹哨者豁免條款使員工在員工祕密的將營業秘密揭露給特定機關或特定人時，免於刑事或民事責任[159]。此條款為一個安全港，對於那些幫助揭露營業秘密犯罪之人提供保護，免遭受痛苦及無情的報復。若無吹哨者豁免之規定，則企業可能面臨巨大損失之風險，而那些擁有資訊可以防止進一步損失之人可能因恐懼受到報復而不敢站出來[160]。

為了要讓員工可以受到吹哨者豁免條款保護之利益，雇主必須在與其員工的契約內通知員工關於吹哨者豁免條款之規定，並解釋吹哨者豁免條款與保密之間要如何運作[161]。此通知對於雇主在面臨營業秘密侵害而能獲得律師費及懲罰性損害賠償時至關重要[162]。吹哨者條款

376, at 376.
[158]Hanson, *supra* note 145, at 171.
[159]See 18 U.S.C. §1833(b)；See also Defend Trade Secrets Act of 2016, § 7, 130 Stat. 376, at 384-86.
[160]Hanson, *supra* note 145, at 171-172.
[161]See Defend Trade Secrets Act of 2016, § 7(b)(3)(A), 130 Stat. 376, at 385
[162]否則，雇主在對於該員工之侵害營業祕密民事訴訟中，將會無法獲得懲罰性賠償及律師費。See Defend Trade Secrets Act of 2016, § 7(b)(3)(C), 130 Stat. 376, at 385.

是 DTSA 當中唯一優先於州法適用之條款[163]，因為它是一個全新的規定，之前並未在 UTSA 或是州法中出現過[164]。

吹哨者豁免條款提供揭露營業秘密之人適當的保護，它是一個重要的安全港條款，但也不是絕對的免責，員工必須提供證據證明他們計畫使用不論何種他們所擁有的文件或訊息來揭露一個違法行為[165]。

(4). 民事救濟

DTSA 針對不當取用(misappropriation)營業秘密提供數種救濟途徑[166]，法院得依職權選擇授予禁制令[167](injunctions)、補償性損害賠償(compensatory damages)、懲罰性損害賠償(exemplary damages)[168]。

DTSA 明確規定，法院可以頒布禁制令以防止實際或潛在的營業祕密不當取用，前提是前開禁制令不可妨害個人就業，也不可以與禁止妨害就業之州法相衝突[169]。任何對於就業的限制必須建立在有不當

---

[163]優先權原則(preemption doctrine)是指當兩個不同層次的法律發生衝突時，更高級別的法律將取代較低級別的法律的原則。當州法和聯邦法發生衝突時，根據美國憲法第 6 條第 2 款的至高性條款（Supremacy Clause），聯邦法將取代(displace)或優先適用於(preempt)州法。不論衝突的法律是來自立法機關、法院、行政機構或憲法，此原則皆有適用。See Cornell Law School website, https://www.law.cornell.edu/wex/preemption （last visited：10/25/2023）.

[164]Hanson, *supra* note 145, at 172.

[165]*Id.*

[166]See 18 U.S.C. § 1836(b)(3)；Mackrides, *supra* note 29, at 77.

[167]禁制令是一個法院命令，可以要求個人為特定行為或停止特定行為。禁制領又可以分為永久禁制令、暫時禁制令及初步禁制令。See Cornell Law School website, https://www.law.cornell.edu/wex/injunction（last visited：10/27/2023）.

[168]See 18 U.S.C. § 1836(b)(3).

[169]See 18 U.S.C. § 1836(b)(3)(A)(i)(I)-(II).

取用營業秘密之證據上，而非僅因個人擁有營業秘密資訊之事實[170]。若法院認定一方需要採取積極行動來保護營業秘密，則可以透過頒布禁制令之方式來處理[171]。在極端的情況下，如果核頒布禁制令並不公平，法院可以制定一個禁制令，對於未來的營業祕密使用附加支付合理權利金的條件[172]。支付權利金的期間，不可以較本來可能禁止使用營業秘密之期間為長[173]。

法院也可就營業秘密之不當取用授予一方當事人補償性損害賠償[174]。DTSA 提供兩種不同計算損害的方式[175]，一種是實際的損失加上不屬於實際損害的不當得利；另一種則是相當於使用不當取用之營業秘密之合理權利金[176]。

若法院認為營業秘密是故意及惡意被不當取用的，則可以授予懲罰性損害賠償[177]。懲罰性損害賠償本質上是懲罰性的，並不直接與實際損害聯結，但是懲罰性損害賠償不能超過補償性損害賠償的 2 倍[178]。此外，若一方的營業秘密是故意及惡意被不當取用，額外的律師費也是可以獲得的[179]。

---

[170]See 18 U.S.C. § 1836(b)(3)(A)(i)(I).
[171]See 18 U.S.C. § 1836(b)(3)(A)(ii).
[172]See 18 U.S.C. § 1836(b)(3)(A)(iii).
[173]*Id*；Mackrides, *supra* note 29, at 77.
[174]See 18 U.S.C. § 1836(b)(3)(B).
[175]*Id.*
[176]See 18 U.S.C. § 1836(b)(3)(B)(i)-(ii)；Mackrides, *supra* note 29, at 77.
[177]See 18 U.S.C. § 1836(b)(3)(C).
[178]*Id.*
[179]See 18 U.S.C. § 1836(b)(3)(D)；Mackrides, *supra* note 29, at 77-78.

最後，在法院認為有惡意提出營業祕密不當取用損害賠償主張或撤銷禁制令請求之狀況下，DTSA 也准許法院授予律師費給獲勝的一方[180]。

(5).實施狀況

根據學者研究，在 DTSA 施行後第一年的 2016 年 5 月 11 號到 2017 年之間之 486 件依據 DTSA 提出之訴訟中，百分之 29 的案件來自科技及企業重鎮城市諸如芝加哥(Chicago)、舊金山(San Francisco)、矽谷(Silicon Valley)、洛杉磯(Los Angeles)、紐約(New York City)，卻良好的分散在各聯邦地方法院(有百分之 74 的聯邦地方法院[181]至少有一件以上的 DTSA 案件)[182]。

學者也將此情況與 2016 年的專利案件研究做了有趣的比較，發現專利訴訟集中在兩個聯邦地方法院，德克薩斯東區聯邦地方法院及德拉瓦聯邦地方法院，而這兩間法院卻只處理了百分之 3 的 DTSA 案件[183]。該研究並發現，DTSA 擴張了原告在聯邦法院提出訴訟的機會[184]。

幾乎所有具有 DTSA 訴訟主張的案件也都有主張一個以上的州法

[180] *Id*；Mackrides, *supra* note 29, at 78.
[181] 美國共有 94 個聯邦地方法院，其中有 89 個在 50 個州內，另外 5 個則是在哥倫比亞特區、波多黎各、關島、美屬維京群島、北馬里亞納群島。See United State Courts website, https://www.uscourts.gov/faqs-court-information（last visited：10/31/2023）.
[182] Miller, *supra* note 32, at 235.
[183] *Id.*
[184] Miller, *supra* note 32, at 235-236. (聯邦法院對於百分之 26 的案件並無 DTSA 之外的管轄權)

請求權，最常見的州法上訴訟主張即為營業秘密的不當取用[185]。值得注意的是，契約相關的訴訟主張經常伴隨 DTSA 之訴訟主張，從這些契約相關訴訟主張出現的頻率可以得知，營業秘密不當取用通常發生在內部人或是分享協議之脈絡下，可能是在兩個公司之間或是雇主與員工間[186]。

有爭議的營業祕密種類證實了此種內部人的脈絡。原告主張顧客及商業資訊(像是行銷、財務、顧客名單)的不當取用頻率遠大於秘密配方或是軟體演算法[187]。雖然有百分之 40 之原告聲稱「技術資訊」受到不當取用，惟根據研究數據顯示，在法院爭議當中的美國「創新」案件其實數量很少[188]。事實上，研究結果確認，歷史上營業秘密訴訟之趨勢走向並無因 DTSA 施行之後而有所改變[189]。

在全部的 DTSA 爭議案件當中，大約有 3 分之 2 涉及營業秘密擁有者之現任或前任員工，有百分之 26 則牽涉現在或以前的商業合作夥伴，而僅有百分之 10 的案件是沒有前開關係之當事人[190]。事實上，百分之 72 的 DTSA 訴訟案件主張被告應該受到保密協議(None Disclosure Agreement，簡稱 NDA)的拘束，NDA 通常被使用來創建對

[185]Miller, *supra* note 32, at 236. (百分之 84 的案件都有提出州法上營業秘密不當取用之訴訟主張)
[186]*Id.*(DTSA 案件附帶州法契約相關訴訟主張比例：違反合約占 70%，違反忠實義務占 40%、不當得利占 22%、違反善意原則占 10%)
[187]*Id.*(顧客名單及商業資訊占 58%、軟體占 22%、配方占 8%)
[188]*Id.*
[189]*Id.*
[190]*Id.*

於機密資訊保護的契約上義務[191]。

只有百分之 9 的案件與網路間諜(cyber espionage)有關[192]，主張受到外國實體不當取用營業秘密的比例則是更低的百分之 6[193]。雖然美國國會是在「美國企業歷史上最大財富移轉至外國實體」之背景下通過 DTSA，顯然 DTSA 並未被用於打擊網路間諜及外國經濟間諜之用途[194]。

(6). 批評

A. 並未被用於遏止網路間諜

儘管 DTSA 的立法在國會受到兩黨的，以及來自智慧財產權法專業團體如美國律師協會智慧財產權部門(Intellectual Property Law Section of American Bar Association)及美國智慧財產權協會(American Intellectual Property Law Association)之支持，DTSA 在學術界卻受到正反不一的評價[195]。

從 DTSA 立法的歷程可以得知，國會的意圖是讓 DTSA 來對抗外國

---

[191] *Id.*

[192] Miller, *supra* note 32, at 237.(絕大部分的 DTSA 營業祕密不當取用案件並未提及網路間諜，大部分的網路間諜案件事發生在美國國內，僅有 4 件案件牽涉到外國網路間諜)

[193] *Id.*(外國被告分別來自；中國 7 名、加拿大 5 名、新加坡 3 名、法國、義大利、台灣各 2 名、哥倫比亞、開曼群島、德國、日本、約旦、模里西斯、瑞典、英國、俄羅斯各 1 名)

[194] *Id.*

[195] Miller, *supra* note 32, at 230.

對手的網路間諜活動，但是論者認為 DTSA 並未解決此一問題[196]。有大量證據證明此種觀點，就是營業秘密法並不適合，或是被誤用來阻止或懲罰網路間諜，根據一項 2010 年的研究，百分之 93 之州法營業秘密案件，牽涉到員工或是商業夥伴之內部人，而在聯邦法上營業秘密案件部分，牽涉到內部人的統計數據則是百分之 85[197]。而在另一項關於 EEA 之研究當中，也得出相同的結果，在 EEA 施行後的 1996 到 2012 年間，在 124 件被起訴的案件當中，超過百分之 90 之案件的被告為員工或是商業夥伴之內部人，儘管在網路竊盜日益增加的情況下，大多數的營業秘密訴訟仍然是牽涉到在公司內部處於可以接觸機密訊息的員工[198]。

在此種情況下，增加營業秘密的保護，只會增加雇主對於員工的影響力，有利於限制員工流動性及減少市場競爭的政策，而對於網路不當使用卻沒有太大幫助[199]。

B. 並未優先於州法適用

DTSA 也被認為，並未提供本來促使 DTSA 通過之法律統一性立法目的，因為 DTSA 並無優先於州法適用[200]。批評者指出，缺乏優先權原

[196] Miller, *supra* note 32, at 231.
[197] *Id.*
[198] *Id.*
[199] *Id.*
[200] Mackrides, *supra* note 29, at 86-87.

則將會導致在不同的州產生不一致的結果[201]。

DTSA若無優先於州法適用，則DTSA並無法產生統一法律的功能，僅僅是在原本混亂的州法上，再加上另一層的保護[202]。儘管國會認為在州法上微小的差異有時候被證明是有決定性的作用，但是國為僅是給營業秘密的擁有者更多的訴訟選擇權，同時也帶給被告潛在的不確定性，因為被告並不能決定會面對州法或是聯邦法的追訴[203]。DTSA鼓勵選擇法院(forum shopping)[204]，並將訴訟權力的天平朝向原告傾斜，多一層的變數，使潛在被告更難理解其責任範圍，而增加的複雜性，也會使訴訟成本提高，論者認為將有害於美國之經濟成長及創新[205]。

C.可能招致「營業秘密侏儒」

評論者亦預測DTSA會造成「營業秘密侏儒」(trade secret troll)的崛起，此處之「侏儒」是指「發起訴訟的目的僅是為了從害怕的被告處獲得和解金或是大額損害賠償」之原告，這個說法是從知名的「專利侏儒」(patent troll)而來[206]。營業秘密侏儒可能會妨害創新及就

[201]Mackrides, *supra* note 29, at 87.
[202]Miller, *supra* note 32, at 232.
[203]*Id.*
[204]選擇法院是指在主張一個權利時，在多個有管轄權之法院中，選擇對其最有利的法院為之，選擇法院可以發生在不同的州的法院間，也可以發生在相同的州的聯邦法院和州法間，或是在不同國家的法院間。目前選擇法院在某些特定情況下雖是受允許的，但是根據伊利原則其他法律衝突原則，在現代法律系統並不鼓勵此種行為。See Cornell Law School website, https://www.law.cornell.edu/wex/forum_shopping（last visited：11/12/2023）.
[205]Miller, *supra* note 32, at 232-233.
[206]Miller, *supra* note 32, at 233.

業成長，別是因為獲取營業秘密權利地位以及發起營業秘密訴訟較在專利領域從事相似活動成本更低，且會牽涉包含競業禁止條款(covenants not to compete)、保密協議、勞動力流動等之其他訴訟主張[207]。除此之外，DTSA 還給與潛在的營業祕密侏儒在判決前扣押被告財產之特殊權力，而不成比例的將權力移轉到原告一方，而可能對那些被誤指為不當取用營業秘密的企業，包括新創企業，造成不必要的傷害[208]。

D. 單方扣押條款並不適當

單方扣押條款讓法院可以在特殊情況下，未經通知即可扣押被告之財產，以防止營業秘密被揭露或使用[209]。國會傾向防止資訊被揭露，並希望單方扣押條款可以對達成此目的有所貢獻[210]。論者認為單方扣押條款是一種允許擁有大量資源的大公司合法對抗經濟能力較弱之競爭對手如(通常是前員工)之武器[211]。藉由單方扣押條款來扣押被告之財產，國會等於是允許法院在缺乏正當法律程序的情況下扣押財產[212]。

論者認為單方扣押條款行不通之原因有 2 個。第一，法官習慣於

[207] *Id.*
[208] *Id.*
[209] See 18 U.S.C. § 1836(b)(2)(A)(i).
[210] Miller, *supra* note 32, at 234.
[211] *Id.*
[212] *Id.*

聽取雙方的論點，如果缺少反對方的一方，法官易於聽取原告之主張而未盡職調查相關的事實及法律[213]。第二，大部分的營業秘密案件牽涉到下列爭議：(1)牽涉爭議的資訊是否符合營業秘密的構成要件?(2)原告是否擁有營業秘密之相關權利；要確定這些爭議的答案，需要訴訟雙方參與表達意見，在只有一方參與的情況下不可能發生[214]。

(五)、2022 年保護美國智慧財產法(Protecting American Intellectual Property Act of 2022, 簡稱PAIP)

1.立法背景

由於現行法制之成效與原先預期仍有落差，而在外交、貿易協議手段亦無法有效處理跨國營業秘密竊取之情勢下，美國參議院與眾議院分別於 2022 年 12 月 20、22 日通過 PAIP[215]，而美國總統於 2023 年 1 月 5 日簽署該法案，期待利用不用經過司法程序之經濟制裁，迅速有效嚇阻外國法人與自然人竊取美國營業秘密[216]。

2.法規主要內容

PAIP 授權美國政府對於涉及營業秘密重大竊盜之外國人及外國

[213]Mackrides, *supra* note 29, at 87.
[214]Mackrides, supra note 29, at 88.
[215]Protecting American Intellectual Property Act of 2022, P. L. 336 (January 5, 2023).
[216]吳彬詣（2023），〈美國《2022 保護美國智慧財產權法》之簡析與我國國家核心關鍵技術營業秘密之借鏡〉，《科技法律透析》， 35 卷 8 期，頁 58.

實體實施制裁，重點包括：

(1)確定對象：要求美國總統每年向國會提出報告，列出符合「故意竊取美國營業秘密，且其行為很可能或已經對美國國家安全、外交、經濟、金融構成重大威脅者」及「對前開故意竊取美國營業秘密之行為提供重要的財務、物質、技術、商品、服務等支援，或從中獲得利益者」條件之外國人、外國實體名稱及外國實體的執行長或董事會成員。

(2)實施制裁：針對外國實體，PAIP 授權美國政府可以實施之制裁手段，包含凍結資產、將實體列入美國商務部之出口管制名單、禁止美國金融機構提供實體貸款、拒絕向實體採購、禁止實體之外匯交易、禁止美國人投資實體之股票或債券、限制實體成員入境、驅逐實體成員出境等；針對外國人，制裁手段包含凍結資產、拒絕入境、撤銷簽證等。

(3)豁免：美國總統若認為符合美國利益，可以豁免外國人或外國實體，但須於 15 日內向國會提交豁免之理由[217]。

3. 相關評論

部分實務界人士對於 PAIP 持正面之看法，認為 PAIP 在本來之

[217]財團法人資訊工業策進會科技法律研究所網站，https://stli.iii.org.tw/article-detail.aspx?no=64&tp=1&d=8933 (最後瀏覽日：05/4/2024)。

EEA 與 DTSA 之外，提供一個聯邦法層級之執法利器。主要原因在於 PAIP 可以避免營業秘密所有人在司法程序救濟上所遇到之諸多障礙諸如管轄權、舉證責任、外國被告之執行等問題，由美國政府在確定對象後，直接實施經濟制裁，以阻止侵害營業秘密之行為[218]。

然而，PAIP 也受到許多批評，包括(1)制裁門檻過低：美國總統僅需向國會提出報告即可實施制裁，並不需提供證據；(2)要件定義模糊：PAIP 條文當中使用許多不確定之法律概念[219]，但是在 PAIP 條文中並未定義這些不確定法律概念，外加 PAIP 式授權行政機關自行認定行為人並實施制裁，並未經過司法機關嚴謹之調查程序，恐淪為美國政府之政治工具；(3)牴觸司法程序：PAIP 條文中並未處理與司法判決牴觸時之處理辦法，所以有可能與法院之判決產生矛盾，若法院認定並無營業秘密竊取行為，是否可以因此撤銷根據 PAIP 所實施之制裁，容有疑義；(4)並無救濟程序：由於 PAIP 授權美國總統可以直接認定竊取營業秘密之行為人，毋庸提供證據及經過司法審判程序，PAIP 也無任何救濟途徑，效果如同法院之確定判決，恐有違反美國憲法第五修正案[220]之虞[221]。

事實上，根據 PAIP 本身之規定，美國總統應於 PAIP 通過後之 6

[218]吳彬詣，前揭註 216，頁 63。
[219]舉例來說，「重大竊取行為」、「實質上」對於美國國家安全造成「重大威脅」。
[220]任何人不經正當法律程序，不得被剝奪生命、自由或財產。
[221]吳彬詣，前揭註 216，頁 63-65。

個月內，就必須向國會提出前開報告，但是在 2023 年 7 月 4 日截止時間前，美國總統並未根據 PAIP 之規定向國會提出報告，其未來會帶來如何之影響，仍有待後續觀察[222]。

二、美國外國投資審查法制發展

本次我國新修正之國安法加入「國家核心關鍵技術」[223]之概念，欲保護的客體則是「國家核心關鍵技術之營業秘密」，需同時分別符合國家核心關鍵技術、營業秘密之構成要件，方會落入範圍內。惟美國並非採取此種國家核心關鍵技術結合營業秘密保護之立法方式，而是以營業秘密法以外之法規來保護國家關鍵技術，則美國在針對其國家關鍵技術之法制保護上之最新發展，就值得我國未來對於我國「國家核心關鍵技術」之保護以及相關立法做為參考。本研究以下將依序針對美國對於外國投資審查、出口管制相關體制、規範及其最新發展作介紹。

(一)、2018 年外國投資風險審查現代化法案介紹

外國投資自美國建國以來一直是美國經濟成長的核心，但是有時

[222]See Kenneth J. Nunnenkamp, Shaobin Zhu, Eli Rymland-Kelly(2023), *AN INITIAL LOOK AT PAIPA'S SCOPE AND LEGAL RISKS,* in https://www.morganlewis.com/pubs/2023/08/an-initial-look-at-paipas-scope-and-legal-risks(last visited：5/12/2024).

[223]國安法第 3 條第 3 項規定，國家核心關鍵技術係指「如流入外國、大陸地區、香港、澳門或境外敵對勢力，將重大損害國家安全、產業競爭力或經濟發展，且符合下列條件之一者，並經行政院公告生效後，送立法院備查: 一、基於國際公約、國防之需要或國家關鍵基礎設施安全防護考量，應進行管制。二、可促使我國產生領導型技術或大幅提升重要產業競爭力。」

候外國資本尋求的不僅僅是經濟上的回報，美國政府 40 年來均依靠美國外資投資委員會(Committee on Foreign Investment in the United States，簡稱 CFIUS)[224]處理涉及外國投資者交易所引起之國家安全議題[225]。CFIUS 是一個由 11 個不同的政府單位[226]所組成的委員會，透過美國情報機構的幫助，審查外國對各種商業及資產的投資[227]。

鼓勵外國投資的開放市場，同時維護國家安全，一直是 CFIUS 的主要目標[228]。自從創建以來，CFIUS 已經經歷了許多困境，但是最嚴峻的挑戰，則是在過去這幾年所發生[229]。為了面對這些挑戰，美國國會於 2018 年制定了「2018 年外國投資風險審查現代化法案」(Foreign Investment Risk Review Modernization Act of 2018，簡稱 FIRRMA)[230]，FIRRMA 代表了迄今為止對 CFIUS 現代化的最重大的努力[231]。

[224]美國外資投資委員會是一個跨部門的委員會，負責審查特定的外國在美國之投資交易或不動產交易，以決定這些交易對於美國國家安全之影響。See U.S. Department of the Treasury website, https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius (last visited：11/16/2023).

[225]Heath P.Tarbert,*Modernizing CFIUS*, 88 GEO. WASH. L. REV. 1477(2020), at 1478.

[226]包括財政部長、國土安全部長、國防部長、商務部長、國務卿、司法部長、能源部長、勞工部長、國家情報局長，以及總統認為適當的其他執行部門、機構或辦公室之負責人。See 50 U.S.C. § 4565.

[227]Tarbert, *supra* note 225, at 1478-1479.

[228]Tarbert, *supra* note 225, at 1479.

[229]*Id.*

[230]Foreign Investment Risk Review Modernization Act of 2018, P. L. 115-232 (August 13, 2018), § 1701 - 1728, 132 Stat. 1636, 2174 - 2207.

[231]Tarbert, *supra* note 225, at 1479.

1.立法背景

在 2008 年全球金融危機後的 10 年間，CFIUS 的案件量大增，同時間傳統的私部門併購開始轉變為各種新型的外國投資，並且以主權導向極複雜的基金結構為特色。有些交易顯示出 CFIUS 在管轄權的部分有嚴重的缺口。隨著 2010 年在科技及數據的使用上有重大的進展，CFIUS 實質的調查內容也開始改變。最後，美國面臨中國的軍事、經濟崛起，中國並宣布了新的「中國製造 2025」[232]計畫，要在其認為有戰略性的各種產業在世界上居於領先地位。這些挑戰為了現代化 CFIUS 的修法提供了需要的推進力[233]。

(1).案件量增加

在 2010 年代，CFIUS 面臨最明顯的挑戰是逐漸增加的案件量。從數據上來看，從 2009、2010 年的不到 100 件案件，到 2017 的 240 件，同時間 CFIUS 的人力卻維持大致相同。除了案件量增加之外，案件本身也遠比之前來的複雜[234]。

---

[232]此計畫為 2015 年中國實施製造強國戰略第一個 10 年的行動綱領。這是「製造強國」戰略的第一步，2025 年中國製造業希望能邁入製造強國行列，2045 年可望進入第一方陣（與美國並列），成為全球具有引領影響力的製造強國。中國製造 2025 的編制發佈與推展，對於中國來說，這是第 1 次從國家戰略層面描述建設製造強國的宏偉藍圖。它以 30 年爲期的長遠前瞻性戰略部署，期許在 2045 年中國建國百年之前，晉升爲與美國並駕其驅的兩大製造強國。見國家發展委員會網站，https://www.ndc.gov.tw/News_Content.aspx?n=2FE923B6D5878FBA&sms=72B16E02BCB79287&s=0AD7EE4AA7F6B300(最後瀏覽日：03/3/2024)。

[233]Tarbert, *supra* note 225, at 1492-1493.

