

我國無形技術外流管控制度之檢討

Examining Intangible Technology Control System in Taiwan

王 偉 霖*

Wei-Lin Wang*

摘 要

我國地域雖小，但因製程及研發技術精良，在世界高科技產業各供應鏈仍有一席之地，此等技術大部分雖作商業用途，但部分技術同時具有國家經濟、軍事國防上之重要意義，通常也被稱為敏感科技。因中國大陸科技產業逐步崛起，積極以「紅色供應鏈」擬取代我國廠商地位，近年常發生中國大陸公司不法竊取我國廠商高科技研發成果或敏感科技之事件。在此氛圍之下，確保我國廠商高科技技術或敏感科技不外流，為刻不容緩之議題，惟我國針對無形技術之管控尚無具體法律制度，有建立體制之迫切必要。

本文在盤點我國防範外國，特別是中國大陸竊取科技相關產業技術及人才挖角之法規進行盤點，並就美國等國家及國際防範涉及國家安全、產業發展關鍵技術和科技外流及人才挖角的法規及作法進行比較後，認為我國刻正研議之「敏感技術保護法」草案在現行法制不足下，有助於建立敏感科技之有效管理機制。惟目前敏感科技之定義與營業秘密法之定義並無不同，為免發生受營業秘密法保障即受敏感科技法拘束

投稿日期：107.05.30 接受刊登日期：107.06.27 最後修訂日期：107.06.27

* 美國華盛頓大學法學博士，銘傳大學財金法律學系專任教授。

* J.S.D., Washington University in St. Louis; Professor of Law, Department of Financial Law, Ming Chuan University.

之情形，進而引發政府過度管制人民財產權之疑慮，建議草案中宜增加主管機關指定敏感科技時，除衡量國家安全、國民利益外，亦應一併衡量產業技術國內外市場比率，相關技術領域趨勢，且在最小必要限度內指定之原則。

關鍵詞：營業秘密；敏感科技；商業間諜；競業禁止；出口管制

目 次

壹、前言

貳、我國防範中國大陸竊取科技相關產業技術及人才挖角之法規盤點

一、營業秘密法之規定

(一) 民事方面

(二) 刑事規範

二、我國競業禁止相關規範

三、出口管制相關規定

(一) 國家安全法

(二) 貿易法

(三) 臺灣地區及大陸地區人民關係條例及其子法

(四) 國家機密保護法

(五) 科技研發相關規定

參、美國等國家及國際防範涉及國家安全、產業發展關鍵技術和科技外流及人才挖角的法規及作法

一、美國與歐盟營業秘密法制

(一) 美國

(二) 歐盟

二、美國等主要國家就競業禁止之規範

(一) 日本

(二) 德國

(三) 美國

三、美國、歐盟、韓國、日本就涉及國家安全、產業發展關鍵技術

和科技出口之限制

- (一) 美國
- (二) 歐盟
- (三) 韓國
- (四) 日本
- (五) 小結

肆、我國因應作為與修法建議

- 一、我國營業秘密法制之相關問題與因應作為
- 二、出口管制及投資審查法制相關問題與因應措施
- 三、我國敏感科技保護法草案

伍、結論

壹、前言

我國地域雖小，但因製程及研發技術精良，在世界高科技產業各供應鏈仍有一席之地，此等技術大部分雖作商業用途，但部分技術同時具有國家經濟、軍事國防上之重要意義，通常也被稱為敏感科技。因中國大陸科技產業逐步崛起，積極以「紅色供應鏈」擬取代我國廠商地位，近年常發生中國大陸公司運用各種方法強取豪奪，甚或不法竊取我國廠商高科技研發成果或敏感科技之事件。如我國砷化鎵晶圓代工產業知名企業穩懋半導體股份有限公司於民國（下同）104 年 8、9 月間，遭大陸廠商以挖角或不正當手法竊取技術文件資料等營業秘密，即屬是例¹。

在此氛圍之下，確保我國廠商高科技技術或敏感科技不外流，為刻不容緩之議題，惟我國針對無形技術之管控尚無具體法律制度，有建立體制之迫切必要。因此，本文以下首先將針對我國防範竊取科技相關產業技術及人才挖角之法規進行盤點，其次就美國等國家及國際防範涉及國家安全、產業發展關鍵技術和科技外流及人才挖角的法規及作法初步介紹，最後檢討我國法制現有問題，並提出建議。