[234]Tarbert, *supra* note 225, at 1493.

要判斷案件複雜程度可以從案件是否需要進入為期 45 天的調查程序得知。在 2007 年只有大約百分之 4 的案件需要進入調查階段，在 2017 年，有大約百分之 70 的案件需要進入調查階段；另一個案件複雜性的指標則是看有多少案件需要 CFIUS 採取相關減輕或禁止措施來保護國家全。減輕措施通常要求雙方協議出最終可被 CFIUS 接受的方法，來完成投資交易。交易的某些方面也可能被禁止，比如說目標美國企業必須要將某種敏感產品線或是子公司出售，才能完成外國人的投資程序。這類案件在 2008 到 2015 年間低於百分之 10，2017 年則是達到百分之 20 上下，而這些案件都需要更多的人力資源來審查[235]。

(2).新型態投資趨勢

與此同時，CFIUS 所面臨的交易複雜性也受到新型態投資趨勢的影響。在 2010 年代，可以看到外國主權國家，尤其是中國，尋求在美國投資以實現其國家目標，不同與原先主要投資的原因僅是財務或是商業上的考量，使 CFIUS 傳統上的分析工作更加辛苦。除此之外，對於美國企業的控股投資，並非由其他公司所進行，而是由多層的私

[235]Tarbert, *supra* note 225, at 1493-1494.

募股權基金(private equity)[236]、風險投資基金(venture capital)[237]以及其他種類的投資基金所進行。由於這些基金有時候擁有數百個持股比例及投票權不同之有限合夥人，對於 CFIUS 來說，更難分辨最終誰會控制美國的目標公司[238]。

(3).軍事與商業應用

國家安全與商業活動間之關係持續演進，也增加了這些交易的複雜性。軍民兩用貨品的議題一向以來都是一個議題。從前，國防工業的創新推動了商業創新，像是噴射機、網際網路及全球定位系統。然而隨著 2010 年代的展開，軍事能力也迅速地在商業創新上發展。無人機、自動駕駛車輛及先進半導體將會成為未來軍事應用之基礎科技，即使在當時它們還不是[239]。

此外，不斷增長的數位化、數據驅動的經濟創造了前所未見的國家安全漏洞，不論是社交網路、醫療保險或是金融，大量美國公民的個人可識別資訊，都被儲存在這些被外國投資者收購的美國公司當中。

---

[236]私募股權指的是購買和管理公司後再出售的投資夥伴關係。私募股權公司代表機構投資者和合格投資者經營這些投資基金。See Investopedia website, https://www.investopedia.com/terms/p/privateequity.asp (last visited：11/19/2023).

[237]風險投資是私募股權的一種形式，也是投資者向被認為具有長期增長潛力的新創公司和小型企業提供的一種融資方式。風險投資通常來自富有的投資者、投資銀行和其他金融機構。風險投資不總是指金錢，實際上，它通常表現為技術或管理專業知識。風險投資通常分配給具有卓越增長潛力的小公司，或者那些增長迅速並且看似準備繼續擴張的公司。See Investopedia website, https://www.investopedia.com/terms/v/venturecapital.asp (last visited：11/19/2023).

[238]Tarbert, *supra* note 225, at 1494-1495.

[239]Tarbert, *supra* note 225, at 1495.

到了 2010 年代末期，收購一家矽谷(Silicon Valley)的新創公司，有時候所引起的國家安全疑慮就跟 CFIUS 傳統聚焦的國防、航太領域一樣嚴重[240]。

(4). 管轄權範圍過於狹隘

隨著案件量快速的變化，CFIUS 的管轄權也跟著變的僵化，其管轄權的規定已經有 30 年的歷史，跟據原先的規定，CFIUS 僅對於外國投資控制美國公司的合併及收購有審查權限，這個狀況在 1980 年到 2010 年代前是合理的，但是到了 2010 年代，非控制性投資[241]跟合資企業[242]變得更加普及，當中有許多交易都不完全符合 CFIUS 的管轄權範圍。儘管 CFIUS 注意到這些交易可能對國家安全帶來相同的危害，但是卻沒有管轄權來審查這些交易。當越來越多的外來威脅意圖利用這些漏洞，這些漏洞變得越來越危險[243]。

除了投資環境變化外，CFIUS 也面臨一些本來就不該存在的法規漏洞。舉例來說，在靠近敏感軍事設施的地點購買美國企業是需要受到 CFIUS 審查的，但是在相同的地點購買不動產卻不需要受到審查，

---

[240] Tarbert, *supra* note 225, at 1495-1496.

[241] 非控制性股權，也被稱為少數股權，是指一個股東擁有不到 50%的流通股份，並且對決策沒有控制權。See Investopedia website, https://www.investopedia.com/terms/n/noncontrolling_interest.asp(last visited：11/21/2023).

[242] 合資是一種商業上的安排，指兩個或兩個以上的主體同意集合其資源，以完成特定的任務。這個任務可以是一個新的項目或是任何其他商業活動。See Investopedia website, https://www.investopedia.com/terms/j/jointventure.asp(last visited：11/21/2023).

[243] Tarbert, *supra* note 225, at 1496.

這些漏洞將容易被利用，並且在具有相同國家安全威脅的交易當中，造成不同結果的可能性[244]。

(5).「中國製造 2025」

當前述的諸多原因在 2010 年代挑戰 CFIUS，當中貫穿上述原因的主題是：中國的崛起。在 2000 年代的大部分時間當中，中國成長快速，但是至少表面上宣稱參加全球自由企業體系，並且進行各種民主改革。但是在 2008 年金融危機之後，習近平主席上台，決定改革許多前 10 年的中國政策，在他的領導之下，中國政府集中政治權力來追求大膽的國家目標，其中部分目標據稱是為了實現取代西方價值的替代方案[245]。

在 2015 年，習近平主席宣布「中國製造 2025」計畫，目標為在 10 年內使中國成為 10 個高科技領域的主導者。為了實現這個目標，中國政府進行了具有野心的產業政策，利用數十年來貿易逆差所賺取的數千億美元，用於資助補貼、智慧財產權採購、國有企業、在美國、日本、歐洲、韓國收購尖端科技公司。次年，美中經濟暨安全審查委員會(U.S.-China Economic and Security Review Commission，簡稱 USCC)[246]督促國會，分析中國政府所主導的諸如「中國製造 2025」

[244]Tarbert, *supra* note 225, at 1497.
[245]*Id.*
[246]美中經濟與安全審查委員會於 2000 年 10 月經由美國國會所創立，其法定職責是針對美國與中

支計畫，對於美國經濟競爭力、國家安全的影響，並研究國會可以採取的措施，以加強美國高科技、高附加價值產業諸如人工智慧、自動駕駛汽車及系統及半導體[247]。

在 2016 年的美國總統大選，兩大政黨的提名人都將中國的貿易及投資政策納入他們擬定的白宮優先計畫事項當中，前國務卿 Hillary Clinton 承諾會實施有針對性的關稅以及加強美國監督貿易的系統。而後來贏得 2016 年美國總統大選的 Donald Trump 更直接，指控中國玩弄貿易系統，並警告中國其操縱貨幣及作弊的日子將會結束。CFIUS 全面翻修的場景因此產生[248]。

2. 重要內容介紹

FIRRMA 是對於 CFIUS 審查權限及管轄權最近期且最具革命性的擴張，該法案於 2018 年 8 月 1 日經參議院通過，並於同月 13 日經總統 Donald Trump 簽署生效，成為 10 多年來對於 CFIUS 運作的首次重大改革，並且開啟監管外國投資美國經濟的新時代[249]。

國雙邊貿易和經濟關係的國家安全影響監控、調查，並向美國國會提交有關的年度報告，並在適當的情況下向國會提供立法和行政行動的建議。See U.S.-China Economic and Security Review Commission website, https://www.uscc.gov/about-us(last visited：11/24/2023).

[247]Tarbert, *supra* note 225, at 1498.

[248]Tarbert, *supra* note 225, at 1498-1499.

[249]J. Russell Blakey, *The Foreign Investment Risk Review Modernization Act: The Double-Edged Sword of U.S. Foreign Investment Regulations*, 53 Loy. L.A. L. Rev. 981 (2020), at 999.

(1). 大幅擴張 CFIUS 的管轄範圍

在 FIRRMA 生效前，CFIUS 對於外國投資的審查權限取決於買方在完成交易後對於實體的控制程度，如果投資導致了投資者對於美國實體或是企業獲得足夠的控制權，CFIUS 便可以審查該交易，否則的話，CFIUS 便無從介入相關的合併或收購。然而，在 FIRRMA 生效後，遊戲規則有了相當大的改變，擴張了 CFIUS 監管審查權的範圍，來涵蓋控制性及非控制性的投資[250]。

FIRRMA 第 1703 條(a)(4)(B)(i)[251]和第 1703 條(a)(4)(B)(ii)[252]部分所涵蓋的大部分交易與 FIRRMA 前之 CFIUS 管轄權範圍保持一致，但較有爭議之處則是在第 1703 條(a)(4)(B)(iii)[253]部分。透過 FIRRMA 第 1703 條(a)(4)(B)(iii)之規定，FIRRMA 擴張了 CFIUS 的管轄權，讓 CFIUS 可以審查所有的交易，不論是控制性或非控制性交易，只要該交易涉及「關鍵基礎設施」(critical infrastructure)、「關鍵技術」(critical technologies)以及美國公民的「敏感個人資料」(sensitive personal data)[254]。

乍看之下，這個變動對於 CFIUS 之審查範圍影響似乎無關緊要，

[250] *Id.*
[251] See The Foreign Investment Risk Review Modernization Act of 2018, § 1703(a)(4)(B)(i).
[252] See The Foreign Investment Risk Review Modernization Act of 2018, § 1703(a)(4)(B)(ii).
[253] See The Foreign Investment Risk Review Modernization Act of 2018, § 1703(a)(4)(B)(iii).
[254] Blakey, *supra* note 249, at 1001.

但對於 CFIUS 權限的修改讓很多人好奇這些術語的含義以及它們將如何影響 CFIUS 的審查能力，為了要理解圍繞在 CFIUS 新建立的審查範圍的廣泛模糊性，必須先了解 FIRRMA 如何定義「關鍵基礎設施」、「關鍵技術」以及美國公民的「敏感個人資料」[255]。

A. 關鍵基礎設施

根據 FIRRMA 的定義，「關鍵基礎設施」是指一切「不論實體或虛擬，若其無法運作或毀滅將對國家安全有衰弱影響之系統和資產。」[256]雖然以上描述根據其解釋可以囊括幾乎所有事物，惟其用語跟 FIRRMA 生效前之規範[257]及國土安全部用來描述美國經濟的 16 個關鍵基礎設施部門[258]用語相同。因此，此部分根據 FIRRMA 進行之審查可能與先前的規定差異不大。然而，以下兩個類別，「關鍵技術」和「敏感個人資料」，將被證明更加難以掌握，並可能擴大 CFIUS 的管轄權，超越所有先前的理解[259]。

---

[255] *Id.*
[256] See Foreign Investment Risk Review Modernization Act of 2018 § 1703(a)(5).
[257] 2007 年外國投資和國家安全法(The Foreign Investment and National Security Act of 2007)。
[258] 16 個關鍵基礎設施部門分別為化工、商業設施、通訊、關鍵製造、水壩、國防產業基地、緊急服務、能源、金融服務、食品農業、政府設施、醫療暨公共衛生、資訊科技、核反應與材料及廢料、運輸、水及廢水等部門。See Cybersecurity & Infrastructure Security Agency website, https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors(last visited：12/2/2023).
[259] Blakey, *supra* note 249, at 1002.

B. 關鍵技術

在通過 FIRRMA 之後，留給 CFIUS 審查的第 2 個主要類別是「關鍵技術」。FIRRMA 對「關鍵技術」主要規定在該法案第 1703 條[260]，而當中這裡的關鍵變化是在第第 1703 條(a)(6)(A)(vi)中加入了「根據 2018 年『出口管制改革法案』[261](Export Control Reform Act of 2018，簡稱 ECRA)第 1758 條所控制的新興和基礎技術」。ECRA 和 FIRRMA 都包含在一個更大的法律架構當中，即 2019 財政年度約翰 S·麥凱恩國防授權法案[262](John S. McCain National Defense Authorization Act for Fiscal Year 2019，簡稱 NDAA)。在 NDAA 第 1758 條中規定，ECRA 授權美國商務部針對新興及基礎技術(emerging and foundation technology)之出口、再出口及國內移轉建立適當的控制措施[263]。除了辨識出新興及基礎技術外，ECRA 同時要求在審議過程中也要考慮「外國新興及基礎技術之發展情況」、「出口管制對於新興及基礎科技在美國發展之可能影響」、「出口管制對限制外國發展新興和基礎科技擴散的效果」等因素[264]。

[260]See Foreign Investment Risk Review Modernization Act of 2018 § 1703(a)(6)(A).
[261]Export Control Reform Act of 2018, P.L. 115-232 (August 13, 2018), § 1741 – 1768, 132 Stat. 1636, 2208 – 2234, codified at 50 U.S.C. §4801 et seq.
[262]John S. McCain National Defense Authorization Act for Fiscal Year 2019, P. L. 115-232, 132 Stat. 1636 (2018).
[263]Blakey, *supra* note 249, at 1003.
[264]Blakey, *supra* note 249, at 1003-1004.

儘管如此，前述關於新興及基礎技術的描述，對於要了解到底何為「關鍵技術」的確切內涵時，並無任何實質的幫助。直到 2018 年 11 月 19 日，工業和安全局[265](Bureau of Industry and Security，簡稱 BIS)，在聯邦公報[266](Federal Register)上發布了一份建議規則的提前通知書（advance notice of proposed rulemaking，簡稱 NOVEMBER ANPRM），提供了一份建議的「代表性技術分類清單」[267]，這些分類將落入 CFIUS「關鍵技術」之範疇中[268]。

在發佈了 NOVEMBEE ANPRM 後，「關鍵技術」，從曾經是一個不明確且理論性的概念，變成了一個全面定義的清單，包含了一些最尖

[265]工業和安全局透過確保有效的出口控制和條約遵循系統及促進美國在戰略科技方面的持續領導地位，來增進美國的國家安全、外交政策和經濟目標。See U.S. Department of Commerce website, https://www.commerce.gov/bureaus-and-offices/bis(last visited：12/08/2023).

[266]由聯邦公報辦公室和國家檔案暨記錄管理局出版，聯邦公報是聯邦機構和組織的規則、研擬中規則、通告、行政規則、其他總統文件之官方每日刊物。See GovInfo website, https://www.govinfo.gov/app/collection/FR/(last visited：12/08/2023).

[267]這些分類包括：1.生物技術，例如：奈米生物學、合成生物學、基因體和基因工程學、神經技術。2.人工智慧(Artificial Intelligence, AI)及機器學習技術，例如：神經網絡和深度學習（例如腦模擬、時間序列預測、分類）、演化和基因計算（例如基因演算法、基因工程）、強化學習、電腦視覺（例如物體識別、圖像理解）、語言和聲音處理（例如，語音識別和生成）、專家系統（例如決策支援系統、教學系統）、語言和音頻處理（例如語言識別和產生）、自然語言處理（例如機器翻譯）、計劃（例如排程、遊戲運算）、聲音和視覺操縱技術（例如聲音複製、深度偽造）、人工智慧雲技術、人工智慧晶片組。3. 定位、導航和定時(Position, Navigation and Timing, PNT)技術。4. 微處理器技術，例如：單晶片系統（systems on chip, SoC）、晶片堆疊記憶體。5.先進計算技術，例如：記憶體內計算技術。6.數據分析技術，例如：視覺化、自動分析演算法、情境感知計算。7.量子資訊技術，例如：量子計算、量子加密、量子感測。8.物流技術，例如：移動電力、建模與仿真、資產可視性、配送物流系統。9.積層製造，例如 3D 列印。10.機器人技術，例如：微型無人機和微型機器人系統、群體技術、自動組裝機器人、分子機器人、機器人編譯器、智慧塵埃。11.人機介面，例如：神經控制介面、心靈機器介面、直接神經介面、腦機介面。12.高超音速技術，例如：飛行控制演算法、推進技術、熱防護系統、特別材料(用於結構、感測器等)。13.先進材料，例如：適應性迷彩、功能性紡織品（先進纖維和織物技術）、生物材料。14.先進監視技術，例如：人臉辨識及聲紋辨識技術。See Federal Register website, https://www.federalregister.gov/documents/2018/11/19/2018-25221/review-of-controls-for-certain-emerging-technologies (lasted visited：12/11/2023).

[268]Blakey, *supra* note 249, at 1004.

端的科技投資機會。然而，NOVEMBEE ANPRM 注意到這個清單對外國投資可能產生的寒蟬效應，其指出對 NOVEMBEE ANPRM 的回應將有助於商務部和其他機構識別和評估新興技術，在不損害國家安全及不妨礙美國商業部門跟上新興領域之國際進展能力前提下，來更新出口管制清單[269]。

C. 敏感個人資料

FIRRMA 新增的第 3 個，也是最模糊的類別則是關於美國人民的「敏感個人資料」[270]。不同於對 CFIUS 審查範圍的其他修正，「敏感個人資料」及類似的詞彙在此之前從未被 CFIUS 相關規範引用過，基本上對外國投資者而言，此術語相當陌生。這一條文是在眾議院在立法過程中後期所要求加入的，因此對於何謂「敏感個人資料」並未提供正式的定義[271]。

作為向投資人提供其可能含義的入門資料，財政部提供了以下描述：「CFIUS 可能審查與保有或收集可能以威脅國家安全之方式被利用之美國公民之敏感個人資料之美國企業相關的交易。『敏感個人資料』的定義包括由美國企業維護或收集的 10 類數據，這些企業（i）的目標客群是敏感人士，或產品及服務係針對敏感人士，包括美國軍

[269] *Id.*
[270] See Foreign Investment Risk Review Modernization Act of 2018 § 1703(a)(4)(B)(iii)(III).
[271] Blakey, *supra* note 249, at 1010.

人或與國家安全有關的聯邦機構員工，（ii）收集或保有至少 100 萬個個人的資料，或（iii）具有被證明的業務目標，即保有或收集至少 100 萬個個人的數據，並且將其作為美國企業主要產品或服務的一部分。資料的類別包括金融、地理位置和健康等方面的資料。基因資訊也包括在內，無論是否符合（i）、（ii）或（iii）」[272]。

此處值得注意的是，FIRRMA 使用的「敏感個人資料」與更標準的術語「個人可識別資料」(personally identifiable information) 有所不同，許多人認為這是一個有意的區別，可以做為進一步擴大 CFIUS 審查範圍的另一種手段。雖然兩者有部分重疊，但是對於外國投資人來說，劃分兩者明確的界線還是相當具有挑戰性。「敏感個人資料」可能包括「個人可識別資料」，像是社會安全碼或是教育背景，但是前者可能還涵蓋了傳統上不屬於「個人可識別資料」的其他資訊，像是生物識別資料、網路歷程資料及社群媒體資料[273]。

(2). 其他條款

FIRRMA 與其前身相比，對於 CFIUS 產生了顯著的變化，而其針對的就是中國。首先，FIRRMA 准許 CFIUS 考慮特定的交易是否牽涉

[272] See U.S. Department of Treasury website, https://home.treasury.gov/system/files/206/Proposed-FIRRMA-Regulations-FACT-SHEET.pdf (last visited：12/12/2023).
[273] Blakey, *supra* note 249, at 1011.

到「特別關注」的國家[274]，並每兩年向國會提交 1 份有關中國實體的外國直接投資交易的報告[275]，該報告必須包括這些外國直接投資的詳細項目、中國政府投資所購買的美國企業清單以及中國在美國投資行為的分析[276]。除此之外，FIRRMA 也要求美國財政部長，作為 CFIUS 的主席，應該建立正式的程序，來和外國盟友及國內其他單位交換對於國家安全來說重要的相關資訊[277]。

3. 未來挑戰

FIRRMA 的考驗在於 CFIUS 未來幾年如何處理其必然面對的挑戰，諸如與出口管制體制之平行運作、面對不斷進化之「大數據」[278]風險、與盟友間之合作、維持對國家安全的專注及加速低風險投資的流程。

(1). 外國投資審查與出口管制之平行運作

外國投資審查僅是美國守護國家安全法律系統的一部分，另外一個重要的平行制度則是由美國商務部(U.S. Department of Commerce) 負責的出口管制制度。CFIUS 制度是側重在外國對於美國企業的投資，而出口管制制度則側重外國購買美國的產品，包括專利

[274]See Foreign Investment Risk Review Modernization Act of 2018 § 1702(c)(1).
[275]See Foreign Investment Risk Review Modernization Act of 2018 § 1719(b)(1).
[276]See Foreign Investment Risk Review Modernization Act of 2018 § 1719(b)(2).
[277]See Foreign Investment Risk Review Modernization Act of 2018 § 1713(3).
[278]大數據指的是以持續增加的速度生成的大型、多樣的資訊集。包含資訊的數量，創建和收集信息的速度，以及數據的多樣性或範圍。See Investopedia website, https://www.investopedia.com/terms/b/big-data.asp(last visited：12/17/2023).

及技術[279]。

由於在 ECRA 規範下，為了要決定需要控制的新興和基礎技術，而為跨機構審查程序時，包括商務、國防、國務以及其他有關的聯邦機構，將會仰賴包括與 CFIUS 案件相關的資訊之多種來源[280]，而任何新技術被認定為新興和基礎技術後，除了須受到出口相關管制外，也會自動被視為 FIRRMA 下 CFIUS 審查中之「關鍵技術」[281]。

透過明確的將 CFIUS 審查與出口管制體系連結在一起，美國國會創造了 1 個互補且重疊的系統，來確保美國最先進、敏感的技術不會未經審查就流出國門而遭外國競爭對手用來拉近能力差距。FIRRMA 和 ECRA 之間的相互呼應也進一步反映美國國國會承認，保護國家安全必需要整個政府的通力合作。因此，CFIUS 未來面臨的挑戰就是與出口管制的平行運作，若失敗的話，則可能對國家安全產生嚴重的風險[282]。

(2). 面對不斷進化之「大數據」風險

CFIUS 最初是源於保護美國國內軍事基礎設施，但是隨著技術的進步，在保護國家安全的戰爭上也開闢了新的戰線。由於各種數據在

[279]Tarbert, *supra* note 225, at 1512.
[280]See 50 U.S.C. §4817(a)(2).
[281]See The Foreign Investment Risk Review Modernization Act of 2018, § 1703(a)(6)(A)(vi).
[282]Tarbert, *supra* note 225, at 1515.

社會中扮演的腳色越來越吃重，加上各種技術持續進化及發展，意味著保護因此產生的數據可能提升至國家安全風險的程度[283]。

美國國會對於此部分之擔憂即反應在前述關於 FIRRMA 針對涉及「敏感個人資料」之交易上擴大 CFIUS 審查權範圍的行動上。儘管如此，在未來幾年當中，「大數據」仍然是 CFIUS 的挑戰。隨著越來越多的美國企業將會依賴數據分析來了解客戶即潛在客戶之行為模式及偏好，將會有更多的相關交易會落入 CFIUS 審查權的範圍內，隱私權、數據之相關法規及框架也將成為影響因素之一。儘管如此，CFIUS 可能需要每 5 年或是更頻繁的檢討相關規範，確保其可以持續保持適當的平衡[284]。

(3).增進與盟友的合作

另一個 CFIUS 持續的挑戰將會是與美國盟友間日益增加的合作。FIRRMA 認識到美國的國家安全與親密盟友間之國家安全息息相關[285]，這些盟友也正在面臨相似的威脅，而且正在進行檢視自身國內關於外國投資審查的相關規範[286]。

首先，有相當多的公司跨越國界，在美國和其他國家都有業務運

[283]Tarbert, *supra* note 225, at 1515-1516.
[284]Tarbert, *supra* note 225, at 1519.
[285]所以 FIRRMA 有註 268 所提及的與盟友分享相關資訊之規定。
[286]Tarbert, *supra* note 225, at 1519.

作。工程師、科學家和其他技術專家無時無刻，透過電子郵件、視訊、共享技術資源以及面對面的方式，即時交流知識和想法。這種資訊的自由流通和合作推動了創新，以及這種創新帶來的種種好處。這同時也代表了處理外國投資相關風險，不再可能僅限於在單一國家的基礎上。任何外國公司擁有的技術，可能是在美國研發的或是與美國一銅研發的[287]。

其次，外國公司收購技術對美國的國家安全影響，並不會因該技術是在美國還是在國外完全開發而有所不同。位於外國盟友國家的公司之能力，從美國國家安全的角度來看，也可能是敏感的。這不是因為其技術源自美國，而是因為該技術可能帶來的軍事能力。同樣地，戰略對手從美國獲得之軍事應用能力，亦可能對外國盟友的國家安全產生影響，不論該外國盟友國家之公司是否有參與這些能力的開發[288]。

第三，價值鏈[289]繼續在跨越國界的範疇內緊密整合。外國盟友國家的公司將持續成為許多美國國防和關鍵基礎設施平台中關鍵零組件可信賴的來源。因此，收購這些公司可能對這些關鍵供應鏈的完整性構成實際威脅[290]。

---

[287]Tarbert, *supra* note 225, at 1519-1520.
[288]Tarbert, *supra* note 225, at 1520.
[289]價值鏈是一系列從最初設計到顧客的手上之相連的步驟，用於創造一個完成的產品。這個鏈條明確辨識了在製造過程中增加價值的每個步驟，包括生產的採購、製造和行銷階段。See Investopedia website, https://www.investopedia.com/terms/v/valuechain.asp (last visited：12/28/2023).
[290]Tarbert, *supra* note 225, at 1520.

因為上述原因，美國的盟友國家也都正在檢視其外國投資相關法規，這並非巧合。FIRRMA 意圖在外國投資審查規範部分，成為這些國家的模範。首先，FIRRMA 要求美國財政部長建立一個正式、定期的程序，與外國盟友和夥伴交換「對委員會的國家安全分析或行動來說重要之資訊」[291]。再來，FIRRMA 指示 CFIUS 主席與外國盟友和夥伴「協調...有關可能對雙方國家安全構成風險之投資或技術趨勢方面的行動」[292]。最後，FIRRMA 呼籲「在適當情況下分享有關特定技術和購得此類技術的實體之資訊，以確保美國之國家安全[293]」。因此，FIRRMA 認識到，單單由美國採取行動已不再足夠保護其國家安全[294]。

隨著在 FIRRMA 確立的新制度下繼續前進，考慮如何適當地加強投資審查機構、提升彼此對風險環境的共同理解，以及思考如何更好的合作來應對這些風險，符合美國與盟友的共同利益。美國盟友之安全毫無疑問地強化了美國的安全[295]。

(4).持續聚焦在國家安全上

抵抗利用 CFIUS 的權力進行貿易和非國防之目的之誘惑仍然是另一個重要挑戰。在歷史上，CFIUS 在審查交易時總是專注於國家安全，

[291] See Foreign Investment Risk Review Modernization Act of 2018 § 1713(3).
[292] *Id.*
[293] *Id.*
[294] Tarbert, *supra* note 225, at 1521.
[295] *Id.*

而不是更廣泛的經濟或政策利益。這種專注尊重自由市場在推動商業決策方面的角色，將政府干預保留給其主要責任和獨特能力的領域，也就是國家安全[296]。

在 FIRRMA 問世之前，有人主張 CFIUS 應該明確的考慮某些交易對於美國經濟的影響，包括美國在關鍵產業損失市場之潛在可能以及外國投資者所屬國家之可能影響美國市場之對外投資政策。這種觀點固然有其說服力，因為美國現在的確具有可靠的方法來衡量各個別投資對於美國就業市場、經濟成長、稅收之影響，CFIUS 的確可以被用來保護美國企業不受到外部競爭的損害[297]。

然而，雖然最後 FIRRMA 確實擴大了 CFIUS 的管轄權範圍，允許其審查某些類型的非控制性的直接投資，但該法案維持了 CFIUS 對國家安全的歷史性的、單獨的關注。這個選擇是刻意的，CFIUS 從一開始就被設計為一個國家安全機制。CFIUS 與出口管制以及國防和情報單位合作，以防範各種形式的國家安全威脅，包括非法轉移軍民兩用技術和專業知識，以及試圖封鎖美國進入戰略場所和資產。若將 CFIUS 的管轄權擴張到經濟層面之考量，必然會降低其校旅行其核心任務之能力。更有甚者，儘管有更可靠的方式來衡量個別投資對於美國企業的影響，但實施經濟層面的審查，將引起一連串的新議題，諸如應考

[296] *Id.*
[297] Tarbert, *supra* note 225, at 1521-1522.

慮哪些因素以及分別被賦予的權重。這樣將會違反了美國長期以來一直提倡的開放投資政策，亦可能會損害美國消費者的利益，使 CFIUS 容易受到各種產業特殊利益集團的游說[298]。

CFIUS 的專屬職權限於國家安全，如 FIRRMA 所強化的，明確表明美國歡迎外國投資，並繼續是世界上對外國投資者最開放的國家之一。盡管國會在 FIRRMA 中重申了這種長期以來的做法，但 CFIUS 仍然需要對抗任何考慮國家安全以外因素之情況，尤其是在面對公眾和政治壓力之情況下[299]。

(5).低風險投資的快速通道

對於 CFIUS 而言，最後一個挑戰將是確保低風險的投資不受 FIRRMA 擴大的管轄範圍的阻礙。FIRRMA 最不樂見的就是阻礙對國家安全無或是很低風險之外國投資。FIRRMA 制定了幾項特別旨在促進在美國的外國直接投資的重要條款。其中最重要的是新的自願申報[300](voluntary declarations)概念。自願申報是一種簡易的備案，列舉有關交易的基本資訊，交易各方可以選擇提交自願申報來取代常規通知(regular notice)。在收到自願申報後，根據 FIRRMA 之規定，

[298]Tarbert, *supra* note 225, at 1522.
[299]*Id.*
[300]See Foreign Investment Risk Review Modernization Act of 2018 § 1706.

CFIUS 有權在 30 天內批准交易並以書面通知相關當事人[301]。

自願申報條款對於企業及 CFIUS 的影響重大，對於低風險的交易，可以促進更快速及更具成本效益的審查。同時，使用自願申報可以使 CFIUS 集中注意力和資源於對美國國家安全構成潛在威脅而值得關注的交易。如果有適當之管理，自願申報過程應能夠鼓勵更多的外國投資進入美國。在未來幾年，CFIUS 面臨的挑戰將會是如何利用這種 30 天的機制來處理自願申報之交易，CFIUS 必須注意到太過謹慎也將會有其代價。畢竟，絕大多數外國投資為美國帶來了巨大的好處。因此，不必要的冗長程序可能會使外國投資受挫，這是國會在 FIRRMA 中強調的一點[302]。

三、美國出口管制法制發展

(一)、美國出口管制簡介

美國對國防物品及服務、軍民兩用貨品及技術、特定核子材料及技術，以及可能協助發展核子、化學和生物武器或幫助其運輸的方法之物品實施出口限制。根據法律規定，國防用品之定義為「符合美國軍火清單上國防物品或國防服務之標準」或「提供與該清單上之國防

[301]Tarbert, *supra* note 225, at 1523.
[302]Tarbert, *supra* note 225, at 1523-1524.

物品相同效力」之物品[303]。軍民兩用貨品是既具有民用又具有軍事應用的商品、軟體或技術[304]。

美國的出口控制符合美國參與的多個多邊出口管制體系[305]的要求。此外，美國限制對某些受到美國經濟制裁之國家之出口，例如古巴、伊朗和敘利亞。透過ECRA、「軍火出口管制法」[306]（Arms Export Control Act，AECA）、「國際緊急經濟權力法」[307]（International Emergency Economic Powers Act，簡稱IEEPA）及其他授權，國會將其明確憲法權限之一部分委託給行政部門，以通過控制出口來管理對外貿易[308]。

美國的出口管制體系橫跨了多個不同的許可和執法機構。商務部負責軍民兩用商品、技術及部分國防物品出口之管理及許可。國務院負責軍火之出口管理及許可。財政部負責管理針對美國制裁之出口管制。這些機構進行出口控制的行政執行，而刑事處罰由國土安全部

[303]International Traffic in Arms Regulations, 22 C.F.R. 120.3.
[304]Congressional Research Service, *The U.S. Export Control System and theExport Control Reform Act of 2018*, at 1. See Congressional Research Service website, https://crsreports.congress.gov/product/pdf/R/R46814(lasted visited：01/05/2024).
[305]多邊出口管制體系是由多個國家共同參與的出口管制協議，旨在限制特定物品的出口，以防止這些物品被用於軍事目的、大規模殺傷性武器的發展或傳播。4個主要的多邊出口管制體系分別為：澳大利亞集團（Australia Group），該集團主要是針對化學、生物武器的反擴散；導彈技術管制體系（Missile Technology Control Regime，簡稱MTCR）則是旨在防止導彈技術的傳播，特別是能攜帶核子武器的導彈技術；核供應國集團（Nuclear Suppliers Group，簡稱NSG）之目的在於限制核子技術及原料的擴散，防止其被用於核子武器的製造；瓦賽納協定（Wassenaar Arrangement）則是關於傳統武器和軍民兩用商品的出口管制。
[306]The Arms Export Control Actof 1976, P. L. 94－329(June 30, 1976), 90Stat.729, codified at22 U.S.C.§2751 et seq.
[307]The International Emergency Economic Powers Act, P. L. 95－223(October 28, 1977), 91Stat.1626, codified at 50 U.S.C 1701 et seq.
[308]Congressional Research Service, *supra* note 304, at 1.

（DHS）和司法部的部門發布[309]。

於 2018 年頒布之 ECRA，為美國總統提供廣泛的法律授權，以實施軍民兩用之出口管制。ECRA 廢止了「1979 年出口管理法」[310]（Export Administration Act of 1979，簡稱 EAA 1979），該法是軍民兩用出口管制的基本法律授權，並於 2001 年失效。在 EAA 1979 失效之後，根據其所創建的出口管制體系由總統宣布國家緊急狀態和援引 IEEPA 繼續實施。與其前身不同，ECRA 沒有失效日期[311]。

(二)、美國出口管制歷史演進

美國在建立(及規避)[312]武器和技術出口管制之體制上，已經有很長的歷史。從美國早期開始，就會定期限制出口，特別是在有戰爭或武裝衝突的時候。因為憲法禁止國會對出口徵稅，因此對武器和技術出口的限制一直是受到數量限制和出口禁令的規範。儘管美國早期有實施出口管的例子，但在美國的大部分歷史中，實施出口管制是罕見的，通常僅限於武裝衝突時期。美國現代的出口管制是始於 1940 年，當時國會授權總統管制軍事裝備和彈藥的出口。隨著美國參與第二次

[309] *Id.*
[310] Export Administration Act of 1979, P.L. 96-72 (September 29, 1979), 93 Stat. 503.
[311] *Id.*
[312] 舉例來說，英國在 18 世紀時禁止出口製造羊毛、絲綢、棉花、亞麻之機械，儘管如此，當時許多美國人仍受到美國建國國父之一之 Alexander Hamilton 鼓勵，試圖規避禁令來曾其美國的製造能力。

世界大戰，國會擴大了這一授權，將管制擴大到包括民用商品[313]。

1.雙功能的出口管制

第二次世界大戰結束後，美國國會開始限制總統使用各種經濟控制的授權。儘管國會宣示其一般政策是消除緊急戰時管制，但國會仍然繼續延長總統管制出口的權限，只是設有明確的期限。最初的理由是，由於戰爭破壞了歐洲和東亞的工業和農業生產力，美國商品之需求很高，通過保留對出口的控制，國會希望減少異常的外國需求對美國商品供應的通貨膨脹影響。因此，早期戰後的出口管制主要用於經濟面向，而非出於外交政策或國家安全之原因[314]。

2.冷戰時期之出口管制

到了 1940 年代末期，美國與蘇聯[315](Soviet Union)之間的關係變得越來越緊張，當各種官員、學者和知識分子開始提出後來被稱為「圍堵」(containment)的政策時，因為技術發展在國防方面扮演日益重要的角色，一些國會成員認為出口管制可能是一個有價值的外交政策和國家安全工具。1949 年，國會通過了「1949 年出口管制法」[316](Export

[313]Congressional Research Service, *supra* note 304, at 2.
[314]*Id.*
[315]蘇聯為 20 世紀的主要政治實體之一，官方名稱為蘇聯社會主義共和國聯盟(Union of Soviet Socialist Republics, USSR)。See New world Encyclopedia website, https://www.newworldencyclopedia.org/entry/Soviet_Union(last visited：01/11/2024).
[316]The Export Control Act of 1949, P.L. 81-11 (February 26, 1949), 63 Stat. 7.

Control Act of 1949， 簡稱 ECA 1949），這是國會在和平時期採取的第 1 個全面的出口管制體系[317]。

在 ECA 1949 中，國會宣示美國將出口控制用於下列 3 個原因：保護國內經濟、促進美國的外交政策以及從國家安全的角度對出口進行必要的警惕，這奠定了現代體制的三項戰略。雖然該法案最初定於 1951 年到期，但韓戰和其他冷戰外交政策考量下，ECA 1949 在大致內容未經修改的情況下持續了近 20 年[318]。

由於了解到如果沒有多邊合作，與外交政策和國家安全目標相關的出口管制將會無效，美國及其在歐洲的主要盟友於 1949 年建立了顧問團體（Consultative Group），這是由資深出口管制官员组成之機構，負責制定禁運物品清單。此顧問團體促成了 2 個委員會。協調委員會(The Coordinating Committee，簡稱 COCOM)於 1949 年成立，負責協調針對蘇聯和東歐的出口限制。中國委員會（The China Committee，簡稱 CHINCOM）於 1952 年成立，則是負責協調針對中華人民共和國的出口限制。為了鼓勵其他友好國家遵守出口管制，國會於 1951 年通過了「共同防衛援助控制法」（Mutual Defense Assistance Control Act of 1951），要求接受美國對外援助的國家

[317] Congressional Research Service, *supra* note 304,at 3.
[318] *Id.*

遵守美國的出口管制[319]。

3.重新檢討與自由化

隨著1960年代末期，美國與蘇聯間之關係逐漸緩和，美國出口管制體系才出現第1次的重新檢討及修正。隨著貿易對於美國及其盟友的經濟越來越重要，及COCOM參與者對於與東歐共產主義國家進行貿易之方法上存在差異，增加了對於美國出口管制體系自由化之壓力。美國的出口管制長期以來一直比COCOM建立的多邊管制更加嚴格，政策制定者和產業界領袖越來越擔心美國的嚴格出口管制對於經濟之影響。部分國會成員和產業專家主張，嚴格的美國出口管制將使美國公司與其位於歐洲及日本之競爭對手競爭時處於劣勢[320]。

針對這些擔憂，美國國會於1969年通過了「1969年出口管理法」[321]（Export Administration Act of 1969，簡稱EAA 1969），以取代ECA 1949。儘管EAA 1969仍授權總統限制出口可從其他國家可獲得之商品，但該法案要求政府向國會報告限制的原因。除此之外，該法案還要求政府告知出口商有關拒絕發放出口許可證的原因、可能導致拒絕發放出口許可證的考慮因素，或者出口許可證申請出現「不當

[319] *Id.*
[320] Congressional Research Service, *supra* note 304, at 4.
[321] Export Administration Act of 1969, P.L. 91-184 (December 30, 1969), 83 Stat. 841.

延遲」的原因[322]。

在整個 1970 年代，美國國會繼續放寬出口管制。例如，在 1977 年，國會宣布，1 個國家是否為共產主義國家將不再決定其是否受到出口管制之限制。相反的，政府應考慮其他因素諸如「該國與美國現在和潛在的關係、該國與美國友好或敵對之國家現在和潛在的關係、該國按照美國政策控制再移轉的能力和意願」等因素[323]。

EAA 1979 取代了 EAA 1969，成為現行之「出口管理規則」[324]（Export Administration Regulations，簡稱 EAR）在當時的法律基礎，進一步寬鬆美國之出口管制體系。1989 年蘇聯解體，部分歸因於美國冷戰時期的出口控制政策的成功。自 1970 年代末期開始，美國國會在其出口管制權限到期前經常不予更新。當 EAA 1969 於 1976 年到期時，美國總統透過援引 1917 年的「與敵人交易法」[325]（Trading with the Enemy Act，簡稱 TWEA）下的權限，維持了這些管制措施。後來，國會最終更新了 EAA 1969，並於 1979 年創建了一個新的 EAA 1979。在 1980 年代和 1990 年代，國會仍然定期使出口管制權限過期。總統再透過援引 1977 年取代 TWEA 的 IEEPA 來維持這些管制措施。除了 2000 年 11 月至 2001 年 8 月對 EAA 1979 的 10 個月重新授

[322] *Id.*
[323] *Id.*
[324] 15 C.F.R. 730 et seq.
[325] TheTrading with the Enemy Actof 1917, P.L. 65-91(October 6, 1917), 40Stat.411, codified at12U.S.C.§95and50U.S.C.§4301et seq.

權外，出口管制體系在 1994 年至 2018 年 ECRA 通過之前的近 24 年間一直由 IEEPA 維持[326]。

(三)、2018 年出口管制改革法案

在美國技術領導地位以及其他國家試圖合法或非法取得美國關鍵技術之辯論當中，出口管制已經是很重要的部分。美國國會在 2018 年通過 ECRA，作為美國修正其貿易及投資政策的部分行動，同時間國會也通過了 FIRRMA[327]。

ECRA 取代了大部分已經失效的 EEA 1979，為軍民兩用貨品及某些軍事零件之出口提供了永久性的法律授權基礎。ECRA 要求美國總統對受到美國管轄物品之出口、再出口及國內移轉進行管制，無論是由美國人或是外國人進行。並要求商務部長建立及維護一個囊括對美國國家安全及外交政策構成威脅的管制物品、外國人、終端用途之清單。ECRA 還要求商務部實施出口許可制度、禁止未經許可之管制物品之出口、再出口和國內移轉以及監視裝船及其他移轉之方式[328]。

ECRA 基本上维持了根據 EAR 所制定的出口管制體系，該體系在 IEEPA 之授權下維持了將近 25 年。在商務部之下，由 BIS 繼續管理

[326]Congressional Research Service, *supra* note 304, at 5.
[327]Congressional Research Service, *Export Controls: Key Challenges*, at 1. See Congressional Research Service website, https://crsreports.congress.gov/product/pdf/IF/IF11154(lasted visited：01/14/2024).
[328]*Id.*

軍民兩用出口管制系统和 EAR，後者包含了軍民兩用物品以及部分軍事零件的出口許可政策。EAR 還包含將會受到拒絕出口政策影響之受制裁、被拒绝或未經驗證之各方清單，並且也規定了出口許可之相關程序及違規時之民、刑事處罰。基本上幾乎所有的出口都受到 EAR 之規範，具體上則是藉由「商業管制清單」[329]（Commerce Control List，簡稱 CCL）在多邊或單邊基礎上建立了對特定物品的出口管制[330]。

在 ECRA 當中最重要的改變就是要求總統建立一個由商務部主導的跨部門程序，包括國防部、國務院、能源部和其他機構，以確定新興和基礎技術[331]。然後，商務部再接著對這些物品建立出口許可政策[332]。ECRA 規定，至少對於受到美國一般禁運或武器禁運的國家，出口此類技術將會需要出口許可。此流程也會被用於辨識，在針對特定外國投資交易審查該交易對於國家安全之影響時，應被納入審查之技術。根據 FIRRMA 之規定，由此流程所選定的關鍵技術將會受到 CFIUS 進

[329]是否需要向美國商務部申請出口許可證的關鍵在於打算出口的物品是否有特定的出口管制分類號（Export Control Classification Number，簡稱 ECCN）。ECCN 是一個包含字母和數字的代碼，例如 3A001，代碼描述了物品並對應相應的出口許可條件。所有的 ECCN 都列在 CCL 中。CCL 分為 10 個大類，每個大類進一步細分為 5 個產品組。See Bureau of Industry and Security website, https://www.bis.doc.gov/index.php/regulations/commerce-control-list-ccl(lasted visited：01/15/2024).

[330]Congressional Research Service, *supra* note 327, at 1.

[331]BIS 在 2022 年 5 月 23 日的一項提案規則中宣告，BIS 將不再區分 ECRA 第 1758 條所規定之「新興」或「基礎」技術。取而代之的，這些技術將被稱為「第 1758 條技術」。這種做法反映了在履行 BIS 根據 ECRA 第 1758 條之法定職責時，在技術上劃分方面存在的困難。除此之外，將這些項目稱為第 1758 條技術目的在於在最大程度的提高 BIS 的靈活性及效力。See Federal Register website, https://www.federalregister.gov/documents/2022/05/23/2022-10907/commerce-control-list-controls-on-certain-marine-toxins#print(lasted visited：01/17/2024).

[332]截至 2022 年 6 月 29 日，實際上被列入 CCL 管制之新興技術項目有 38 項。See Bureau of Industry and Security website, https://www.bis.doc.gov/index.php/documents/2022-update-conference/3073-rev3-emerging-tech-update-2022-section-1758-controls-tongele/file(lasted visited：01/17/2024).

行額外的審查。雖然這些技術的辨識流程及速度可能因此延遲FIRRMA和 ECRA 的主要條款的實施，此流程回應了潛在對手可能通過對美國公司之投資來獲得新興技術的擔憂[333]。

(四)、新興與基礎技術出口管制面臨之挑戰

ECRA 要求商務部與其他單位合作來確定和管制新興和基礎技術。儘管已經確定了一些具體的技術，但一些國會成員針對這些決定流程之成果及速度有所批評，並可能重新評估由商務部所主導之確定流程之速度及效果，諸如為何被確定出來的技術數量這麼少、是否與跨單位之確定程序有關、有沒有其他替代方案或單位可以選擇[334]。

事實上，在 2022 年 10 月 28 日，眾議院議員 Jim Banks 於眾議院提出「2022 年優先考量國家安全出口管制法案」[335](Prioritizing National Security in Export Controls Act of 2022)，該法案試圖將 ECRA 賦予商務部之相關權限移轉到國防部下轄之國防科技管理局(Defense Technology and Security Administration)，並指出下列事實：(1) 2018 年，國會以壓倒性的跨黨派基礎通過了 ECRA，要求商務部加強對向高風險國家，尤其是中國，轉移新興和基礎技術的限制。然而，這幾年來幾乎沒有進展；(2)商務部在調和其保護美國

[333]Congressional Research Service, *supra* note 327, at 2.
[334]Congressional Research Service, *supra* note 304, at 37.
[335]Prioritizing National Security in Export Controls Act of 2022, H.R. 9241, 117th Cong. (2022).

國家安全的使命與促進對高風險國家，尤其是中國，之美國出口目標方面顯得無能為力；(3) 截至 2022 年 8 月，由商務部領導的審查美國對中國技術出口之流程當中，幾乎批准了所有的申請，一些特別重要之技術銷售甚至是增加的；(4) 儘管可能有數萬家中國實體符合美國對軍事最終使用者出口限制的標準，美國商務部目前的實體清單[336]上只列有 70 家中國實體。(5) 根據 2018 年通過的 ECRA，負責在美國商務部下執行出口控制之 BIS 至今還未採取任何行動，限制基礎技術轉移給中國[337]。(6) 在 2022 年 5 月，BIS 放棄了基礎技術此一標準，這被視為其對國會之蔑視達到頂峰。目前該法案正提交眾議院內之相關領域之委員會審議[338]，該法案之後續動態發展值得關注[339]。

[336]EAR 包含一份特定外國人名單，包括企業、研究機構、政府和私人組織、個人以及其他類型的法人，這些人對特定物品的出口、再出口和/或轉讓（國內轉移）受到特定的出口許可要求。See Bureau of Industry and Security website, https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/entity-list(last visited：01/26/2024).

[337]根據 ECRA 規定是要求 BIS 要辨識出應該受出口管制之新興及基礎技術，但是 BIS 僅辨識出部分新興技術，並無辨識出基礎技術，後來甚至不再區別 2 者，所以才會有這樣的批評出現。

[338]美國眾議院之立法流程，通常是先由眾議員提出法案，該法案再交由相關的委員會進行審議，如果獲得委員會的通過，該法案就會被列入眾議院之議程表，以便進行投票、辯論或修正。如果法案以眾議院之簡單多數通過（435 名議員中的 218 名），法案就會移交給參議院。在參議院，法案被分配給另 1 個委員會，如果獲得通過，就會在參議院進行辯論和投票，再次以簡單多數（100 名參議員中的 51 名）通過該法案。最後，由眾議院和參議院成員共同組成的委員會解決眾議院和參議院版本之間的差異。最後版本的法案返回眾議院和參議院進行最後批准。政府印務局負責印刷修改後的法案。總統有 10 天的時間簽署或否決待簽之法案。See United States House of Representatives website, https://www.house.gov/the-house-explained/the-legislative-process(last visited：1/27/2024).

[339]See CONGRESS.GOV website, https://www.congress.gov/bill/117th-congress/house-bill/9241?s=1&r=14(last visited：1/22/2024).

參、韓國防範國家關鍵技術外流法制

韓國與我國均屬於地窄人稠，高人口密度國家，經濟發展模式與產業結構均極為類似，兩國均為以出口為導向之國家，製造業扮演重要的腳色，產業均聚焦於電子及精密儀器[340]，且其保護國家關鍵技術之立法模式，與我國將國家核心關鍵技術分散於國安法、營業秘密法、臺灣地區與大陸地區人民關係條例之法律中規範之立法模式不同，韓國係唯一以專法「防止產業技術外流及產業技術保護法」(Act on Prevention of Divulgence and Protection of Industrial Technology，簡稱 ITPA)立法保護其國家關鍵技術即「產業技術」(Industrial Technology)與「國家核心技術」[341](National Core Technology)，集防止技術竊取、外國投資審查、出口管制於同一部法律。而營業秘密保護在韓國是以「不正競爭防止及營業秘密保護法」(Unfair Competition Prevention and Trade Secret Protection Act，簡稱 UCPA)規範，產業技術、國家核心技術與營業秘密各自有不同之構成要件，並無必然之關聯，與美國、及我國此次新修法，將國

[340]見經濟部網站，https://www.moea.gov.tw/MNS/populace/news/News.aspx?kind=1&menu_id=40&news_id=108510(最後瀏覽日：01/29/2024)。

[341]依據產業技術保護法第 2 條第 2 巷之規定，「國家核心技術」是指依據該法第 9 條規定所指定的產業技術。這項技術在韓國和海外市場具有高技術和經濟價值，對相關行業具有高增長潛力，並且在向外界揭露的情況下可能對國家安全和國家經濟的發展產生重大不利影響之技術。See Korea Legislation Research Institute website, https://elaw.klri.re.kr/eng_service/lawView.do?hseq=24351&lang=ENG(last visited：01/29/2024).

家核心關鍵技術與營業秘密一同規範之立法模式不同，其法制發展狀況亦值得我國未來針對國家核心關鍵技術保護部分立法之參考。

一、韓國防止產業技術外流及產業技術保護法

(一)、立法背景

面對中國吸取他國高科技技術的強大野心，韓國產業關鍵科技技術遭竊取並流向海外的個案日漸增加，其中大部份的產業技術又都流向中國，給韓國帶來無法龐大之經濟損失。為了防止關鍵技術繼續外流，實踐國家保護產業技術之責任與義務，韓國於 2006 年制定 ITPA，全文共 6 章 39 條，立法目的[342]為防止產業技術不當洩漏及保護產業技術，以強化國家產業競爭力，並對國家安全及經濟發展做出貢獻[343]。

當時雖然技術外流事件頻傳，韓國卻無完善之法律制度保護國家核心技術，相關規定散見在不同法規，且有其侷限性，比如說營業秘密之保護係在 UCPA 規範，為該法之目的在於防止不正當使用他人商標、商號等不正當競爭行爲和侵害他人營業秘密之行爲，以維持健全交易秩序，且在適用上有其侷限，諸如適用對象僅限於企業，其他機構適用上有所困難、僅限事後處罰，缺乏事前預防機制、影響國家安

[342]ITPA 第 1 條之規定。
[343]鄭嘉文、許祐寧（2017），〈跨境投資技術保護與營業秘密之法制研析〉，《科技法律透析》，29 卷 12 期，頁 42-43。

全之核心技術在合法移轉如牽涉到企業併購時，管制措施不足。其他法規如「對外貿易法」僅針對戰略物資；「技術開發」促進法僅限於戰略技術；「促進利用資訊通信網及資訊保護相關法律」主要處理網路營運相關的侵害行為，保護個人資料，並無處理技術外流問題。為了防止技術因不正當的方 法而流失，乃決定制定專法，建立整體性制度保護產業技術[344]。

二、區分「產業技術」與「國家核心技術」

「產業技術」是指是由相關中央政府行政機關主管，根據法律授權所確定、公布、宣布或認證的特定分類下的技術。目標是在相關機關之權限下，透過辨識出對商品或服務之發展、生產、傳播、使用所不可或缺之方法與技術資訊，以增進產業之競爭力。該條文並列舉了特定法律下所規範之技術[345]。

「國家核心技術」則是指依據 ITPA 第 9 條之規定指定的產業技術。此技術在韓國和海外市場具有高技術和經濟價值，對相關產業具有高增長潛力，並且若在國外揭露的情況下可能對國家安全和國家經

[344]吳宛芳（2021），《韓國「防止產業技術外流及保護產業技術法」與我國敏感科技保護法制之借鏡》，頁 32，國立陽明交通大學科技法律學院科技法律研究所碩士在職專班論文。

[345]包含 ITPA 第 9 條所規定之國家核心技術、產業發展法第 5 條規定之最先進技術、產業創新促進法第 15-2 條規定之新技術、電氣技術管理法第 6-2 條所規定之新電氣新技術、環境技術和產業支持法第 7 條所規定之新技術、建築技術促進法第 14 條所規定之新建築技術、健康醫療服務技術促進法第 8 條規定之健康及新技術、促進和提升根基產業法第 14 條規定之確定之核心根基技術、其他法律或相關法律授權所確定、公布、宣布或認證的技術。

濟發展產生重大不利影響[346]。而國家核心技術也是屬於產業技術之一種。依據韓國產業通商資源部(Ministry of Trade, Industry and Energy，簡稱 MOTIE)2022 年 7 月 26 日第 2022-557 號公告，目前韓國預計將國家核心技術新增至 75 項，包含半導體及顯示器等韓國具有領先地位之產業技術[347]。

也因為國家核心技術之前述重要特徵，IPTA 針對國家核心技術之指定、變更、取消之流程、保密及保護措施、出口、跨境收購、合併、合資等行為之許可及報備、侵害態樣、罰則都有對應之規範。

(二)、國家核心技術之指定、變更、取消

依據 ITPA 第 7 條之規定，在 MOTIE 下成立產業技術保護委員會(Industrial Technology Protection Committee，簡稱 ITPC)，ITPC 由不超過 25 名之成員組成，主席為 MOTIE 之部長。該委員會之主要職權包含(1)國家核心技術之指定、變更和取消事項、(2)國家核心技術之出口事項、(3)有關擁有產業技術、國家核心技術之機構之跨境收購及合併事項、(4)其他經總統令確定為防止產業技術外流和保護產業技術所需之事項[348]。

[346]ITPA 第 2 條第 2 項之規定。
[347]韓國科學及資通訊部公布〈國家戰略技術培育計劃〉並選定 12 個國家戰略技術，資訊工業策進會科技法律研究所，https://stli.iii.org.tw/article-detail.aspx?tp=1&d=8932&no=64（最後瀏覽日：2024/02/12）。
[348]ITPA 第 7 條之規定。

MOTIE 部長可選擇應被指定為國家核心技術之技術，或是其收到在相關中央政府機關負責人之權限下已經選擇應被指定技術之通知時，經 ITPC 審議後，部長可以指定該技術為國家核心技術。如果由 MOTIE 部長選擇的應被指定技術正好在其他中央政府行政機關之負責人之權限下，部長在 ITPC 審議之前應先與相關中央政府機關的負責人進行諮詢[349]。

MOTIE 部長及相關中央政府機關之負責人應基於該技術對國家安全和國家經濟的連帶影響、相關產品在韓國和海外市場的市占率、相關領域研究之趨勢以及技術擴散之協調等因素，做全面的考慮後，在最小範圍內選擇應被指定之技術[350]。

如果 MOTIE 部長，認為有必要改變某個國家核心技術之範圍或內容，或取消其國家核心技術之指定，或其收到相關中央政府機關負責人之請求，改變該機關負責人權限下之國家核心技術的範圍或內容，或取消國家核心技術之指定時，經 ITPC 審議後，其可以在更改或取消該指定。MOTIE 部長選擇之國家核心技術是由其他中央政府行政機關之負責人所管轄，應在 ITPC 審議前與該負責人進行諮詢[351]。

如果 MOTIE 部長根據 ITPA 第 9 條第 1 項之規定指定國家核心技

[349]ITPA 第 9 條第 1 項之規定。
[350]ITPA 第 9 條第 2 項之規定。
[351]ITPA 第 9 條第 3 項之規定。

術，或者根據 ITPA 第 9 條第 3 項之規定更改國家核心技術的範圍、內容或取消其指定時，應當公告周知此事[352]。

當 ITPC 依據 ITPA 第 9 條第 1 項、第 3 項將被指定技術指定為國家核心技術、或進行變更或取消指定之情事進行審議時，若有利害關係人提出請求，如擁有或管理受指定技術的之企業等，應依據總統令之規定，提供其表達意見之機會[353]。

韓國在國家核心技術之指定上，對於國家核心技術擁有者之負擔在立法設計上盡量降低，賦予國家核心技術所有人主動提出申請國家核心技術指定之變更、取消之權利，並給予利害關係人有參與程序之機會，試圖減輕國家核心技術擁有者之負擔。另在指定國家核心技術上有統一基準來遵循，並就變更、取消的準則及程序有明確規範，顯示韓國 MOTIE 對國家核心技術之管控下，仍有尊重市場經濟自由，給予利害關係人些許空間[354]。

(三)、國家核心技術之特別規定

1.保密及保護措施

國家機關、地方政府、公共機構以及由總統令確定之其他機構，

[352]ITPA 第 9 條第 4 項之規定。
[353]ITPA 第 9 條第 4 項之規定。
[354]吳宛芳，前揭註 344，頁 54-55。

均不得公開有關國家核心技術的資訊，若該資訊之揭露不會對國家安全和國家經濟發展產生不利影響，則不在此，且應以書面或電子文件形式蒐集相關人士之意見，並徵得 MOTIE 部長和相關部門或機構之負責人之同意，於法律規定之期限內將該案件提交給 ITPC 進行審議[355]。

擁有及管理國家核心技術之機構負責人，應採取法律所規範之相關措施以防止國家核心技術之外流，包含指定保護區域、控制存取、管理人員流動、簽署保密協議等方式，任何人不得無故拒絕、干涉、挑戰前開保護措施[356]。若違反規定，拒絕、妨害或躲避保護措施者，可處以 1 千萬韓元以下之行政罰緩[357]。若機構負責人沒有採取保護措施保護國家核心科技，MOTIE 部長可對其提出改善建議，機構負責人應制定及執行改善計畫並通知 MOTIE 部長[358]。

2. 通報義務及啟動調查

如果 ITPA 第 14 條所規定[359]之侵害行為可能即將或已經被犯下，擁有包括國家核心技術之產業技術之機構或通過國家研發計畫發展之產業技術之機構負責人，應立即向 MOTIE 部長和情報調查機構負責人報告，並且可以要求採取必要的措施[360]。

[355]ITPA 第 9-2 條之規定。
[356]ITPA 第 10 條之規定。
[357]ITPA 第 39 條第 1 項第 1 款之規定。
[358]ITPA 第 13 條之規定。
[359]詳見本研究之肆、三、(五)部分。
[360]ITPA 第 15 條第 1 項之規定。

在收到前述之請求或知悉前述之侵害行為已經發生，MOTIE 部長和情報調查機構負責人應進行調查並採取其他必要措施[361]。

ITPA 藉由前開規定，以利對技術外流事件能確實掌握情況，並事前預防技術外流的發生。值得注意的是，不僅國家核心技術擁有人有此義務及權利，透過國家研發計畫發展之產業技術亦同，顯示韓國產業技術保護法具有強烈保護國家法益的目的[362]。

3. 出口之許可及報備

在出口管制方面，則是區分是否有使用政府補助作為國家核心技術之研究、發展，而異其出口管制之模式。若有，則當擁有該國家核心技術之機構欲銷售、移轉國家核心技術給外國企業或其他實體時，應事先取得 MOTIE 部長之許可[363]；若無，則該機構需先向 MOTIE 部長報備，當 MOTIE 部長認為該國家核心技術之出口可能對國家安全產生實質影響時，得在與相關中央政府機構負責人諮詢後及經 ITPC 審議後，命令相關機構採取諸如暫停、禁止、回復原狀等措施[364]。

為了保護國家核心技術而限制企業技術出口，重點是如何兼顧企業之自主經營權，不對企業造成過度之限制。韓國對於企業事前申報

[361]ITPA 第 15 條第 2 項之規定。
[362]吳宛芳，前揭註 344，頁 56。
[363]ITPA 第 11 條第 1 項之規定。
[364]ITPA 第 11 條第 5 項之規定。

規定要件將對企業之限制最小化並將規定明確化。出口許可之審查時間原則上是 45 天，而報備制之審查時間為 15 天，相對較短，若判定結果不會對國家安全造成嚴重影響，即可出口。除此之外，對於並未使用國家補助作為國家核心技術之研究、發展者，設有國家核心技術的事前檢討規定，讓擁有國家核心技術的企業在有技術出口或併購等規劃時，可預先向主管機關申請，提早得知該技術是否與國家安全相關，該條第 2 項規定主管機關要在 15 天內告知判定結果，此外依第 3 項此判定結果可以維持 1 年有效期限。對於企業在輸出技術時可減少等待審查期間[365]。

4.跨境收購、合併、合資等行為之許可及報備

當擁有使用政府補助研究、發展之國家核心技術之機構，欲進行跨境收購、合併、合資等行為，需事先獲得 MOTIE 部長之許可。當 MOTIE 部長在審查其行為對於國家安全之影響、諮詢相關中央政府機關負責人並經過 ITPC 審議後，方得許可前開行為，並且可以附加必要之條件[366]；反之，當擁有非使用政府補助研究、發展之國家核心技術之機構，欲進行前開行為時，則僅需先向 MOTIE 報備；除此之外，不論有無使用政府補助研究、發展國家核心技術，若相關機構發現有

[365]吳宛芳，前揭註 344，頁 59-60。
[366]ITPA 第 11-2 條第 1、4 項之規定。

特定之外國人欲進行跨境收購、合併、合資等行為，都必須立即向MOTIE報告，MOTIE部長得要求該外國人配合許可程序[367]。

當MOTIE部長認為前述幾種情況之跨境收購、合併、合資等行為之國家核心技術外流，可能對國家安全產生實質影響時，得在與相關中央政府機構負責人諮詢及經ITPC審議後，命令欲進行跨境收購、合併、合資等行為之機構採取諸如暫停、禁止、回復原狀之措施[368]。

也就是說，擁有國家核心技術之機構，不論是主動或被動參與跨境收購、合併、合資等行為，均應向MOTIE報告。若跨境收購、合併、合資等行為將嚴重影響國家安全，MOTIE自得採取必要措施[369]。

在ITPA立法之初，僅對國家核心技術出口管制有所規範，並未就牽涉國家核心技術之跨境收購、合併、合資等行為有所規範，當時即有論者認為此將成為國家核心技術外流之破口。例如2004年中國京東方（BOE）收購韓國企業HYDIS，取得關鍵技術後，2006年則任由BOE-HYDIS聲請破產保護並脫手離開，就曾引發輿論。惟當時韓國政府認為外國人投資情況可以適用「外國人投資促進法」(Law for Promotion of Foreign Investment)處理，而國內企業海外投資則以「外匯交易法」(Foreign Exchange Transactions Act)規範即足，

[367]ITPA第11-2條第2、3、6項之規定。
[368]ITPA第11-2條第7項之規定。
[369]鄭嘉文、許祐寧，前揭註343，頁44。

無須額外增加管制以免疊床架屋，而後因收購、合併韓國擁有國家核心技術之企業導致韓國國家核心技術外流之情況頻繁發生。為防止國家技術外流到國外，韓國陸續透過修法加強管制。在 2011 年 7 月新增規定[370]，有使用國家補助者，欲進行跨境收購、合併、合資等行為，必須先向韓國知識經濟部長(Minister of Knowledge Economy)[371]報備，無使用補助者，則無須受限。其後隨著海外競爭者之技術奪取型收購、合併等取得技術手段逐漸進化，2019 年 8 月再度修改規定，成為現行規定，對於外資進一步加強管控，強化對國家核心技術的保障[372]。

5. 面臨之挑戰

(1). 並無配套之補償措施

若是自主研發，並未使用國家補助而依照 ITPA 之規定，被指定為國家核心技術，擁有國家核心技術之企業因此受到之經濟上損失[373]，韓國政府並無配套之補償措施。有韓國學者因此認為此種對財產權施加限制之作法，恐怕有違憲之疑慮[374]。

若無改善國家核心技術擁有者之權利與義務不平衡的情況，則

[370]當時即新增 ITPA 第 11-2 條。
[371]即 MOTIE 部長之前身。
[372]吳宛芳，前揭註 344，頁 58-59。
[373]出口或收購、合併。投資受到限制可能因此造成企業發展受到影響而有經濟上之損失。
[374]吳宛芳，前揭註 344，頁 60。

擁有國家核心技術擁有者將會排斥其擁有之技術被指定為國家核心技術，將會導致國家核心技術管理不確實。若要改善此問題，可以考慮針對被指定為國家核心技術之對象，提供稅務優惠、進軍海外市場之技術保護支援、訴訟支援等方案，或是可以更進一步提供其他誘因來促使企業對於國家核心技術之重視。透過改善國家核心技術擁有者之權利與義務之不平衡，企業才有可能自發性、積極參與保護國家核心技術[375]。

(2). 技術保護政策及支援不足

韓國大部分技術外流事件通常發生原因是歸因於擁有者不確實之人力管理及設備管理。韓國產業技術保護協會 2009 年曾經做過調查，調查結果顯示大企業和中小企業之的技術保護水準有相當之落差，各種資源相對較少之中小企業更需要政府之奧援以保護所擁有之國家核心技術。目前韓國國家情報院(National Intelligence Service)的產業安全中心(National Industrial Security Center)主導對國家核心技術所有人提供支援的代表性機關。該中心提供產業安全教育支援、透過諮商，檢查企業技術保護管理情況[376]。這些支援相當有價值，但應該要針對企業規模不同而提供差別化的支援措施，特別是針

[375]吳宛芳，前揭註 344，頁 79-80。
[376]See National Intelligence Service website, https://eng.nis.go.kr/EID/1_7_2.do(last visited：02/20/2024).

對中小企業，增加更多支援[377]。

(四)、侵害態樣

ITPA 第 14 條，規定任何人均不得為下列行為：

(1)以竊取、欺騙、威脅或其他不正當之方法取得任何擁有產業技術之機構之產業技術，或使用、公開該產業技術(包含秘密的提供資訊給特定人)[378]。

(2)依法律或契約負有保密義務之人，意圖獲得不當之利益或明知會造成擁有產業技術機構之損失，而洩漏產業技術；或使用、揭露已經洩漏之產業技術；或使第 3 方利用該產業技術[379]。

(3)明知產業技術涉及(1)或(2)中之任何行為，而獲得、使用或公開產業技術;或在取得產業技術後得知產業技術涉及(1)或(2)中之任何行為，而使用或公開產業技術[380]。

(4)因重大過失而不知產業技術涉及(1)或(2)中之任何行為，而獲得、使用或公開產業技術;或在取得產業技術後因重大過失而不知產業技術涉及(1)或(2)中之任何行為，而使用或公開產業技術[381]。

(5)未依法律獲得許可或以不正當之方法獲得許可，而出口國家

[377]吳宛芳，前揭註 344，頁 60-61。
[378]ITPA 第 14 條第 1 項第 1 款之規定。
[379]ITPA 第 14 條第 1 項第 2 款之規定。
[380]ITPA 第 14 條第 1 項第 3 款之規定。
[381]ITPA 第 14 條第 1 項第 4 款之規定。

核心技術[382]。

(6)意圖在外國使用國家核心技術，或明知國家核心技術將在外國使用，卻未依據法律獲得許可，或以詐騙或其他不正當之方法獲得許可，進行跨境收購、合併等行為[383]。

(6-2)意圖在外國使用國家核心技術，或明知國家核心技術將在外國使用，卻未依據法律報備，或以詐騙或其他不正當之方法進行報備後，進行跨境收購、合併等行為[384]。

(6-3) 根據 ITPA 第 34 條[385]或與擁有產業技術之機構間依據契約負有保密義務之人，拒絕、逃避依據相關擁有產業技術之機構之要求返還、刪除產業技術之記錄，如文件、圖畫或電子紀錄等，或意圖獲取不當利益或對擁有產業技術之機構造成損失而保留副本[386]。

(7)未能遵守 MOTIE 部長根據 IPTA 第 11 條或第 11-2 條所發出

[382]ITPA 第 14 條第 1 項第 5 款之規定。
[383]ITPA 第 14 條第 1 項第 6 款之規定。
[384]ITPA 第 14 條第 1 項第 6-2 款之規定。
[385]ITPA 第 34 條規定：「以下人員不得洩露或不當取用其職務上所知秘密。1. 擁有產業技術機構之管理人員、職員（包括教授、研究員、學生）；2. 根據 ITPA 第 9 條之規定，履行國家核心技術指定、變更及解除業務者或根據 ITPA 第 16 條履行國家核心技術保護、管理等支援業務者；3. 根據 ITPA 第 11 條及第 11-2 條，審查國家核心技術出口及收購、合併等相關事項或事前審查、調查業務者；3-2.根據 ITPA 第 11-2 條第 3 項及第 6 項進行跨境收購、合併等之外國人及外國人之管理者及職員；4.依照 ITPA 第 15 條規定執行受理和防止侵害行爲等業務者；5.根據 ITPA 第 16 條第 4 項第 3 款規定從事諮詢業務或實地調查者；6.根據 ITPA 第 17 條第 1 項之規定，執行產業技術保護及管理現狀事實調查業務者；7.根據 ITPA 第 20 條第 2 項之規定，受僱於產業安全技術開發商從事產業安全技術研究、開發之業務者；8.依 ITPA 第 23 條之規定執行產業技術紛爭調解業務者；9.根據 ITPA 第 33 條之規定，受 MOTIE 部長部分權限委託執行業務者；10.執 行依據官方資訊公開法請資訊揭露、產業技術訴訟業務等總統令所規定之業務時，得知產業技術資訊者。」
[386]ITPA 第 14 條第 1 項第 6-3 款之規定。

之命令[387]。

(8)未依據資訊被提供之目的，而使用或揭露依據總統令規定之任何法律程序所提供之包含產業技術在內之資訊[388]。

ITPA 第 34 條則係針對附有保密義務之人，不得洩漏或不當取用其職務上所知悉之秘密所作之規範[389]。

ITPA 第 14 條所規範之行為主體部分，除了該條第 6-3 項係限於具有保密義務之人外，其餘並不限於企業或擁有產業技術之機構之內部人，意即任何人均可成為 ITPA 侵害行為之主體。保護客體則是產業技術及國家核心技術，並不包括商業上資訊。ITPA 採用列舉之方式，單純對違反 ITPA 第 14 條行為進行處罰，或對「意圖在國外使用或促成其在國外被使用」而違反第 14 條之行為進行處罰[390]。

(五)、罰則

意圖在國外使用國家核心技術或促成國家核心技術在國外使用而違反 ITPA 第 14 條第 1 項第 1 款至第 3 款中之任何 1 款之規定者，將被判處 3 年以上有期徒刑，同時可處以 15 億韓元以下[391]之罰款[392]。

任何意圖在國外使用產業技術或促成產業技術在國外使用(不包

[387]ITPA 第 14 條第 1 項第 7 款之規定。
[388]ITPA 第 14 條第 1 項第 8 款之規定。
[389]ITPA 第 34 條之規定，詳細內容請見前揭註 385。
[390]吳宛芳，前揭註 344，頁 63。
[391]以 2024 年 2 月 9 日之匯率為計算基礎，1 新臺幣可兌換 42.53 韓元。
[392]ITPA 第 36 條第 1 項之規定。

含違反 ITPA 第 36 條第 1 項之人)而違反 ITPA 第 14 條第 1 項第 4 款以外之任何 1 款之規定者，將被判處 15 年以下之有期徒刑，或處以 15 以下億韓元之罰款[393]。

任何違反 ITPA 第 14 條第 1 項第 4 款、第 6 款、第 6-2 款及第 8 款以外之任何 1 款之規定者，將被判處 10 年以下之有期徒刑，或處以 10 億韓元以下之罰款[394]。

任何違反第 14 條第 4 款或第 8 款者，將被判處 3 年以下之有期徒刑，或處以 3 億韓元以下之罰款[395]。

違反 ITPA 第 36 條第 1 項至第 4 項之規定，而有因此取得財產者，其所取得之財產應被沒收；若沒有辦法完全或部分沒收該財產，則應收取相等價值之金額[396]。

任何違反 ITPA 第 34 條洩露或不當取用秘密者，將被判處 5 年以下之有期徒刑或暫停資格 10 年以下或罰處以不超過 5 千萬韓元以下之罰款[397]。

除此之外，ITPA 對於前開犯罪行為也有未遂犯[398]、預備犯、陰謀

[393]ITPA 第 36 條第 2 項之規定。
[394]ITPA 第 36 條第 3 項之規定。
[395]ITPA 第 36 條第 4 項之規定。
[396]ITPA 第 36 條第 5 項之規定。
[397]ITPA 第 36 條第 6 項之規定。
[398]ITPA 第 36 條第 7 項之規定。

犯[399]及法人刑事責任[400]之規定。惟在實務上，幾乎沒有預備犯或陰謀犯之案例，因為是在著手之前發生，很難發現及舉證[401]。

值得注意的是，在 2019 年 8 月 20 日 ITPA 修正前，非法於海外流漏產業技術或國家核心技術之刑事責任，均為 15 年以下之有期徒刑或處以 15 億韓元以下之罰款，惟考量到國家核心技術之重要性超過一般產業技術，遂將非法海外洩漏國家核心技術之部分，增加刑度至 3 年以上有期徒刑，並同時得處以 15 億韓元以下之罰款[402]。

產業技術侵害行為除了違反保密令罪[403]是告訴乃論罪之外，其他犯罪行為皆為非告訴乃論罪，顯現出產業技術保護法著重在國家法益保護之特徵[404]。

(六)、民事相關規定

如果一個侵害產業技術行為之人，已經損害或及將損害擁有產業技術之機構之商業利潤，該機構可以請求法院禁止或阻止其行為[405]。當擁有產業技術之機構根據前開規定提出請求時，得要求採取必要之

[399]ITPA 第 37 條之規定。
[400]ITPA 第 38 條之規定。
[401]吳宛芳，前揭註 344，頁 64。
[402]吳宛芳，前揭註 344，頁 64。
[403]ITPA 第 36-2 條規定：「1.無故在韓國境內或境外違反保密令之任何人，將被判處 5 年以下有期徒刑或處以 5 千萬韓元以下之罰款。2. 在未經提出保密令申請之人提出刑事投告訴的情況下，不得對違反前項之任何人提起公訴。」保密令則是產業技洩漏或侵害訴訟之當事人得依據 ITPA 第 22-4 條向法院請求核發。
[404]吳宛芳，前揭註 344，頁 64。
[405]ITPA 第 14-2 條第 1 項之規定。

措施來禁止或防止侵害行為，例如摧毀侵害行為之物品和移除以侵害行為為目的之設施[406]。

2019 年 8 月 20 日修正 ITPA 時，並新增了損害賠償及懲罰行賠償金之規定。任何人因違反 ITPA 第 14 條之規定而洩漏、侵害產業技術而對擁有產業技術之機構造成損害，應負損害賠償之責任[407]。如果發現產業技術侵害是故意行為，法院可以考慮相關因素諸如侵害者是否處於優越地位、故意程度或知曉會造成損害之程度、侵害所造成損害之程度、侵害者所獲得之利益、侵害之期間及頻率、侵害行為所受到之罰款、侵害者之財產狀況、侵害者之補救行為等後，最高可將損害賠償金額定為損害金額之 3 倍[408]。

(七)、施行現況

韓國在 ITPA 制定之後，仍然面臨海外技術外流案件逐年增加之情況。根據韓國 2014 年之研究，2005 年到 2013 年海外技術外流案件從 29 件增加到 49 件，快要增加 1 倍；其中，中小企業占外流案件之百分之 73；外流之技術領域，電機電子為最大宗，占百分之 35，再來則是機械、情報通訊、化學、生物技術等。產業技術洩漏方法變

[406]ITPA 第 14-2 條第 2 項之規定。
[407]ITPA 第 22-2 條第 1 項之規定。
[408]ITPA 第 22-2 條第 2 項之規定。

得越來越複雜、智能化，使 ITPA 受到挑戰[409]。

從營 UCPA 及 ITPA 之技術外流刑事偵查案件統計資料方面觀察，韓國檢察廳 2017 年到 2019 年之統計資料顯示[410]，UCPA 偵查案件 2017 年是 387(754 人)、2018 年是 426(920 人)、2019 年是 472(916 人)件。ITPA 案件 2017 年則是 16(37 人)、2018 年是 23(50 人)、2019 年是 9(70 人)件，可以觀察整體技術外流刑事偵查案件及涉案人數數量兩者整體均呈現逐漸增加之趨勢[411]。

經檢察官認定有犯罪嫌疑而起訴、聲請簡易判決或是緩起訴之狀況，UCPA 案件 2017 年是 56 人、2018 年是 78 人、2019 年是 57 人。ITPA 案件部分，2017 年是 7 人，2018 年是 12 人，2019 年也是 12 人，則是維持持平[412]。顯見韓國每年仍有相當數量之技術外流發生。

而依照韓國最高法院發布之數據觀察，2017 年至 2019 年 UCPA 及 ITPA 案件之 1 審判決結果，UCPA 案件總共 369 件當中有 85 件無罪，無罪比例約占全部案件百分之 23。ITPA 案件總共 34 件當中有 5 件無罪，無罪比例約占全部案件百分之 14。而一般韓國刑事案件 1 審無罪比利 2017 年是百分之 0.71、2018 年是百分之 0.79、2019 年是百分之 0.82，與技術外流之刑事案件之無罪比例相比，技術外流刑事案

[409]吳宛芳，前揭註 344，頁 81。
[410]因符合 ITPA 要件之產業技術同時也可能有符合營業秘密要件，故將兩者數據合併觀察，以了解技術外洩之刑事案件全貌。
[411]吳宛芳，前揭註 344，頁 81-82。
[412]吳宛芳，前揭註 344，頁 81-82。

件之無罪比例仍然非常高[413]。除此之外，技術外流案件之緩刑宣告刑度與其他重大刑事案件相比，稍嫌偏低，有鑑於國家核心技術外流到國外對於韓國經濟負面影響及對於受害業者之衝擊相較，ITPA 原先所規範之刑度顯得微不足道，韓國於 2019 年對於 ITPA 之修正當中，即將原本 15 年以下之有期徒刑，修正為 3 年以上有期徒刑，以求此修法能夠遏止國家核心技術外流至國外之犯罪行為[414]。

根據 MOTIE 於 2020 年提供給韓國國會之數據顯示，2015 年至 2020 年 8 月之間產業技術外流事件相關案件共有 121 件。其中，國家核心技術 29 件。國家核心技術牽涉之產業領域分別為造船、汽車 15 件、電氣電子 12 件、情報通訊 1 件、其它 1 件，百分之 90 以上集中在韓國半導體、造船及汽車產業。產業技術外流洩案件持續上升，可能是產業結構變化、勞動者離職率提高、核心技術人才待遇低、資訊儲存數位化等使得產業技術機密更易流出所造成[415]。

二、ITPA 與韓國「不正競爭防止及營業秘密保護法」之比較

韓國以專法 ITPA 保護產業技術與國家核心技術外，其營業秘密法則是以 UCPA 來保護，與美國、我國之立法模式並不相同，已如前

[413]營業秘密保護法的無罪率高之可能原因在於 UCPA 對營業秘密的要件之要求要有秘密管理性。韓國因此經數度修法，逐步放寬該要件，2018 年由「依相當努力維持秘密」修改為「依合理努力維持秘密」，再於 2019 年修改為「以秘密管理」即足以滿足該要件。

[414]吳宛芳，前揭註 344，頁 82-83。

[415]吳宛芳，前揭註 344，頁 83-84。

述，為何韓國要另立專法來處理關鍵技術之保護，可以從以下 ITPA 與 UCPA 之立法目的、規範對象、構成要件、保護範圍及客體、保護、管理之責任、侵害態樣、罰則等規範內容比較當中觀察兩者之差異及在國家鍵技術保護上所扮演之不同角色。

(一)、立法目的

韓國營業秘密之保護是由 UPCA 所規範，其立法目的為「透過防止不公平競爭之行為，如對公眾知悉之他人商標、商業名稱等之不正當使用，以及任何侵害他人營業秘密之行為，來維護健全之交易秩序。」[416]可知 UPCA 著重在交易秩序之維護，而與「防止產業技術不當洩漏及保護產業技術，以強化國家產業競爭力，並對國家安全及經濟發展做出貢獻」之 ITPA 第 1 條所規範之立法目的強調國家安全、防止產業技術外流、產業競爭力、經濟發展等目的不同，各司其職。

(二)、規範對象

ITPA 在立法之初就有將企業、大學、研究機構、專門機構等納入規範，以補足 UCPA 之不足。UCPA 起初僅針對企業所擁有之營業秘密才受到保護[417]，2013 年 7 月修法後才擴張營業秘密擁有者之主體到企業以外之個人、非營利機構上。目前兩者所保護之主體適用對象有

[416]UCPA 第 1 條之規定。
[417]2013 年 7 月修法前之 UCPA 第 18 條規定。

所重疊[418]。

(三)、構成要件

依據 UPCA 第 2 條第 2 款之規定,營業秘密係指「未為公眾所知,具有獨立的經濟價值,並且已經透過相當努力保持秘密之任何對於生產和銷售方法以及其他商業活動有用之技術或運營資訊。」所以,依據該條規定,要成為受 UPCA 保護之營業秘密,須具備(1)非公眾所知悉、(2)獨立經濟價值及(3)透過相當努力保持其秘密性等 3 要件。

在非公眾知悉方面,係指該項未公開之資訊不為多數不特定人所知悉,除了透過資訊持有人之外,無法被從一般管道取得[419]。ITPA 則是透過產業技術乃至國家核心技術的指定、公告,將該當技術納為保護、管理的範圍,並賦予相關人士保密責任,若因產業技術或國家核心技術不具備非公眾知悉之要件而未被納入保護範圍,反而會出現與立法目的不合之結果。舉例來說,某些產業技術可能因為部分內容有申請專利權而公開,若因此認為不具備非公眾知悉之要件而被排除在 ITPA 之外,即會發生此種狀況[420]。

在獨立經濟價值方面,UCPA 部分是指而是指營業秘密所有人透

[418]吳宛芳,前揭註 344,頁 68-69。
[419]章忠信,韓國營業秘密之保護法制,
http://www.copyrightnote.org/ArticleContent.aspx?ID=8&aid=3032(最後瀏覽日:02/25/2024)。
[420]吳宛芳,前揭註 344,頁 69。

過營業秘密的使用，會有相當競爭優勢；或是必須花費相當的費用或努力，才能取得或開發出來[421]。而 ITPA 之國家核心技術之經濟價值則是展現在其「在韓國和海外市場具有高技術和經濟價值，對相關產業具有高增長潛力，並且若在國外揭露的情況下可能對國家安全和國家經濟發展產生重大不利影響」之定義中，個別產業技術之價值則是透過個別相關法律來賦予產業技術價值。其中主要之差異在於，ITPA 要保護之價值是由 ITPA 及其他個別產業技術相關法律之政策目標所決定，與 UCPA 所保護之營業秘密所有人之 UCPA 保護的是私權，而 ITPA 則是著重在產業技術、國家核心技術之社會、國家利益之保護[422]。

在透過相當努力保持其秘密性要素方面，係指必須將相關資訊被標示或通知係秘密資訊，限制接觸人員或接觸方式，或要求接觸者承擔保密義務等，明確被認定係秘密資訊而被維護或管理者[423]。此要件之目的在於區別能自由使用與不能自由使用之資訊，維護健全之交易秩序，營業秘密擁有者可自由決定是否將其所掌握之資訊排除在營業秘密保護之外。另一方面，ITPA 則是透過政府來指定、公告特定技術為產業技術及國家核心技術，一旦被指定為產業技術或國家核心技術

[421]章忠信，韓國營業秘密之保護法制，
http://www.copyrightnote.org/ArticleContent.aspx?ID=8&aid=3032(最後瀏覽日期：02/25/2024)。
[422]吳宛芳，前揭註 344，頁 70。
[423]章忠信，韓國營業秘密之保護法制，
http://www.copyrightnote.org/ArticleContent.aspx?ID=8&aid=3032(最後瀏覽日期：02/25/2024)。

之後，技術擁有者需要採取必要之保護措施，處分權將會受到限制[424]。

在 2019 年 UCPA 修法前，UCPA 要求營業秘密擁有者必須以合理之努力維護資訊之秘密性，修法後稍微降低其門檻，改為要求擁有者把該資訊當作秘密來管理，在擁有者主張其資訊應該被 UCPA 保護時，不再需要證明有以合理之努力，亦可以符合此要件[425]。

(四)、保護範圍及客體

UCPA 保護之營業秘密，因為並未公告周知，掌握在營業秘密擁有者手中，通常都是有訴訟糾紛時，由法院來判斷其受保護之營業秘密之範圍，著重在事後之處罰。而 ITPA 之產業技術及國家核心技術都是相關機關首長依法律規定而指定、公告之技術，無法任意改變受保護之範圍，並且著重於事前之技術保護措施[426]。

再者，UCPA 保護之客體是「對該企業有用之商業秘密」，除了技術資訊之外，亦包括經營上之資訊。ITPA 法保護客體則是產業技術和國家核心技術，僅限於技術資訊，兩者保護之客體不完全相同[427]。

(五)、保護、管理之責任

UCPA 規範下之營業秘密，營業秘密擁有者可自由決定是否公開

[424]吳宛芳，前揭註 344，頁 71。
[425]章忠信，韓國營業秘密之保護法制，
http://www.copyrightnote.org/ArticleContent.aspx?ID=8&aid=3032(最後瀏覽日期：02/25/2024)。
[426]吳宛芳，前揭註 344，頁 71-72。
[427]吳宛芳，前揭註 344，頁 73。

或如何管理、保護營業秘密，並無法律規定要求擁有者具體上要如何保護或管理營業秘密，縱使受到侵害，也並無向主關機關報告之義務。然而，ITPA 對於產業技術及國家核心技術之擁有者之保護、管理責任有所規範[428]，違反者將有行政處罰[429]。

若產業技術或國家核心技術有受到侵害或有受侵害之虞者，擁有者有通報主管機關之義務[430]，違反者亦有行政處罰[431]。此外，若是未依照法律之規定獲得許可、或報備而禁行跨境收購、合併或出口，產業技術及國家核心技術之擁有者亦將負擔刑事責任[432]。

(六)、侵害態樣

在侵害態樣上，UCPA 與 ITPA 之立法體例雖有些許不同，但是內容則大致相同[433]。在修法的方向上，2019 年 7 月修正施行之營業秘密法，將侵害之態樣擴大至擅自流出、不回應返還、刪除之要求，與 ITPA

[428]ITPA 第 10 條之規定。
[429]ITPA 第 39 條第 1 項第 1 款之規定。
[430]ITPA 第 15 條第 1 項之規定。
[431]ITPA 第 39 條第 1 項第 2 款之規定。
[432]ITPA 第 14 條 5-7 款之規定及 ITPA 第 36 條之規定。吳宛芳，前揭註 346，頁 72。
[433]UCPA 第 18 條第 1、2 項規定:「1.明知在國外使用或讓他人在國外使用營業秘密，仍有下列各項行為者，處以 15 年以下有期徒刑或 15 億韓元以下之罰金。惟處以罰金之情況，若因違反行為所得財產利益之 10 倍金額超出 15 億韓元，則處以所得利益額之 2 至 10 倍之罰款。(1).以獲得不正當利益或讓營業秘密所有人受損害為目的，該當下列各款行為(a)、取得、使用或向第三者洩漏營業秘密行為。(b)、無理由將營業秘密流出其指定場所外之行為。(c)、經營業秘密所有人告知應刪除或返還，但卻持續持有的行為者。(2).竊取、欺騙、脅迫或其它不正當手段取得營業秘密之行為。(3).知悉其為第(1)項或第(2)項的營業祕密，卻仍取得或使用(依第 13 條第 1 項許可範圍使用為例外)該營業秘密的行為。2.第 1 項各款行為者處以 10 年以下有期刑期或 5 億韓元以下之罰金。惟處以罰金刑情況，若因違反行為所得財產利益之 10 倍金額超出 15 億韓元，則處以所得利益額之 2 倍以上 10 倍以下之罰金。」

第 14 條規範之侵害態樣雷同。比較大的差異點是在於 ITPA 針對國家核心技術之出口、跨境收購、合併等行為有所規範[434]，而 UCPA 則無此限制[435]，ITPA 之侵害態樣種類較多。

(七)、罰則

從刑度方面觀察，除了 ITPA 之國家核心技術海外流漏之刑度較高，為 3 年以上之有期徒刑外，UCPA 之營業秘密與 ITPA 之產業技術在國內外流之情況下，刑度均為 10 年以下之有期徒刑，而國外外流之狀況下則是 15 年以下之有期徒刑，兩者之刑度除罰金有些許差異外，相當一致[436]。論者即有認為，ITPA 主要目的是保護國家安全，而 UCPA 之目的在於維護健全之交易秩序，層次不同，而認為 ITPA 之刑罰應該更加嚴峻，目前之罰則規定仍有檢討空間[437]。

(八)、小結

從以上 ITPA 與 UCPA 之規範內容比較可以清楚得知，ITPA 與 UCPA 各自有不同的功能。UCPA 側重在防止不公平競爭及營業秘密擁有者私權之保護，以便維護健全交易秩序，而 ITPA 則是強調防止產業技術外流、維護國家安全、經濟發展、產業競爭力等公益面向，目的不

[434]ITPA 第 11 條、11-2 條之規定。
[435]吳宛芳，前揭註 344，頁 74。
[436]ITPA 第 36 條第 1-3 項之規定、UCPA 第 18 條第 1-2 項之規定。
[437]吳宛芳，前揭註 344，頁 74。

同。且兩者各自有不同之構成要件、保護範圍及保護客體。IPTA 規定產業技術、國家核心技術之擁有者有保護、管理之責任，侵害態樣也比 UPCA 之種類更多。UCPA 只能在侵害發生後，事後追究相關責任，ITPA 則是在事前就先設下各種防線，遏止產業技術、國家核心技術外流之發生。

肆、我國防範國家關鍵技術外流法制

在高科技時代，只要能擁有關鍵技術之研發能力，或是掌握智慧財產權之規則制定權，便能擠身強權，成為世界之領導者。智慧財產權之爭奪戰線，逐漸從過往的專利權、商標權，推進到對技術研發秘密之爭奪，中國對我國科技人才及技術之吸收範圍持續擴大，推動「中國製造 2025」計畫、千人計畫[438]、均係運用我國人才技術與管理能力[439]，希望在短時間內填補科技落差，減少研發成本及縮短研發時程。關鍵技術係科技產業之核心領域，我國科技人才及關鍵技術之外流，除了影響產業發展及兩岸產業鏈關係，商業投資上之滲透亦可能讓我國失去既有之產業優勢，產業失去競爭力，更對國家安全有重大影響。我國面對敵對勢力之威脅遠較其他國家嚴重，除了透過合法手段諸如

[438]在 2018 年前的 10 年間，中國根據該計畫以雄厚資金持續尋求吸納在國外訓練過的菁英科學家，美國認為該計畫對美國之利益及技術構成威脅，目前該計畫已由啟明計畫所取代。見聯合新聞網，https://udn.com/news/story/7332/7391850(最後瀏覽日：03/3/2024)。

[439]見中時新聞網，https://www.chinatimes.com/realtimenews/20210218004523-260409?chdtv(最後瀏覽日：03/3/2024)。

企業併購、商業投資、技術移轉、技術合作取得之外，亦可能以非法手段竊取我國企業之營業秘密[440]。

在此狀況下，防止我國產業關鍵技術不外流，便是至關重要之課題，惟我國針對關鍵技術之管控並無具體法律制度，亟需建立制度[441]。本文先前已經分別介紹美國、韓國在此方面之法制，為了能完整了解我國之相關法制，以下亦將從防止技術竊取、投資審查、出口管制等面向介紹此次國安法等相關法律修正前，我國在防範關鍵技術外流之相關法制。

一、營業秘密法制及其他防止技術竊取法制

(一)、營業秘密民事法律規範

技術之擁有者，如果符合我國營業秘密法第 2 條之規定：「本法所稱營業秘密，係指方法、技術、製程、配方、程式、設計或其他可用於生產、銷售或經營之資訊，而符合左列要件者：一、非一般涉及該類資訊之人所知者。二、因其秘密性而具有實際或潛在之經濟價值者。三、所有人已採取合理之保密措施者。」得受營業秘密法之保護[442]。

[440]趙晞華（2021），〈我國敏感科技技術外流之防制及處罰機制〉，《軍法專刊》， 67 卷 1 期，頁 19。
[441]王偉霖（2018），〈我國無形技術外流管控制度之檢討〉，《華岡法萃》， 64 期，頁 69。
[442]王偉霖，前揭註 441，頁 70。

若技術若符合營業秘密法之定義，依同法第 10 條之規定，若有營業秘密遭到侵害之情況，諸如以不正當方法取得營業秘密者；知悉或因重大過失而不知其為前款之營業秘密，而取得、使用或洩漏者；取得營業秘密後，知悉或因重大過失而不知其為第 1 款之營業秘密，而使用或洩漏者；因法律行為取得營業秘密，而以不正當方法使用或洩漏者；依法令有守營業秘密之義務，而使用或無故洩漏者，得依同法第 11 至第 13 條之規定，請求損害賠償、排除或防止侵害、銷毀侵害行為做成之物或專供侵害所用之物或其他適當處置[443]。

(二)、營業秘密刑事法律規範

起初我國營業秘密法僅有民事規範，營業秘密法之定位為民事特別法，對於侵害營業秘密之刑事責任，則回歸到刑法竊盜罪、侵占罪、背信罪或洩漏業務上知悉之工商秘密罪處理。後來隨著國際商業活動日漸興盛，產業界侵害營業秘密案件層出不窮，諸如員工「帶槍投靠」新公司、侵害者以不法手段竊取他人營業秘密、來自他國之經濟間諜等情形，除了損害我國產業之國際競爭力外，亦可能威脅國家安全，營業秘密刑罰化之問題才逐漸受到重視，我國並於 102 年增訂侵害營業秘密之刑事責任[444]。

[443]王偉霖，前揭註 441，頁 70。
[444]林志潔、羅于盛（2023），〈十年磨一劍：從營業秘密的刑事處罰 到國家安全法的修法〉，《全國律師》，27 卷第 4 期，頁 21。

營業秘密法第 13 條之 1 為一般侵害營業秘密罪[445]，為基本侵害態樣，其刑度最輕，且為告訴乃論[446]；同法第 13 條之 2[447]為一般侵害營業秘密域外使用罪，建立在一般侵害營業秘密罪之基礎上，因有在域外使用之意圖，對於我國產業競爭力之影響更嚴重，因而在刑度上有所加重；同法第 13 條之 3 除了第 1 項是規定一般侵害營業秘密罪為告訴乃論之外，第 2 項[448]並規定對於共犯之 1 人告訴或撤回告訴者，其效力不及於其他共犯，稱之為「窩裡反條款」，有助於檢警調機關對於犯罪之打擊；同法第 13 條之 4[449]則為「法人刑事責任兩罰制」規定，除了行為人受處罰外，行為人背後之組織亦應受罰，因為其監督不力，企業組織受罰應從屬於行為人之犯罪行為，以行為人有犯罪行為為前提。兩罰制之設立係為了督促企業對營業秘密之保護及正當商

[445]我國營業秘密法第 13 條之 1 規定：「意圖為自己或第三人不法之利益，或損害營業秘密所有人之利益，而有下列情形之一，處五年以下有期徒刑或拘役，得併科新臺幣一百萬元以上一千萬元以下罰金：一、以竊取、侵占、詐術、脅迫、擅自重製或其他不正方法而取得營業秘密，或取得後進而使用、洩漏者。二、知悉或持有營業秘密，未經授權或逾越授權範圍而重製、使用或洩漏該營業秘密者。三、持有營業秘密，經營業秘密所有人告知應刪除、銷毀後，不為刪除、銷毀或隱匿該營業秘密者。四、明知他人知悉或持有之營業秘密有前三款所定情形，而取得、使用或洩漏者。前項之未遂犯罰之。」
科罰金時，如犯罪行為人所得之利益超過罰金最多額，得於所得利益之三倍範圍內酌量加重。

[446]我國營業秘密法第 13 條之 3 第 1 項規定：「第十三條之一之罪，須告訴乃論。」

[447]我國營業秘密法第 13 條之 2 規定：「意圖在外國、大陸地區、香港或澳門使用，而犯前條第一項各款之罪者，處一年以上十年以下有期徒刑，得併科新臺幣三百萬元以上五千萬元以下之罰金。前項之未遂犯罰之。科罰金時，如犯罪行為人所得之利益超過罰金最多額，得於所得利益之二倍至十倍範圍內酌量加重。」

[448]我國營業秘密法第 13 條之 3 第 2 項規定：「對於共犯之一人告訴或撤回告訴者，其效力不及於其他共犯。」

[449]我國營業秘密法第 13 條之 4 規定：「法人之代表人、法人或自然人之代理人、受雇人或其他從業人員，因執行業務，犯第十三條之一、第十三條之二之罪者，除依該條規定處罰其行為人外，對該法人或自然人亦科該條之罰金。但法人之代表人或自然人對於犯罪之發生，已盡力為防止行為者，不在此限。」

業使用管理，企業可能是被害人或加害人，企業除了要完善自身營業秘密之保護外，對於員工之管理監督亦應注意，以免受到牽連[450]。

109 年同法又增訂第 13 條之 5、第 14 條之 1 到 14 條之 4。第 13 條之 5 規定外國法人可以成為告訴主體，提出民刑事訴訟[451]；第 14 條之 1 到 14 條之 4 則是關於偵查保密令之規範，第 14 條之 1 規定檢察官偵查中得職權核發偵查保密令給案件中之相關人士[452]；第 14 條之 2 規定偵查保密令之相關程序要件[453]；第 14 條之 3 規範偵查保密令之撤銷、變更及救濟程序[454]；第 14 之 4 條則是規定違反偵查保密令之

[450]林志潔、羅于盛，前揭註 444，頁 22。

[451]我國營業秘密法第 13 條之 5 規定：「經認許之外國法人，就本法規定事項得為告訴、自訴或提起民事訴訟。」

[452]我國營業秘密法第 14 條之 1 規定：「檢察官偵辦營業秘密案件，認有偵查必要時，得核發偵查保密令予接觸偵查內容之犯罪嫌疑人、被告、被害人、告訴人、告訴代理人、辯護人、鑑定人、證人或其他相關之人。受偵查保密令之人，就該偵查內容，不得為下列行為：一、實施偵查程序以外目的之使用。二、揭露予未受偵查保密令之人。前項規定，於受偵查保密令之人，在偵查前已取得或持有該偵查之內容時，不適用之。」

[453]我國營業秘密法第 14 條之 2 規定：「偵查保密令應以書面或言詞為之。以言詞為之者，應當面告知並載明筆錄，且得予營業秘密所有人陳述意見之機會，於七日內另以書面製作偵查保密令。前項書面，應送達於受偵查保密令之人，並通知營業秘密所有人。於送達及通知前，應給予營業秘密所有人陳述意見之機會。但已依前項規定，給予營業秘密所有人陳述意見之機會者，不在此限。偵查保密令以書面為之者，自送達受偵查保密令之人之日起發生效力；以言詞為之者，自告知之時起，亦同。偵查保密令應載明下列事項：一、受偵查保密令之人。二、應保密之偵查內容。三、前條第二項所列之禁止或限制行為。四、違反之效果。」

[454]我國營業秘密法第 14 條之 3 規定：「偵查中應受保密之原因消滅或偵查保密令之內容有變更必要時，檢察官得依職權撤銷或變更其偵查保密令。案件經緩起訴處分或不起訴處分確定者，或偵查保密令非屬起訴效力所及之部分，檢察官得依職權或受偵查保密令之人之聲請，撤銷或變更其偵查保密令。檢察官為前二項撤銷或變更偵查保密令之處分，得予受偵查保密令之人及營業秘密所有人陳述意見之機會。該處分應以書面送達於受偵查保密令之人及營業秘密所有人。案件起訴後，檢察官應將偵查保密令屬起訴效力所及之部分通知營業秘密所有人及受偵查保密令之人，並告知其等關於秘密保持命令、偵查保密令之權益。營業秘密所有人或檢察官，得依智慧財產案件審理法之規定，聲請法院核發秘密保持命令。偵查保密令屬起訴效力所及之部分，在其聲請範圍內，自法院裁定確定之日起，失其效力。案件起訴後，營業秘密所有人或檢察官未於案件繫屬法院之日起三十日內，向法院聲請秘密保持命令者，法院得依受偵查保密令之人或檢察官之聲請，撤銷偵查保密令。偵查保密令屬起訴效力所及之部分，在法院裁定予以撤銷之範圍內，自法院裁定確定之日起，失其效力。法院為前項裁定前，應先徵詢營業秘密所有人及檢察官之意見。前項裁定並應送達營業秘密所有人、受偵查保密令之人及檢察官。受偵查保密令之人或營業秘密所有人，對於第一項及第二項檢察官之處分，得聲明不服；檢察官、受偵查保密令之人或營業秘密所有人，對於第五項法院之裁定，得抗告。前項聲明不服及

刑事責任[455]。

(三)、其他防止技術竊取法制

1.刑法

我國刑法第 317 條規定，依法令或契約有守因業務知悉或持有工商秘密之義務而無故洩漏之者，處 1 年以下有期徒刑、拘役或 3 萬元以下罰金；同法第 318 條規定，公務員或曾任公務員之人，無故洩漏因職務知悉或持有他人之工商秘密者，處 2 年以下有期徒刑、拘役或 6 萬元以下罰金；同法第 318 條之 1 規定，無故洩漏因利用電腦或其他相關設備知悉或持有他人之秘密者，處 2 年以下有期徒刑、拘役或 1 萬 5 千元以下罰金；同法第 318 條之 2 規定，利用電腦或其相關設備犯第 316 條至第 318 條之罪者，加重其刑至 2 分之 1；同法第 319 條規定，前開罪名為告訴乃論。

2.國家機密保護法

國家機密保護法第 32 條第 1 項規定，洩漏或交付經依本法核定之國家機密者，處 1 年以上 7 年以下有期徒刑；第 2 項規定，洩漏或

抗告之程序，準用刑事訴訟法第四百零三條至第四百十九條之規定。」

[455]我國營業秘密法第 14 條之 4 規定：「違反偵查保密令者，處三年以下有期徒刑、拘役或科或併科新臺幣一百萬元以下罰金。於外國、大陸地區、香港或澳門違反偵查保密令者，不問犯罪地之法律有無處罰規定，亦適用前項規定。」

交付前項之國家機密於外國、大陸地區、香港、澳門、境外敵對勢力或其派遣之人者，處 3 年以上 10 年以下有期徒刑；第 3、4、5 項則是分別針對過失犯、未遂犯、預備犯、陰謀犯之規定；第 6 項規定，犯前 5 項之罪，所洩漏或交付屬絕對機密[456]者，加重其刑至 2 分之 1。

3. 國家安全法

原國安法第 2 條之 1 規定[457]，人民不得為外國、大陸地區、香港、澳門、境外敵對勢力或其派遣之人為下列行為：一、發起、資助、主持、操縱、指揮或發展組織。二、洩漏、交付或傳遞關於公務上應秘密之文書、圖畫、影像、消息、物品或電磁紀錄。三、刺探或收集關於公務上應秘密之文書、圖畫、影像、消息、物品或電磁紀錄。

原國安法第 5 條之 1[458]第 1 項規定，意圖危害國家安全或社會安定，為大陸地區違反第 2 條之 1 第 1 款規定者，處 7 年以上有期徒刑，得併科新臺幣 5 千萬元以上 1 億元以下罰金；為大陸地區以外違反第 2 條之 1 第 1 款規定者，處 3 年以上 10 年以下有期徒刑，得併科新臺幣 3 千萬元以下罰金；第 2 項規定，違反第 2 條之 1 第 2 款規定者，處 1 年以上 7 年以下有期徒刑，得併科新臺幣 1 千萬元以下罰

[456]國家機密保護法第 4 條規定：「國家機密等級區分如下：一、絕對機密 適用於洩漏後足以使國家安全或利益遭受非常重大損害之事項。二、極機密 適用於洩漏後足以使國家安全或利益遭受重大損害之事項。三、機密 適用於洩漏後足以使國家安全或利益遭受損害之事項。」

[457]後來於 111 年 5 月 20 日修法時變更條次為第 2 條，並有部分文字修正。

[458]後來於 111 年 5 月 20 日修法時變更條次為第 7 條，並有部分文字修正。

金；第 3 項規定，違反第 2 條之 1 第 3 款規定者，處 6 月以 5 年以下有期徒刑，得併科新臺幣 3 百萬元以下罰金；第 4 項是規定第 1 至 3 項之未遂犯；第 5 項是規定第 2 項之過失犯；第 6、7 項是規定自首、自白之相關規定；第 8、9 項則是關於沒收之規定。

4. 通訊保障及監察法

通訊保障及監察法第 5 條第 1 項第 16 款之規定，將營業秘密法第 13 條之 2 之一般侵害營業秘密域外使用罪納入得為通訊監察之案件。惟營業秘密法第 13 條之 1 之一班侵害營業秘密罪則不在此列，導致蒐證不易[459]。

5. 國家情報工作法

根據國家情報工作法第 7 條第 1 項第 4 款之規定，營業秘密得為得為情報機關蒐集、研析、處理、運用之範圍[460]。惟尚有許多疑義仍有討論空間。諸如其義務及界限、是否有過於寬鬆及如何運用因此

[459]趙晞華，前揭註 440，頁 24。

[460]國家情報工作法第 7 條規定：「情報機關應就足以影響國家安全或利益之下列資訊進行蒐集、研析、處理及運用：一、涉及國家安全或利益之大陸地區或外國資訊。二、涉及內亂、外患、洩漏國家機密、外諜、敵諜、跨國性犯罪或國內外恐怖份子之滲透破壞等資訊。三、其他有關總體國情、國防、外交、兩岸關係、經濟、科技、社會或重大治安事務等資訊。四、為外國勢力或境外敵對勢力以刺探、收集、竊取、洩漏、交付或其他不正當方法取得之營業秘密資訊。前項資訊之蒐集，必要時得採取秘密方式為之，包括運用人員、電子偵測、通（資）訊截收、衛星（光纖）偵蒐（照）、跟監、錄影（音）及向有關機關（構）調閱資料等方式。情報機關執行通訊監察蒐集資訊時，蒐集之對象於境內設有戶籍者，其範圍、程序、監督及應遵行事項，應以專法定之；專法未公布施行前，應遵守通訊保障及監察法等相關法令之規定。外國人或大陸地區人民來臺從事與許可停留、居留目的不符之活動或工作者，主管機關得協調內政部警政署、內政部移民署或法務部調查局，對其實施查（約）訪。拒絕接受查（約）訪者，移請權責機關依法令處理。」

獲得之情資[461]。

同法第 18 條第 1 項規定，情報機關於獲取足以影響國家安全或利益之資訊時，應即彙送主管機關處理；其涉及社會治安之重大事件或重大災難者，除依法處理外，應即彙送主管機關。惟應該如何界定「足以影響國家安全」之範圍，及主管機經濟部應如何處理，亦有疑義[462]。

此外，同法第 22 條係規定有關情報機關從事反制間諜工作及調閱涉嫌間諜行為之人時之相關流程。然而，是否可因涉嫌人有刺探營業秘密之行為，即認定其從事間諜行為，而採行反制間諜行為或適用情報機關之移送程序，或是需要營業秘密擁有者提出告訴，尚值商榷[463]。

6. 積體電路布局保護法

積體電路布局保護法第 4 條規定，電路布局專責機關及前條第 2 項後段所規定之公益法人或團體所屬人員，對於職務或業務上所知悉或持有之秘密不得洩漏[464]。

---

[461]趙晞華，前揭註 440，頁 24。
[462]趙晞華，前揭註 440，頁 24。
[463]趙晞華，前揭註 440，頁 24。
[464]根據經濟部之資料顯示，積體電路布局保戶申請案件逐年降低，近 3 年都不到 100 件，主要原因是因為廠商近來都以專利或營業秘密來保護技術，走布局登記者比較少，重要性在降低，但是仍有部分廠商使用此種方式。見中時新聞網，
https://tw.sports.yahoo.com/news/%E7%A9%8D%E9%AB%94%E9%9B%BB%E8%B7%AF%E5%B8%83%E5%B1%80%E7%94%B3%E8%AB%8B-%E9%80%A33%E5%B9%B4%E4%B8%8D%E5%88%B0%E7%99%BE%E4%BB%B6-201000338.html

(四)、問題所在

我國在 85 年年即制定營業秘密法，102 年並因應跨境違法行為即對產業之嚴重損害而將侵害營業秘密行為予以刑罰化，109 年為了避免營業秘密之 2 度外流之風險，增訂偵查保密令之規定。營業秘密法著重在營業秘密擁有者之私權保護，惟涉及國家關鍵技術者，參酌美國、韓國之立法意旨，應受到國家之強制保護。然而，若管制過於嚴格，又可能損害產業之發展。我國雖已有營業秘密法與前述之相關防止技術竊取法律規定，惟營業秘密之侵害類型甚多，相關法規不足以完整規範，且刑度亦屬偏低，不足以有效保護營業秘密[465]。

此外，營業秘密法第 13 條之 1 之一般侵害營業秘密罪，各款之手段與不法程度均不同，卻未依不同等級之營業秘密而區分不同之法定刑，若涉及國家安全或國家整體經濟秩序，卻任由營業秘密擁有者自行決定是否提出告訴，等於是將國家安全放置於私法自治之談判桌上，曝露出此罪之缺陷。又國家機密與國防以外秘密之保護，雖然有國家機密保護法、刑法有相應之規範即刑責，但是卻無針對「國家關鍵技術」保護之規範[466]。

(最後瀏覽日期：03/10/2024)。

[465]趙晞華，前揭註 440，頁 27-28。

[466]趙萃文（2022），〈論國安法及兩岸條例修正建構之「國家核心關鍵技術營業秘密保護」法制〉，《軍法專刊》， 68 卷 6 期，頁 51-52。

再者,營業秘密法第 13 條之 2 雖名為域外侵害營業秘密之處罰,但是除了除「意圖在外國、大陸地區、香港或澳門使用」之主觀要件外,其餘構成要件皆與同法第 13 條之 1 相同,有論者認本條並非域外侵害營業秘密之立法模式,因為該條之構成要件並非針對域外使用之行為,本條事實上只能處罰意圖於外國、大陸地區、香港或澳門使用,而於我國境內實施侵害營業秘密行為之人。且本條並非最輕本刑 3 年以上有期徒刑之罪,因此本條罪名並不及於意圖在外國、大陸地區、香港或澳門使用,但於我國境外犯本罪之行為人[467],亦無法處罰國際經濟間諜犯罪[468]。

二、外國投資審查法制

(一)、外國人投資條例

外國人投資條例目的在於規範外國人在我國境內之投資、保障、限制及處理[469],並禁止投資人投資下列事業:一、對國家安全、公共秩序、善良風俗、國民健康有不利影響之事業;二、法律禁止投資之事業[470]。投資人申請投資於法律或基於法律授權訂定之命令而限制投

[467]我國刑法第 7 條規定:「本法於中華民國人民在中華民國領域外犯前二條以外之罪,而其最輕本刑為三年以上有期徒刑者,適用之。但依犯罪地之法律不罰者,不在此限。」
[468]王偉霖,前揭註 441,頁 100。
[469]外國人投資條例第 1 條之規定。
[470]外國人投資條例第 7 條第 1 項之規定。

資之事業，應取得目的事業主管機關之許可或同意[471]。

根據「僑外投資負面表列－禁止及限制僑外人投資業別項目」[472]之規定，禁止投資之項目包含軍事、國防相關產業、陸上運輸、無線電事業等；限制投資項目則涵蓋農牧業、化學原料製造、軍事、公共基礎設施、水上傳播運輸、自來水事業、電信傳播等產業[473]。

(二)、臺灣地區及大陸地區人民關係條例

依臺灣地區及大陸地區人民關係條例(簡稱兩岸條例)第35條之規定，臺灣地區人民、法人、團體或其他機構，經經濟部許可，得在大陸地區從事投資或技術合作；其投資或技術合作之產品或經營項目，依據國家安全及產業發展之考慮，區分為禁止類及一般類。根據「在大陸地區從事投資或技術合作審查原則」[474]第2點規定，禁止類包含基於國際公約、國防、國家安全需要、重大基礎建設及產業發展考量，禁止前往大陸投資之產品或經營項目；一般類則是凡不屬禁止類之產品或經營項目，歸屬為一般類[475]。

兩岸條例第40條之1第1項規定，大陸地區營利事業非經許可，非經主管機關許可，並在臺灣地區設立分公司或辦事處，不得在臺從

[471]外國人投資條例第7條第2項之規定
[472]見經濟部網站，https://law.moea.gov.tw/LawContent.aspx?id=GL000176#lawmenu(最後瀏覽日期：03/11/2024)。
[473]趙晞華，前揭註440，頁25。
[474]見經濟部網站，https://law.moea.gov.tw/LawContent.aspx?id=GL000881(最後瀏覽日：03/12/2024)。
[475]趙晞華，前揭註440，頁25。

事業務活動[476]。同法第 93 條之 2 第 1 項之規定，違反第 40 條之 1 第 1 項規定，未經許可而為業務活動者，處 1 年以下有期徒刑，拘役或科或併科罰金，並自負民事責任；行為人有二人以上者，連帶負民事責任，並由主管機關禁止其使用公司名稱[477]。

兩岸條例第 73 條規定，大陸地區人民、法人、團體、其他機構或其於第三地區投資之公司，非經主管機關許可，不得在臺灣地區從事投資行為。另依「大陸地區人民來臺投資許可辦法」第 4 條規定，投資行為包含持股達百分之 10、設立公司、合夥、或提供 1 年期以上

[476]111 年 5 月 20 號修法時，增訂「大陸地區之營利事業於第三地區投資之營利事業」之文字，修正理由如下：「第一項前段規範目的為要求大陸地區之營利事業如欲在臺從事業務活動，均須經主管機關許可，俾利行政管理，是以，大陸地區之營利事業透過第三地區投資之營利事業在臺從事業務活動，本即為第一項規範意旨所涵蓋，惟鑒於各界關切陸資逐漸透過外商（含香港、澳門）公司之名義繞道來臺投資，可能引發我國政治、經濟、社會及文化上正常發展之疑慮，又為有效遏阻大陸地區之營利事業透過臺灣在地協力者或繞道第三地區投資之營利事業，在臺從事挖角高科技人才及其他不當行為，為期明確，爰參考現行第七十三條第一項規定，修正第一項前段規定，除原「大陸地區之營利事業」外，增訂「大陸地區之營利事業於第三地區投資之營利事業」，非經主管機關許可，並在臺灣地區設立分公司或辦事處，亦不得在臺從事業務活動。」

[477]111 年 5 月 20 修法時，新增將本人名義提供或容許前款之人使用而為業務活動之類型及提高刑度。修正理由如下：「一、近來，面對大陸地區營利事業不斷透過臺灣地區之在地協力者或第三地區公司為其進行人才招募、面試、簽約、洽談薪資、銷售等業務活動，並積極透過各種手段，例如經許可來臺投資卻從事與許可目的不符之行為、未經許可直接在臺僱用員工蒐集並竊取營業秘密、藉由獵人頭公司在臺挖角以不當方式誘拉我各產業之人才，以規避我國法律規範，已嚴重影響我國家安全及經濟利益，爰修正第一項規定，說明如下：(一)鑒於臺灣地區人民、法人或團體出借名義予大陸地區營利事業，幫助其在臺從事業務活動，目前實務均係以共同實施或幫助協力論罪，為彰顯該行為本身具有高度可罰性，爰增訂第一項第二款，明確獨立之構成要件類型，並配合第九十三條之一之修正，明定將本人名義提供或容許他人使用而為業務活動者，應依本條予以處罰。至行為人無論以本人名義或以他人名義違反第四十條之一第一項規定者，係依第一項第一款規定處罰之，併予敘明。(二)又大陸地區營利事業透過迂迴方式規避本條規定而在臺從事業務活動之情形十分猖獗，近來更特別針對我高科技產業進行人才挖角，企圖達成我消彼長之磁吸效果，此舉已嚴重影響我經濟秩序及國家利益。然實務判決依原規定僅得判處一年以下有期徒刑或得易科罰金，或處以緩刑，情重罰輕，嚇阻效果有限。基於國家整體利益，保護我產業發展，並有效遏阻違法行為，爰修正第一項規定，將其刑責提高至『三年以下有期徒刑、拘役或科或併科新臺幣一千五百萬元以下罰金』，以維護交易秩序及國家安全。」

貸款等[478]。同辦法第 8 條規定，投資人所為投資之申請，有如下情況時：一、經濟上具有獨占、寡占或壟斷性地位；二、政治、社會、文化上具有敏感性或影響國家安全；三、對國內經濟發展或金融穩定有不利影響，得限制或禁止之。其投資之經營有前開情事之一者，得撤銷或廢止其投資。是否影響國家安全，以經濟部投資審議委員會[479]公告之「具敏感性或國安(含資安)疑慮之業務範疇」為判斷標準，其公布事業範圍包含能源、水資源、通訊、傳播、交通、金融與銀行、緊急救援與醫院、中央與地方政府機關、科技園區與工業區等部門之資安、管理、控制等相關系統[480]。

(三)、問題所在

就外來投資部分，我國向來是由經濟部投資審議委員會進行審核，除了中國來我國投資需要受到兩岸條例、大陸地區人民來臺投資許可辦法限制，且在投資審議時須先參考「具敏感性或國安（含資安）疑慮之業務範疇」，其他外國人投資我國時，僅須受到外國人投資條例限制，而該條例規定，除了對國家安全、公共秩序、善良風俗、國民

[478]大陸地區人民來臺投資許可辦法第 4 條第 1 項規定：「投資人依本辦法規定應申請許可之投資行為如下：一、持有臺灣地區公司、獨資、合夥或有限合夥事業之股份或出資額。但不包括單次且累計投資均未達百分之十之上市、上櫃及興櫃公司股份。二、在臺灣地區設立分公司、獨資、合夥或有限合夥事業。三、對前二款所投資事業提供一年期以上貸款。四、以契約或其他方式對臺灣地區獨資、合夥、有限合夥事業或非上市、上櫃或興櫃公司具有控制能力。五、前條第二項第三地區投資之公司併購臺灣地區非上市、上櫃或興櫃公司之營業或財產。」

[479]於 112 年 9 月 26 日改制成為經濟部投資審議司。見經濟部網站，https://dir.moea.gov.tw/about.view?type=atIo&lang=ch(最後瀏覽日期：03/15/2024)。

[480]趙晞華，前揭註 440，頁 26。

健康有不利影響之事業、法律禁止投資之業、以及經濟部公告禁止及限制僑外人投資業別項目外，其餘事業均屬准許投資之範疇。也就是說，我國既有之投資審議法制除了針對中國之外，似乎無法充分預防外資投資我國廠商而致技術外流之情況[481]。

由我國之投資審查相關法規觀察，可知我國對於關鍵技術管制之規範體系，此部分仍有法規上之漏洞，有檢討改進之空間。論者認為，在未來之設計審查制度上，可以參照歐美國家主要以國家安全或經濟安全為審查原則，作為啟動審查之因素，對於外資投資我國企業所設技術保護機制做全面性之規範[482]。

值得注意的是，美國在修訂 FIRRMA 時，亦有批評密度過高之審查機制將會破壞既有之審查制度，同時將損害產業追蹤關鍵技術之能力，在設計相關法制時，亦應注意此問題，方能促進我國關鍵技術保護體制之完善[483]。

三、出口管制法制

我國雖無法成為為防止武器擴散條約之締約國或相關國際組織如禁止化學武器組織（Organization for the Prohibition of Chemical Weapons, OPCW）之成員，但是為了確保國家安全，與國際

[481]王偉霖，前揭註 441，頁 102。
[482]王偉霖，前揭註 441，頁 102。
[483]王偉霖，前揭註 441，頁 103。

社會合作共同防止軍品及軍民兩用貨品及技術出口後不被用於不法用途，自願的履行國際協定，善盡國際責任。相關國際規範包括：聯合國安理會防止供應北韓、伊朗或其他恐怖組織等發展核武、彈道飛彈或大規模毀滅性武器之物品相關決議、核供應國集團、澳洲集團、導彈技術管制協議、瓦賽納協議及禁止化學武器公約等國際條約。前開國際規範之主要目的在防止核生化學武器之擴散[484]。

除此之外，我國出口管制法規之目的也包含藉由建立出口管制制度、協助業者做好出口管控，使得外國高科技貨品進口我國後不至於外流至危險國家或份子手中，也避免違反他國及國際出口管制規範。最後，建構完善之出口管制體系有助於我商引進外國高科技產品，有助於促進我國產業升級、增進國家經濟利益[485]。

我國並無出口管制專法，主要是依據「貿易法」之相關規定，以及貿易法第 13 條第 6 項授權主關機關經濟部制定「戰略性高科技貨品輸出入管理辦法」及依據同法第 13 條第 3 項之相關公告諸如「戰略性高科技貨品種類、特定戰略性高科技貨品種類及輸出管制地區」、「戰略性高科技貨品管理清單」及「戰略性高科技貨品出口實體管理名單」，共同建構出我國之出口管制體系[486]。

[484]楊健弘（2023），〈臺美出口管制法規體系之比較研析－以軍民兩用貨品及技術為核心〉，《月旦法學雜誌》，332 期，頁 202。
[485]楊健弘，前揭註 484，頁 202。
[486]楊健弘，前揭註 484，頁 202。

(一)、貿易法

貿易法所稱之貿易，是指「貨品」之輸出入行為及有關事項，「貨品」包含其上所附屬之商標權、專利權、著作權及其他以立法保護之智慧財產權[487]。若有危害國家安全或對公共安全之保障有妨害時，主管機關得暫停特定國家或地區或特定貨品之輸出入或採取其他必要措施[488]。惟貿易法僅規範貨品本身及其上之智慧財產權，「關鍵技術」本身並非附屬在貨品上，不在其管制之範疇內[489]。

(二)、戰略性高科技貨品輸出入管理辦法

部分高科技貨品，除了一般商業用途外，亦有軍事用途，我國為了善盡國際責任及保護我國人民出口利益，主管機關經濟部依據貿易法第 13 條第 6 項訂定「戰略性高科技貨品輸出入管理辦法」，執行戰略性高科技貨品輸出入管理[490]，包括：核能物質與設施、特殊材料

[487]貿易法第 2 條之規定。
[488]貿易法第 6 條第 1 項第 2 款之規定。
[489]趙晞華，前揭註 440，頁 26。
[490]貿易法第 13 條規定：「為確保國家安全，履行國際合作及協定，加強管理戰略性高科技貨品之輸出入及流向，以利引進高科技貨品之需要，其輸出入應符合下列規定：一、非經許可，不得輸出。二、經核發輸入證明文件者，非經許可，不得變更進口人或轉往第三國家、地區。三、應據實申報用途及最終使用人，非經許可，不得擅自變更。輸往管制地區之特定戰略性高科技貨品，非經許可，不得經由我國通商口岸過境、轉口或進儲保稅倉庫、物流中心及自由貿易港區。前二項貨品之種類、管制地區，由主管機關公告，並刊登政府公報及主管機關所屬網站，免費供民眾閱覽。違反第二項規定之特定戰略性高科技貨品，主管機關得予扣留，並依本法或相關法律裁處。除已依法裁處沒入者外，主管機關應予退運。前項之扣留，主管機關得委託海關執行之。第一項及第二項許可之申請條件與程序、輸出入、過境、轉口或進儲保稅倉庫、物流中心、自由貿易港區之管理、輸出入用途與最終使用人之申報、變更與限制、貨品流向與用途之稽查及其他應遵行事項之辦法，由主管機關定之。」

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、航太與推進系統等 10 大類。若未經許可而出口此 10 大類貨品[491]，將因違反貿易法第 27、27-1、27-2 條之規定而有有期徒刑、拘役、科或併科罰金或罰鍰、停止輸出入貨品或撤銷進出口廠商登記等處罰[492]。

(三)、問題所在

貿易法針對戰略性高科技貨品輸出加強管制，著重在實體出口貨品管控，對於軟體或技術層面審查不足[493]，且出口審查單位為經濟部國際貿易局貿易安全與管理小組[494]，工作權責及執法能量有限[495]。針對出口管制部分,有論者認為宜將貿易法規範對象擴大至技術、軟體、設計等虛擬層面，管制項目應自戰略性高科技貨品，擴張至關鍵基礎

[491]見經濟部國際貿易署網站，https://www.trade.gov.tw/Pages/Detail.aspx?nodeID=4433&pid=725764 (最後瀏覽日：03/18/2024)。

[492]趙晞華，前揭註 440，頁 27。

[493]另國安法、國家機密保護法、兩岸人民關係條例及其子法，及科學技術基本法及其子法與相關行政規則對技術輸出雖有規範，然若該技術不屬公務上機密事項，未經核定屬國家機密，且無政府補助者，可能也不受相關法律拘束。雖我國科技部(2022 年 7 月 27 日改制為國家科學及技術委員會)為另有制定「政府資助敏感科技研究計畫安全管制作業手冊」，與我國廠商以契約方式約定敏感科技之管理，然此手冊適用者僅為政府相關部門以補助、委辦或出資等方式之研發成果，不包含未經政府補資助之技術。見王偉霖，前揭註 434，頁 101。

[494]2023 年 9 月 26 日改制成為經濟部國際貿易署貿易管理組貿易安全管理科。見經濟部國際貿易署網站，https://www.trade.gov.tw/Pages/Detail.aspx?nodeID=4167&pid=698921(最後瀏覽日：03/18/2024)。

[495]因出口管制涉及高度工業及產品製程之專業性，故美國出口管制主管機關為 BIS，而非貿易部門主管。BIS 轄下具有多個辦公室，且編制有律師及工程師等專業人員，負責產品鑑定、許可證審查及核發工作。我國出口管制法規之主管機關為經濟部，而業務執行單位為經濟部國際貿易局貿易管理辦公室(改制前)。然而，貿易管理辦公室人數在 10 人以下，並無判斷高科技貨品之專業能力，必須委外進行鑑定，故量能難以與美國 BIS 之龐大組織與專業人士相提並論。因此，除了另立專法外，成立跨部會之出口管制專責單位（如專案辦公室），甚至獨立機關，增加人力配置並納入法律、資訊工程、產業分析等專業人士。如此始能全面提升出口管制之力道與效能，確保我國國家安全及科技競爭優勢。見楊健弘，前揭註 484，頁 208-209。

設施、關鍵技術產業，並思考成立跨部會審查單位及機制[496]。

承上，亦有認為受限於貿易法適用範圍及主管機關之量能，要將貿易法規範對象擴大，可能會有困難，若將出口管制體系放置於貿易法下將會箝制我國出口管制體系規範技術之可能性，此種體系性之問題並非修改文字能解決，未來可朝訂立專法之方式來規範出口管制體系，以達成全面規範貨品及技術出口管制之政策目的[497]。

此外，我國自主研發之高科技貨品及關鍵技術眾多，許多項目都是外國覬覦之對象，也可能作為軍事用途。然我國出口管制之目的並未包括「確保產業競爭優勢」及「外交政策需要」，亦未針對我國貨品出口後之「再出口」制定詳細規範，恐難防止我國之關鍵技術流入不當之使用者而損害相關企業或國家利益[498]。

四、敏感科技保護法草案未獲立法院通過

因我國現行之營業秘密法對於國家安全之保障仍有不足，而我國過往對於牽涉國家安全之敏感科技之保護係散落於如營業秘密法、國家機密保護法、兩岸條例、政府資助國家核心科技研究計畫安全管制作業手冊以及各部會訂定研發成果歸屬及運用辦法等，惟各法規之運用範圍均有所侷限，並未有統一之體系及規範，無法防止技術外流

[496]趙晞華，前揭註 440，頁 27。
[497]楊健弘，前揭註 484，頁 207。
[498]楊健弘，前揭註 484，頁 208。

之狀況。為了保護涉及我國國家安全之敏感科技，立法院曾於 2002、2005、2018 年曾討論我國是否應該設立「敏感科技保護法」[499]。

草案中對之「敏感科技」係指學術研究以外對國家安全及公共利益有重大影響之高敏感性與特殊性之科學資訊，且符合營業秘密之秘密性、經濟價值、合理保密措施等要件[500]。主管機關為確保國家安全及公共利益且有必要時，會定期審查敏感科技之項目與輸出國家地區，並報請行政院公告。若未經許可而輸出或公開敏感科學技術者則會有相關刑事責任。該草案雖然可以建立敏感科技之保護制度，防止國家關鍵技術之外流，但是草案內容受到企業反彈，造成該法案數度被提出，卻又數度胎死腹中[501]。

綜觀草案推動過程，歷經多年，因為在立法院無法獲得共識，而直到現在都未有結果。推動沒有成功之原因可能為下：1.對於敏感科技之定義及範圍並不明確，對於廠商之研發及投資規劃產生不確定性；2.企業自行研發技術，政府並未資助，若限制其技術之發展，恐怕影響企業之發展，無法擴大市占率而損害其競爭力；3.政府若介入管制

[499]林志潔、羅于盛，前揭註 444，頁 25。
[500]以立委王定宇等人於 2018 年提出之草案版本為例，對於敏感科技之定義為：：「本法所稱敏感科學技術，係指學術研究以外對國家安全及公共利益有重大影響之高敏感性與特殊性之科學資訊，且符合下列要件者：一、非一般涉及該類資訊之人所知。二、因其秘密性而具有實際或潛在之經濟價值。三、權利人已採取合理之保密措施。前項高敏感性與特殊性之科學資訊包括資料、計畫、編輯、程式裝置、公式、設計、原形、步驟、過程、程序、配方、程式或符號等。」見吳宛芳，前揭註 344，頁 23。
[501]林志潔、羅于盛，前揭註 444，頁 25。

，審查期間過長，將造成企業經營效率降低，恐會錯失商機；4.現行法制已經足夠，營業秘密有刑罰規定，足堪保護企業；5.草案出其立法理由具有針對性，容易讓在中國投資之台商反彈，有中國因素在內會造成意識形態及政黨之對立[502]。

伍、國安法及兩岸條例修法之介紹及評析

一、修法背景

(一)紅色供應鏈之威脅

2021 年 3 月間，法務部在提交給立法院經濟委員會之「紅色供應鏈」專題報告中提及，中國企業在我國招募人才，常未經主關機關許可在我國設立分公司或辦事處，而是以名為我國公司，實則為中資公司，私下從事業務。報告亦說明，調查局依據國家情報工作法第 7 條第 1 項第 4 款之規定，加強查察在我國之中國企業及可疑之港資、僑外資，並建立資料庫，蒐集公司營運狀態及違異常動態，若發覺有滲透洩密、挖角覽才、虛設行號、地下通匯及從事非許可業務者，即立案偵辦[503]。

有鑑於高科技產業為我國經濟命脈，近年來紅色供應鏈滲透我國

[502]吳宛芳，前揭註 344，頁 26-27。
[503]趙萃文，前揭註 466，頁 50。

產業狀況越來越嚴重，以各種手段吸收我國人才，竊取國家核心關鍵技術，規避我國法律規範，未經許可在我國從事業務活動，或假借他人名義，違法來我國投資，對我國之資訊安全、經濟發展、產業競爭力及國家安全，都有嚴重危害，保障不足之情況，已經相當明顯[504]。

美國自 1996 年起以聯邦層級之經濟間諜法保護營業秘密，對於侵害營業秘密者課與刑事責任，區分經濟間諜罪與竊取營業秘密罪，嚇阻競爭對手不法竊取營業秘密，防止國家安全及經濟發展受到侵害。由於我國與中國雙邊商業競爭之白熱化，我國政府深感產業發展已經涉及國家安全之急迫性，為了保護我國高科技產業，防止關鍵技術外流，立法院於 2022 年 5 月 20 日三讀通過國安法修正草案，新增「經濟間諜罪」、「國家核心關鍵技術營業秘密之域外使用罪」及相關配套措施[505]。

(二)營業秘密法刑罰化後之缺漏

1.無法有效防範經濟間諜

首先，營業秘密法第 13 條之 1 為告訴乃論之罪，且打破刑事告訴不可分之原則，允許對於共同被告單獨撤回告訴，雖然號稱是要鼓勵吹哨者，惟實務上最常見的則是被害企業市圖用刑事手段來達成民

[504]同前註。
[505]同前註。

事賠償，嚇阻營業秘密外流之功能有限，反而有以刑逼民之疑慮，無法有效保護公平競爭之社會法益。而號稱保護國家產業競爭力之營業秘密法第 13 條之 2，雖然本有防制經濟間諜之考量，惟其要件與美國之 EEA 第 1831 條相較，並不要求行為人主觀上需知悉其行為將裨益外國政府，並且未區分與外國政府或是公平競爭無關之營業秘密竊取行為，一律加重刑責，造成保護法益不明，處罰失當。且現今科技發達，行為人若欲圖利外國政府，可以在我國設立公司，並竊取他人營業秘密，並在我國內使用，無須使用傳統域外使用手段，便可輕易規避此條規定，無法有效防範經濟間諜[506]。

2. 並無事前監理及管制手段

我國雖有貿易法針對出口進行管制，惟貿易法之目的為「發展對外貿易，健全貿易秩序，以增進國家之經濟利益」[507]，為了發展經濟，原則上是鼓勵貨物自由流通，除有國際條約、貿易協定、國家安全、生態保育等政策需要，才能對貨品之貿易來限制。而「戰略高科技貨品輸出入管理辦法」之目的在於防止武器擴散及不法用途，若無此種情況，主管機關仍會核發出口許可。此外，承前所述，貿易法規範之標的為有形實體之貨品本身之輸出入刑為，若無形技術不附於貨品本

[506]林志潔、羅于盛，前揭註 444，頁 24。
[507]貿易法第 1 條之規定。

身，或不在戰略高科技貨品輸出入管理辦法」所規範之範圍內者，並不受到貿易法之拘束。換言之，根據以上原因，我國在技術輸出之法律規範上仍有缺漏，除了營業秘密法之事後處罰外，無法於事前防範技術外流之發生[508]。

二、立法模式選擇

對於我國營業秘密刑罰化之法律規範上缺漏，在立法上如何補強對於國家安全法益之保護，在立法模式的選擇上，可能的立法模式包含：1.制定專法；2.增修國安法及兩岸條例並制定出口管制法；3.增修國安法及兩岸條例並輔以出口管制輔導[509]。

制定專法也就是本文前所提及之敏感科技保護法草案，惟多年來均並未成功。除了制定專法保護外，第 2 種可能之模式即在事前針對技術輸出制定「出口管制法」，觀察美國之 ECRA、日本之「外匯及外國貿易法」、韓國之 ITPA 都可以做為我國之立法參考，並與國安法、兩岸條例共同成為保護國家安全及產業競爭力之防線且與國際接軌[510]。

可考慮之方式為在貿易法中制訂出口管制專章或是直接制定出口管制法，制定專章之好處可能是法律規範整體之變動幅度較小，但

[508]林志潔、羅于盛，前揭註 444，頁 24。
[509]林志潔、羅于盛，前揭註 444，頁 25-27。
[510]林志潔、羅于盛，前揭註 444，頁 25-26。

是缺點是由於貿易法之立法目的並非管制出口，若加入了出口管制之專章，恐怕會增加貿易法之複雜程度及產生爭議。如果單獨制定出口管制法，可以使技術輸出管制脫離貿易法之現行架構，在條文用語及管制措施上將會更有彈性[511]。

由於敏感科技保護法草案數度失敗，而於貿易法中制訂出口管制專章或是單獨定立出口管制法也因牽動較大，短期內無法達成，在各種立法權衡與角力下，我國本次修法採取之方式，則是前述的第 3 種做法，修改國安法來處理經濟間諜罪的問題、修改兩岸條例規範相關人員之移動、輔以內部的出口管制規定，將本來欲在專法當中規範之議題拆分在不同規範內[512]。

此種分散立法之方式與制定單一專法相較，在全面性與周延性方面雖有不足，但是與修法前相比，在立法密度上還是有加強，符合保護國家安全之國際立法趨勢[513]。

三、修法重點

(一)、國家安全法

國安法於 2022 年 6 月 8 日修正公布，新增「經濟間諜罪」與「國

[511]林志潔、羅于盛，前揭註 444，頁 26。
[512]同前註。
[513]林志潔、羅于盛，前揭註 444，頁 27。

家核心關鍵技術營業秘密域外使用罪」，將該等案件列為國家安全案件。依據行政院之修正草案總說明，修法目的為「更周延保護我國高科技產業競爭力與國家經濟利益，並防止國家核心關鍵技術之營業秘密遭外國、大陸地區、香港、澳門、境外敵對勢力或其所設立或實質控制之各類組織、機構、團體或其派遣之人侵害」、「建構國家核心關鍵技術營業秘密之層級化保護體系」、「以維護國家安全及經濟發展命脈」。本次國安法之修正同時修正兩岸條例，強化國家核心關鍵技術人員之赴陸規範，並明確規範大陸企業繞道第三第及藉由人頭在臺灣從事業務活動之管理機制，具有較強的針對性，可能也於美國近年與中國之科技戰有所關連[514]。

1.「國家核心關鍵技術之營業秘密」之定義與要件

在定義部分，「國家核心關鍵技術」係指如流入外國、大陸地區、香港、澳門或境外敵對勢力，將重大損害國家安全、產業競爭力或經濟發展。在要件部分，需基於國際公約、國防之需要或國家關鍵基礎設施安全防護考量，應進行管制；或可促使我國產生領導型技術或大幅提升重要產業競爭力。在程序部分，認定程序及其他應遵循事項之辦法，授權由國家科學及技術委員會會商有關機關定之，並應定期檢

[514]章忠信（2023），〈保護?還是管制?在國家安全法新增經濟間諜罪之後〉，《全國律師》，27 卷第 4 期，頁 37。

討[515]。

而營業秘密的部分，依據國安法第 3 條第 6 項之規定，國安法之營業秘密與營業秘密法之營業秘密定義相同，因此，某項公司機密，除了被認定為國家核心關鍵技術之外，尚需具備「秘密性」、「經濟價值」、「合理保密措施」三要件，才有國安法關於「國家核心關鍵技術之營業秘密」相關規定之適用[516]。

然而，在此次國安法修正當中，將營業秘密與國家核心關鍵技術兩者之要件彼此綁定，是否妥適，則仍有很大的探討空間。一方面來說，資訊本身是否屬於國家核心關鍵技術，認定是由政府掌握，另一方面，資訊本身是否符合營業秘密之三要件，則掌握在營業秘密所有人之手中，政府無從得知相關資訊。換句話說，只要營業秘密所有人刻意規避合理保密措施之要件，即可不受國安法之規範[517]。

若要真的要達到避免國家核心關鍵技術外流、保護國家安全之目的，其實並不應該將重要之構成要件取決於私人之作為與否，但是在立法時，可能因為未了避免打擊範圍過廣，而以上述之方式立法，也因此要構成本次國安法修法之「國家核心關鍵技術營業秘密之域外使用罪」或是「為外國等侵害國家核心關鍵技術營業秘密罪」，在構成

[515]國家安全法第 3 條第 3-5 項之規定。趙萃文，前揭註 459，頁 56。
[516]林志潔、羅于盛，前揭註 444，頁 28。
[517]林志潔、羅于盛，前揭註 444，頁 28。

要件上都相當難構成，舉證門檻甚高[518]，將來要如何適用，成效如何，有待我國司法機關之實務運作來檢驗。

2.新增「經濟間諜罪」與「國家核心關鍵技術之域外使用罪」

(1).經濟間諜罪

國安法第 3 條第 1 項之規定[519]，即為本次新增之經濟間諜罪。該項新增其實係將營業秘密法第 13 條之 1 第 1 項 4 款之侵害營業秘密行為之構成要件，複製於本項。其中兩個差異在於，侵害目的從營業秘密法之一般侵害，在國安法調整為「為外國、大陸地區、香港、澳門、境外敵對勢力或其所設立或實質控制之各類組織、機構、團體或其派遣之人」而為侵害行為，因涉及為外國等境外國家、地區、敵對勢力或相關組織等之利益，故被認定為係「經濟間諜罪」；此外，侵害之標的從營業秘密法的「營業秘密」，在國安法提升成為「國家核心關鍵技術之營業秘密」[520]。

[518]林志潔、羅于盛，前揭註 444，頁 29。
[519]國安法第 3 條第 1 項規定：「任何人不得為外國、大陸地區、香港、澳門、境外敵對勢力或其所設立或實質控制之各類組織、機構、團體或其派遣之人，為下列行為：一、以竊取、侵占、詐術、脅迫、擅自重製或其他不正方法而取得國家核心關鍵技術之營業秘密，或取得後進而使用、洩漏。二、知悉或持有國家核心關鍵技術之營業秘密，未經授權或逾越授權範圍而重製、使用或洩漏該營業秘密。三、持有國家核心關鍵技術之營業秘密，經營業秘密所有人告知應刪除、銷毀後，不為刪除、銷毀或隱匿該營業秘密。四、明知他人知悉或持有之國家核心關鍵技術之營業秘密有前三款所定情形，而取得、使用或洩漏。」
[520]章忠信，前揭註 514，頁 38。

(2).國家核心關鍵技術域外使用罪

國安法第 3 條第 2 項之規定：「任何人不得意圖在外國、大陸地區、香港或澳門使用國家核心關鍵技術之營業秘密，而為前項各款行為之一。」。

3.建立層級化之保護體系

我國營業秘密法之刑罰化曾經大量參考美國 EEA 之規定，該法於 1996 年制定，對於侵害營業秘密者課以刑事責任，並區分「經濟間諜罪」與「竊取營業秘密罪」[521]。此次國安法修法億再次參照 EEA 與我國營業秘密法，可謂整合兩者而成[522]。

此次國安法修正新增「經濟間諜罪」與「國家核心關鍵技術營業秘密域外使用罪」,而在國安法修正之後,我國對於營業秘密之保護,採取層級化之保護體系,國安法與營業秘密法之法定刑差距非常大,刑度由輕到重分別為：一般侵害營業秘密罪[523]、一般侵害營業秘密之域外使用罪[524]、國家核心關鍵技術營業秘密之域外使用罪[525]、經濟間諜罪[526]。一般侵害營業秘密罪是營業秘密法下之基本款，刑度最輕，

[521]詳見本文貳、一、(三)部分。
[522]林志潔、羅于盛，前揭註 444，頁 29。
[523]營業秘密法第 13 條之 1 之規定。
[524]營業秘密法第 13 條之 2 之規定。
[525]國安法第 3 條第 2 項之規定。
[526]國安法第 3 條第 1 項之規定。

且為告訴乃論；一般侵害營業秘密之域外使用罪是建立於一般侵害營業秘密罪之上，因為意圖在域外使用而加重處罰；而國安法第 3 條第 1 項係指有外國勢力派遣之「經濟間諜」，第 2 項則是無外國勢力介入，兩者構成要件不同，對於國家安全之影響程度不同，就反應在刑度之輕重上，所以違反國安法第 3 條第 1 項將會重於違反國安法第第 2 項[527]。

4. 酌量加重罰金刑

參照營業秘密法第 13 條之 1 第 3 項及第 13 條之 2 第 3 項之規定，對於犯罪所得之利益超過國安法第 8 條第 1、2 項之罰金最高額時，於同條第 4 項賦予法院於科罰金時得酌量加之權限[528]，惟並未比照營業秘密法區分「一般侵害營業秘密罪」與「一般侵害營業秘密之域外使用罪」而做不同倍數之規範，而是一律於所得利益之 2 至 10 倍酌量加重，應係認為國安法之「經濟間諜罪」與「國家核心關鍵技術營業秘密之域外使用罪」都是情節嚴重之犯罪，而作相同之規範，由法院實於實際案件當中依職權做決定[529]。

[527]林志潔、羅于盛，前揭註 444，頁 29-30。
[528]國安法第 8 條第 4 項規定：「科罰金時，如犯罪行為人所得之利益超過罰金最多額，得於所得利益之二倍至十倍範圍內酌量加重。」
[529]章忠信，前揭註 514，頁 39-40。

5. 法人兩罰與舉證免責

修法並新增法人兩罰制度與舉證免責規定[530]，若受雇人因執行職務觸犯經濟間諜罪或國家核心關鍵技術之營業秘密域外使用罪，除受雇人須依法受罰外，亦課予業者負有監督防止其員工不法侵害國家核心關鍵技術營業秘密之責任，明定對雇主(法人、非法人團體或自然人)亦課以各該項之罰金。惟若雇主對於犯罪之發生，已為盡力防免者，則不在此限。此舉證免責端看是否盡到法令遵循及改善措施，並非僅要求一般性、抽象性之宣示規範，而是必須有具體、積極、有效之防止措施[531]。

6. 提高刑罰並擴大域外保護

營業秘密法第 13 條之 1 之一般侵害營業秘密罪之刑度為 5 年以下有期徒刑，同法第 13 條之 2 之一般侵害營業秘密之域外使用罪之刑度則為 1 年以上 10 年以下之有期徒刑，因為均非最輕本刑 3 年以上有期徒刑之罪，不符合刑法第 7 條有關域外效力之規定。新修正之國安法新增之「經濟間諜罪」及「國家核心技術營業秘密域外使用罪」之刑度分別為 3 年以上 10 年以下有期徒刑及 5 年以上 12 年以下之

[530]國安法第 8 條第 7 項之規定。
[531]趙萃文，前揭註 466，頁 58。

有期徒刑，擴大域外保護[532]。

7.偵查保密令及祕密保持令之適用及提高刑罰

為了防止 2 次洩密之風險，本次修法引進偵查保密令之規定，於國安法第 9、10 條規定，檢察官在偵辦國家核心關鍵技術之營業秘密相關案件時，得適用營業秘密法第 14 條之 1 至 14 條之 3 關於偵查保密令之規定，並提高其刑罰及增加域外效力[533]，以避免在境外違反偵查保密令而脫免刑責[534]。

在祕密保持令的部分，由於 2007 年智慧財產案件審理法引進祕密保持令時，並無「經濟間諜罪」及「國家核心關鍵技術營業秘密域外使用罪」之概念，2022 年修正國安法時，國安法第 9 條第 2 項雖使犯國安法第 8 條之罪之案件得以適用智慧財產案審理法關於祕密保持令之規定，惟並未如國安法第 10 條第 1 項之規定，針對違反偵查保密令而使用或揭露「國家核心關鍵技術之營業秘密」加重刑度，只能使用智慧財產案件審理法第 35 條處理，惟該條刑度較輕，僅為 3 年以下有期徒刑之罪，且為告訴乃論。直到智慧財產案件審理法於 2023 年 2 月 15 日修正公布，同年 8 月 30 日施行後，於該法 72 條[535]

[532]趙萃文，前揭註 466，頁 58。
[533]國安法第 10 條規定：「違反前條第一項偵查保密令者，處五年以下有期徒刑、拘役或科或併科新臺幣一百萬元以下罰金。於外國、大陸地區、香港或澳門違反偵查保密令者，不問犯罪地之法律有無處罰規定，亦適用前項規定。」
[534]趙萃文，前揭註 466，頁 58。
[535]智慧財產案件審理法第 72 條規定：「違反本法秘密保持命令者，處三年以下有期徒刑、拘役

第 2 項針對違反祕密保持令而使用或揭露「國家核心關鍵技術之營業秘密」加重處罰，並刪除告訴乃論罪之規定，方解決此問題[536]。

此外，為了避免違反祕密保持令而使用或揭露「國家核心關鍵技術之營業秘密」之行為脫免刑責，新修正之智慧財產案件審理法第 73 條第 3 項之規定如同國安法第 10 條第 2 項之規定，參照營業秘密法第 14 條之 4 第 2 項之規定，明定於我國境外違反祕密保持令者，亦須依法處罰[537]。

8. 智慧財產及商業法院為第一審法院

為了保護國家核心關鍵技術之營業秘密不被境外國家、敵對勢力等不法侵害，維護我國高科技產業競爭優勢，整體經濟發展命脈及國家安全之維護，若有犯國安法第 8 條第 1 項至第 3 項之罪者，均屬破壞國家法益情節重大，依同法第 18 條第 2 項之規定，比照內亂、外患、妨害國交罪之管轄規定，改由智慧財產及商業法院為第一審管轄法院，不符該案判決者，上訴最高法院，以兩個審級，速審速結[538]。

或科或併科新臺幣一百萬元以下罰金。犯前項之罪，其受命令保護之營業秘密，屬國家安全法第三條所指國家核心關鍵技術之營業秘密者，處五年以下有期徒刑、拘役或科或併科新臺幣三百萬元以下罰金。於外國、大陸地區、香港或澳門犯前二項之罪者，不問犯罪地之法律有無處罰規定，亦適用前二項規定。」

[536]章忠信，前揭註 514，頁 41-42。

[537]章忠信，前揭註 514，頁 42。

[538]章忠信，前揭註 514，頁 42。

9.設定專業法庭或指定專股審理

由於侵害「國家核心關鍵技術之營業秘密」之犯罪具高度機密性及敏感性，必須仰賴專業判斷，國安法第 19 條規定，法院為了審理違反該項規定之犯罪案件，得設立專業法庭或指定專股辦理[539]。

(二)、兩岸條例

此次「國家核心關鍵技術營業秘密保護」法制修法，兩岸條例亦配合國安法修法，修法重點為「國家核心關鍵技術與人員之管制」，可以分為「建立更完善赴陸管理機制」及「防範陸資或陸企違法來臺從事投資或業務活動」兩部分[540]。

1.建立更完善赴陸管理機制

(1).進入許可

為了要遏阻侵害營業秘密之行為，並保護國家核心關鍵技術，適當管制高科技人才，有其必要。兩岸條例第 9 條第 4 項第 6 款規定，受政府機關、機構委託、補助或出資達一定基準，從事涉及國家核心關鍵技術業務之個人或法人、團體、其他機構之成員及受委託、補助、出資終止或離職未滿三年者，進入大陸地區應經審查會審查許可。同

[539]同前註。
[540]趙萃文，前揭註 466，頁 60。

法第 91 條第 3 項規定，違反申請許可者，可處新臺幣 200 萬元以上，1,000 萬元以下罰鍰[541]。

(2). 返臺通報

兩岸條例第 9 條第 5 巷規定，前開人員進入大陸地區返臺後，應向原服務機關、委託、補助或出資機關、機構通報。但直轄市長應向行政院、縣市長應向內政部、其餘機關首長應向上一級機關通報。同法第 91 條第 4 項規定，違反返臺通報規定者，得處新臺幣 2 萬以上，10 萬以下之罰鍰[542]。

(3). 子法訂定

兩岸條例第 9 條第 13 項規定，受委託、補助或出資之一定基準及其他應遵行事項之辦法，授權由國家科學及技術委員會會商有關機關定之。同條第 12 項規定，赴陸許可辦法及返臺通報程序，授權由內政部擬定，報請行政院核定之[543]。

2. 防範陸資或陸企違法來臺從事投資或業務活動

兩岸條例本次修正，同時也在防止隱蔽陸資滲透及陸企利用人頭違法在臺活動，對我國產業及經濟發展、國家安全產生危害。

---

[541]趙萃文，前揭註 466，頁 60。
[542]同前註。
[543]同前註。

(1). 管制行為

管制之行為可區分為「違法從事業務活動」及「違法從事投資行為」。前者係指中國大陸營利事業利用其於第三地投資之事業，未經許可在臺成立分公司或辦事處，趁此機會挖角我國高科技人才。後者則是陸資借人頭名義來臺投資，擾亂我國交易安全或藉此從事不法行為[544]。

(2). 管制對象

本次修正兩岸條例區分規範對象為「大陸地區營利事業」及「陸資」，且為了全面防止管制對象藉由繞道第三地或人頭滲透，亦一併修正相關規定[545]。

在大陸地區營利事業部分，依據兩岸條例第 40 條之 1 之規定，新增大陸地區營利事業於第三地區投資之營利事業，非經主管機關許可，並在臺灣地區設立分公司或辦事處，不得在臺從事業務活動之規定。並修正其分公司在臺營業準用公司法之相關規定。此外，依據同法 93 條之 2 之規定，大陸地區營利事業或其於第三地區投資之營利事業，應經主管機關許可，始得在臺從事業務活動，新增將本人名義

[544]許祐寧（2022），〈立法院修正《國安法》及《兩岸條例》強化國家核心關鍵技術保護〉，《科技法律透析》，34 卷 8 期，頁 17。
[545]許祐寧，前揭註 544，頁 18。

提供或容許前開營利事業使用者，處 3 年以下有期徒刑，拘役或科或併科新臺幣 1,500 萬元以下罰金及對法人並罰之規定。且本條原先之刑度僅為 1 年以下有期徒刑、拘役或科或併科新臺幣 15 萬元以下罰金，情重罰輕，嚇阻效果有限。本次修正為了有效嚇阻違法行為，遂加重刑度，以維護交易秩序及國家安全[546]。

陸資部分，依據兩岸條例 93 條之 1 之規定，增訂將本人名義提供或容許應經主管機關許可在臺投資之大陸人民等使用者，得處新臺幣 12 萬元以上 2,500 萬元以下罰鍰[547]。

四、修法評析

(一)、國家安全法部分

此次修法，加強保護「國家核心關鍵技術」之法治建設，避免高科技產業營業秘密外洩，損害國家競爭力及產業利益，目標正確，值得肯定。為此項對國家發展影響重大之法案，從法務部 2021 年 7 月 21 日預告草案到 2022 年 5 月 20 日立法院三讀通過，時間不到 1 年，進度算是相當迅速，是否達到各方之共識，非無討論空間[548]。

[546]同前註。
[547]同前註。
[548]章忠信，前揭註 514，頁 42-43。

1. 主管機關選擇之問題

營業秘密法之主管機關權責歸屬，在立法之初，即有疑義，此次修法將「經濟間諜罪」於國安法規範，亦加深此部分之問題。營業秘密之保護，屬於公平競爭之一環，包含我國在內之大陸法系國家，均係以競爭法規範營業秘密之保護,我國公平交易法於1991年立法時,即以第19條第5款規定，事業不得有以脅迫、利誘或其他不正當方法獲取他事業之產銷機密、交易相對人資料或其他有關技術秘密而有妨害公平競爭之虞之行為,而公平交易法之主管機關為公平交易委員會[549]。

1996年制定營業秘密法,是對美貿易諮商時承諾之立法,當時對該法之主管機關即有爭議,最後草案雖由經濟部商業司研擬,惟在該法中並未如專利法、商標法、著作權法、積體電路電路布局保護法一樣，在條文中明訂主觀機關為經濟部，並由經濟部指定專責機關辦理相關業務。目前營業秘密業務由經濟部智慧財產局下之法務室主責，並未像專利權、商標權、著作權業務等設有專組主責，並不適當[550]。

本次修法將「國家核心關鍵技術之營業秘密」納入國安法法保護,目的在於將其拉至國家安全層級之保護，將「經濟間諜」等罪拉高處

[549]公平交易法第6條規定：「本法所稱主管機關為公平交易委員會。本法規定事項，涉及其他部會之職掌者，由主管機關商同各該部會辦理之。」；章忠信，前揭註514，頁43。
[550]章忠信，前揭註514，頁43。

罰力度，比照內亂、外患、妨害國交罪，對外宣稱由法務部、國防部、內政部共同擬訂，惟主管營業秘密法業務之經濟部並不在其中。此次修法之主要議題在於營業秘密之加強保護，主管營業秘密之經濟部卻不在修法草案提案機關之列，此種安排恐怕有討論之空間[551]。

又國安法之主管機關為法務、國防、內政三部，相關聯之法律、法規命令、行政規則、職權命令等，散見在經濟部、國家科學及技術委員會及大陸委員會等不同機關，主管機關過多，也可能造成法律執行上之困難或機關本身之不重視[552]。

2.法律制度設計之問題

本次國安法之修正，目的雖然在於建構營業秘密層級化之保護體系，卻將同屬於營業秘密之保護規範，割裂在營業秘密法及國安法當中，然後再於國安法當中不只 1 次援引營業秘密法之規定[553]，或於國安法當中重複營業秘密法之規定[554]。據此，有學者認為，其實針對「經濟間諜罪」與「國家核心關鍵技術營業秘密域外使用罪」之處罰規定，只需於營業秘密法中增訂即可，無須疊床架，於國安法中另行規範[555]。

從國去立法歷史觀察，國科會於 2002 年提出之「國家科技保護

[551]章忠信，前揭註 514，頁 43-44。
[552]趙萃文，前揭註 466，頁 81。
[553]國安法第 3 條第 6 項(營業秘密定義)、第 9 條第 1 項(偵查保密令)之規定。
[554]國安法第 3 條第 1 項(侵害營業秘密行為態樣)、第 8 條第 4 項(加重罰金刑)、第 8 條第 7 項(兩罰及舉證免責規定)、第 10 條第 2 項(境外違反偵查保密令處罰)之規定。
[555]章忠信，前揭註 514，頁 44。

法草案」、2005 及 2008 年行政院提出之「敏感科學技術保護法草案」、都是為了處理管制敏感科學技術之輸出問題，但是全都因為無法獲得共識而遭受屆期不續審或法案撤回之命運。有學者認為，此次國安法之修正，是以透過「保護營業秘密私權」之名義，來進行「部分國家核心關鍵技術」[556]行政管制，而不另以行政管制法律制度處理，將個人法益之營業秘密升級成為「國家核心關鍵技術之營業秘密」，以國家法益之名義納入控管，法制設計上並非適當[557]。

3.侵害態樣之問題

有學者認為，此次國安法修正之「經濟間諜罪」與「國家核心關鍵技術營業秘密域外使用罪」一方面繼承了營業秘密法將 4 款侵害態樣不分輕重混於 1 項的問題，另一方面也不容易區別此兩項犯罪之區別。簡言之，國安法之「經濟間諜罪」必須是為了境外勢力之利益而侵害，不問使用之國家或地區，而「國家核心關鍵技術營業秘密域外使用罪」是為了在境外使用之目的而侵害，然而，只要在境外使用，似乎就難以避免境外勢力獲得利益之結果[558]。

[556]指「被侵害之國家核心關鍵技術之營業秘密」，不及於營業秘密所有者自行輸出或技術移轉之部分。
[557]章忠信，前揭註 514，頁 45。
[558]章忠信，前揭註 514，頁 45。

4.加重罰金刑之問題

營業秘密法與國安法都有加重罰金刑之規定，但是營業秘密法第13條之1之「一般侵害營業秘密罪」、與第13條之2之「一般侵害營業秘密域外使用罪」均針對犯行輕重及罰金多寡，做「所得利益3倍」或「所得利益2至10倍」之不同加重處罰。惟國安法第8條第1項、第2項之「經濟間諜罪」、「國家核心關鍵技術域外使用罪」卻沒有此種區分，而是在同法第8條第4項規定，一律「於所得利益之2至10倍範圍內酌量加重」，並未特別於立法理由中交代原因，與營業秘密法之立法模式產生不一致之狀況[559]。

5.適用程序上之問題

國安法增訂「經濟間諜罪」、「國家核心關鍵技術域外使用罪」後，與原本營業秘密法之「一般侵害營業秘密罪」、「一般侵害營業秘密域外使用罪」形成層級化之保護體系。不過原本營業秘密法之「一般侵害營業秘密罪」、「一般侵害營業秘密域外使用罪」之偵審由地方檢察署與法院負責，採三級三審制，惟國安法第18條第2項將「經濟間諜罪」、「國家核心關鍵技術域外使用罪」改由智慧財產及商業法院為第一審管轄法院，採二及二審制。雖然同屬營業秘密，卻會因

[559]章忠信，前揭註514，頁45-46。

是否被認定為「國家核心關鍵技術之營業秘密」而適用不同之審級。在實務上，若有原先認定為「經濟間諜罪」、「國家核心關鍵技術域外使用罪」而適用二級二審制，後來改認定為「一般侵害營業秘密罪」、「一般侵害營業秘密域外使用罪」之情況，要如何能回歸三級三審制，仍有疑問。而採用二級二審制之程序，則有侵害被告審級利益之虞[560]。

6. 小結

我國立法院雖曾數次討論是否仿效他國，制定專法保護我國敏感科技，針對技術與資訊之流出，一方面就合法之合作與購買部分進行管制，另一方面就非法竊取行為予以處罰。惟因牽動兩岸商業活動甚鉅，產業遊說之力量甚強，因此以失敗告終。近年在美中科技戰之背景與紅色供應鏈之威脅下，各國紛紛強化相關法制，保護自身關鍵技術，我國自然無法自外於世界趨勢，尤其是美國之法規監管密度。我國此次修法，雖係以分散立法之方式來處理各種議題，離專法之目標尚有距離，但仍勝過過去毫無防備意識、門戶大開，核心競爭力遭受侵蝕卻無法可用之窘境[561]。

然而，有學者認為，縱使要強化「國家核心關鍵技術之營業秘密」之保護，法制之完整體系，不應該因此遭受破壞，營業秘密之相關規

[560]章忠信，前揭註 514，頁 46。
[561]林志潔、羅于盛，前揭註 444，頁 33。

範，不宜割裂在不同的規範當中。營業秘密法之主管機關應該在營業秘密法中明確規範，尊重其專業，立法及執行，應由其負責規劃。屬於私權之營業秘密應與國家利益之「國家核心關鍵技術」出口管制，在立法與執行上都應該脫鉤處理，以免產生更多爭議。而國安法之修法既然是保護「國家核心關鍵技術之營業秘密」，應以「保護營業秘密」為核心，而非著重在管制「國家核心關鍵技術」，在相關子法之訂定及國家核心關鍵技術之認定上，應以產業為中心，而非以政府強力主導為主軸[562]。

(二)、兩岸條例部分

兩岸條例本次修正，明文將陸資於第三地區投資之事業以及提供本人名義供投資使用之人頭行為，納入管制，及大幅提高違反之刑責。將會提高外國企業來臺投資之門檻，因為必須額外檢視企業股權及投資架構，確認有無陸資參與其中[563]。

在人員管制部分，可能對於投資或合作影響更為劇烈，根據兩岸條例修正管制人員赴陸部分，是限制在政府委託出資之情形，可能會衍伸出政府補助出資達一定基準應受管制之認定疑問。在實務上，政府補助之產、學、研合作案難以完全切割，若合作案之標的內容涉及

[562]章忠信，前揭註 514，頁 46。
[563]許祐寧，前揭註 544，頁 19。

國家核心關鍵技術時，針對在職人員之高強度之赴陸管制可能會從學術界、研究機構擴散至產業界，影響高科技產業接受政府補助、委託、技術合作與投資之意願，或阻礙員工參與國家核心關鍵技術之研發，不利企業吸納海外高科技人才，此部分影響仍須審慎評估[564]。

五、與美國、韓國立法之比較

(一)、兼採美國、韓國之立法模式

國安法之「經濟間諜罪」、「國家核心關鍵技術域外使用罪」，分別採用美國、韓國之立法模式。國安法之「經濟間諜罪」與美國 EEA 對於主觀構成要件之要求雷同，均規定行為人行為時於主觀上認識是為了「外國勢力」所為，此部分是採取美國 EEA 對於外國勢力介入而加重刑罰之立法模式。而「國家核心關鍵技術域外使用罪」之主觀要件則要求須有「在域外使用之意圖」，此部分則是參考韓國 UCPA 及 ITPA 之「防止資訊洩漏境外」立法模式[565]。

(二)、保護標的範圍較小

國安法之「經濟間諜罪」、「國家核心關鍵技術域外使用罪」之保護客體為「國家核心關鍵技術之營業秘密」，需同時符合國家核心

[564]許祐寧，前揭註 544，頁 19。
[565]劉怡君（2023），〈經濟間諜的防制與執法－他山之石與我國之挑戰〉，《全國律師》，27 卷 4 期，頁 7。

關鍵技術及營業秘密之構成要件，看似結合美國、韓國兩者之法制，實際操作上卻會造成國安法上述罪名之適用範圍比美國、韓國之相關規範更狹小[566]。

(三)、並無預備犯、共謀犯之規定

國安法之「經濟間諜罪」、「國家核心關鍵技術域外使用罪」雖有處罰未遂犯，但是並無前置處罰預備犯及共謀犯，目前國安法之規定無法處理此部分之預備及共謀行為。相較之下，美國 EEA 針對經濟間諜罪及竊取營業秘密罪設有處罰共謀犯[567]之規定，將刑事責任前置到未遂犯之前，以收嚇阻犯罪之效，通常立法者僅針對對於社會、國家法益具有高度威脅之犯罪，才會制定共謀犯之處罰規範。而韓國之 UCPA 與 ITPA 也都有處罰共謀犯之規定[568]。

(四)、非獨立組織體責任及組織免責規範

國安法第 8 條第 7 項針對「經濟間諜罪」、「國家核心關鍵技術域外使用罪」設有組織體之罰金刑事責任，且須以自然人成立刑事責任為前提。同項後段但書則設有組織體之免責規定，以鼓勵企業建立內部控制及法令遵循措施。韓國 UCPA 及 ITPA 也是採取此種立法模

[566]劉怡君，前揭註 565，頁 7-8。
[567]See 18 U.S.C. § 1831(a)(5).
[568]UCPA 第 18-3 之規定及 ITPA 第 37 條之規定。劉怡君，前揭註 565，頁 9。

式。相反的，美國部分則比較不同，EEA 針對組織體有獨立於自然外之刑事責任，也沒有前述之免責規定[569]。雖然組織體刑事責任搭配合理防免犯罪發生之免責條款可以讓組織體有動機去推動內部控制及法令遵循制度，惟對於防免行為應該達到何種程度，仍有爭議，有待我國司法實務經驗之累積[570]。

(五)、美國、韓國法制之省思

1.保護標的擴大

國安法之「經濟間諜罪」、「國家核心關鍵技術域外使用罪」保護標的為「國家核心關鍵技術之營業秘密」，構成要件結合「國家核心關鍵技術」及「營業秘密」兩者，且國家核心關鍵技術牽涉國家安全、產業競爭性及經濟發展關聯性之舉證，對於檢察機關來說難度極高，難以適用，立法目的恐怕難以達成。且國安法此次修法之立法意旨著重在國家安全及產業競爭力，保護核心應該在於國家核心關鍵技術本身，韓國 ITPA 所採之立法模式，保護範圍不限於營業秘密，應該更符合我國需求[571]。

[569]See 18 U.S.C. § 1831(b).
[570]劉怡君，前揭註 565，頁 9。
[571]劉怡君，前揭註 565，頁 12。

2.刑事責任前置

國家核心關鍵技術或營業秘密，一旦外洩所造成之影響及損害就難以回復原狀，因此事前之預防遠勝於事後之追訴。美國之 EEA 與韓國之 ITPA、UCPA 皆將刑事責任提前到預備、共謀階段，以收嚇阻之效。我國既然立法政策上將「經濟間諜罪」、「國家核心關鍵技術域外使用罪」提升到國家安全層級，考量其影響層面甚廣，未來可考慮朝此方向修法[572]。

3.組織體責任採用

目前國安法所採取之組織體刑事責任，係以自然人之刑事責任為基礎，實務上可能會有執法機關因此缺乏談判籌碼，難以突破組織型犯罪結構之問題。簡言之，我國此種立法架構下，使從事犯罪行為之自然人與組織體成為命運共同體，降低自然人出面成為吹哨者揭發組織體犯罪行為之誘因，反而有礙透過組織體責任改造組織體內部控制制度之立法初衷。若能重新思考在我國法制架構下採用獨立組織體刑事責任可能性，與自然人之刑事責任脫鉤，可增加執法機關之彈性與談判空間，有助於即時發現組織體內之弊端[573]。

[572]劉怡君，前揭註 565，頁 12-13。
[573]劉怡君，前揭註 565，頁 13-14。

陸、心得與建議

一、營業秘密與國家核心關鍵技術保護法制部分

我國此次國安法之修法，試圖建立層級化之營業秘密保護制度，強化國家安全與產業競爭力之保護，立意良善，並且在法規當中新增「國家核心關鍵技術」之概念，使我國在保護國家關鍵技術之法制上，更前進一步，具有劃時代之象徵意義。

然而，我國所採取之「國家核心關鍵技術」與「營業秘密」結合成為「國家核心關鍵技術之營業秘密」立法模式，將大幅限縮國安法相關條文之適用範圍，而且可預期的是將會造成保護國家核心關鍵技術上的漏洞，此部分需要等待未來司法實務經驗累積，再觀察是否有繼續修法脫鉤兩者或是另立專法保護國家核心關鍵技術之必要性。另一方面，營業秘密法之相關規範分別規範在不同的法規範，恐怕徒增困擾，是否考慮將相關規範統一在營業秘密法中處理，也是其中一個選項。

本次修法雖然觸及了「國家核心關鍵技術之營業秘密」之防範竊取部分，但是在外資投資審查，以及出口管制方面，並無相關配套措施，欠缺保護「國家核心關鍵技術」之整體法律制度，與世界主要國家之立法趨勢脫節，對於國家安全及產業競爭力之保護，恐有缺漏，

未來在這兩個面向都應該繼續補強法律規範之密度。此外，目前我國對於陸資、外資分由不同之制度審查，並無太大實益，且若欲保護「國家核心關鍵技術」，應一視同仁對於外資、陸資都採取相同審查標準，方能排除外資、陸資藉由投資我國產業之方式來取得我國產業之關鍵技術。

二、申請訪問學者部分

(一)、申請過程及資料準備

筆者欲申請美國的學校，所以此部分是以討論美國學校為主。在時程方面，最近幾年法務部大概都是在 1、2 月間開始接受申請，申請截止日後 1、2 周由部長面試申請者。筆者在 2019 年及 2023 年各參加過 1 次面試。第一次參加人數有 13 人，面試內容主要是由各申請者以欲申請進修國家之語言自我介紹及報告研究方向。第 2 次面試申請者只有 2 人，面試內容主要則是以中文報告欲從事之研究內容。面試完畢後，則要等到 5、6 月相關審核流程完畢，才能確定是否能夠出國進修，所以在等待審核流程同時，就必須與潛在的進修學校窗口聯繫，了解所需之申請資料內容為何，否則在時間上將會有所不足。申請資料視各校需求，基本都會包含履歷、研究計畫、語文能力證明、兩封推薦信等等，而有些學校會有額外的要求，比如史丹佛大學就會

另外要求申請訪問學者之申請者必須先尋求1位願意指導的教授,取得教授同意後，才能申請訪問學者的計畫。在選擇學校之前，務必先釐清需要的條件為何。哈佛大學的訪問學者是向該校的伯克曼網路暨社會研究中心申請，申請時僅要求筆者繳交履歷及研究計畫，並未要求推薦信及語文能力證明，但是為求準備充足，仍應先備齊相關資料為佳。

哈佛大學部分,由於柏克曼研究中心在網路上並未開放申請管道,所以申請者要直接向承辦人聯繫，並繳交對方所要求資料，再來就是等待其是否錄取之通知，筆者大約是等到5月左右收到錄取通知，然後於6月間收到法務部的公文，才確定可以出國進修，再來就向AIT是預約入境美國入境簽證，由於簽證申請人數眾多，越早進行越好，如果是要用現場面試的方式，通常都要排隊1個月左右。

(二)、訪問學者之學術活動

柏克曼研究中心內部有許多美國及世界各國前來從事研究之學者、專家，該中心或其他合作之學術機構，時常會舉辦各種主題之研討會、工作坊等學術活動，分享大家的研究內容，若在自身研究工作之餘,有時間精力的話,都可以自由參加,了解最新的研究領域內容。

在哈佛法學院上課部分,法學院提供訪問學者每學年度6學分之旁聽課程選擇，須先行聯繫授課教授取得其同意，再將申請表交給教

授簽名後，繳回註冊組，最後經註冊組許可後即可旁聽該課程。有些課程因為礙於教室場地大小、修課人數多寡、是否屬於小班制課堂討論等因素，教授未必會同意開放旁聽，所以為了要獲得旁聽之機會，也必須多跟教授們聯繫溝通。

除此之外，若法務部當年度有計畫要參加美國當地的國際研討會或是相關政府機關拜會行程，也有可能會詢問在地的訪問學者是否有意願參加，所以亦有機會參與校外單位舉辦之研討會或是參訪其他美國政府單位之機會。

(三)、建議

在柏克曼研究中心之活動主要都是學術面向的為主，針對司法機關實務層面的接觸，就比較缺乏，比較沒有機會到美國當地的法院、檢察署或參訪或學習，如果未來法務部能夠在學術單位之外，與學校所在地之相關機關建立合作關係，能夠讓在地的訪問學者有機會接觸美國當地司法機關運作模式，對於我國及美國之雙方交流必有更大的助益，這是未來可以努力之方向。