貳、我國防範中國大陸竊取科技相關產業技術及人才挖角之法規盤點

中國大陸廠商或個人竊取我國廠商科技相關產業技術，通常係透過所謂商業間諜或挖角人才之方式為之。在現行法規下，就商業間諜之防範，我國廠商得透過營業秘密法規定主張權利或尋求保護；在人才挖角方面，我國廠商通常係以簽署競業禁止約定之方式加以預防。另外，如果我國廠商製造產品屬軍事國防用途，或所用技術包含軍事國防方面之

1 請參科技報橘網站，中國科技間諜入侵台灣晶圓產業，一杯咖啡偷走 75 億元的關鍵砷化鎵技術，2018 年 02 月 22 日，<https://buzzorange.com/techorange/2018/02/22/thief-like-movies/>，最後瀏覽日期：2018 年 06 月 27 日。

技術，又或者廠商所使用之技術係政府出資補助研發所得智慧財產權者，如要出口至中國大陸，政府亦有權管制。以下將分別盤點我國法關於營業秘密、競業禁止，以及出口管制之規定。

一、營業秘密法之規定

（一）民事方面

我國廠商所有技術，如符合我國營業秘密第 2 條規定²：「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。」得受營業秘密之保障。

技術得為營業秘密者，我國廠商依同法第 10 條規定，對以竊盜、詐欺、脅迫、賄賂、擅自重製、違反保密義務、引誘他人違反其保密義務或其他類似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一款之營業秘密，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 條至第 13 條之規定，主張：1. 損害賠償請求權；2. 排除侵害、防止侵害請求權；3. 銷毀或其他必要處置請求權³。

除以上救濟方式外，我國廠商若於判決確定後再透過強制執行之方式禁止侵害者使用或揭露營業秘密，可能已緩不濟急，故我國廠商亦可預向法院聲請定暫時狀態處分，禁止侵害營業秘密者為一定行為，而在

2 營業秘密各要件之詳細說明，請參拙作，營業秘密法理論與實務，頁 33-63，元照，2017 年 2 版。

3 侵害行為內涵與各救濟方式之詳細說明，請參同前註，第 6 章。

員工被挖角的情形下，亦得請法院禁止該員工任職於競爭對手⁴。

（二）刑事規範

因民事規範不足以嚇阻侵害者以商業間諜或挖角方式侵害我國廠商營業秘密，又刑法中妨害秘密、竊盜、背信等規定無法充分評價此等行為，故立法者於 102 年 1 月增訂營業秘密法之刑事規範。

修正後營業秘密法第 13 條之 1 規定，意圖為自己不法之利益，或意圖為第三人不法之利益，或意圖損害營業秘密所有人之利益而有⁵：

1. 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。2. 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。3. 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。4. 明知他人知悉或持有之營業秘密有前三種情形，而取得、使用或洩漏者。應處以 5 年以下有期徒刑或拘役，得併科新臺幣 100 萬元以上 1,000 萬元以下罰金。同條第 2 項並設有未遂犯之處罰規定，如侵害營業秘密行為人所得之利益超過罰金最多額，得於所得利益之 3 倍範圍內酌量加重；依同法第 13 條之 3 規定，本條之罪採告訴乃論。

同法第 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 1 年以上 10 年以下有期徒刑，得併科新臺幣（下同）300 萬元以上 5,000 萬元以下之罰金。本條之罪亦處罰未遂犯。

若發生法人之代表人、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 13 條之 1 及第 13 條之 2 之罪者，依第 13 條

4 如臺積電梁孟松案，請參智慧財產法院 102 年度民營上字第 3 號民事判決。另請參拙作，論我國引進營業秘密法不可避免揭露理論（*Inevitable Disclosure Theory*）之可行性與適用限制，萬國法律，第 203 期，頁 20-43，2015 年 10 月。

5 各罪名之詳細說明，請參拙作，同註 2，第 7 章。

之 4 規定除依各該規定處罰行為人外，對該法人或自然人亦科罰金。

二、我國競業禁止相關規範

競業禁止係指事業單位為保護其商業機密、營業利益或維持其競爭優勢，要求特定人與其約定在在職期間或離職後之一定期間、區域內，不得受僱或經營與其相同或類似之業務工作⁶。在我國法，競業禁止又可分為法定競業禁止與約定競業禁止。其中法定之競業禁止，依我國現行法之規定，有民法債篇的經理人及代辦商之競業禁止規定⁷，與公司法有關經理人的競業禁止等⁸。

約定之競業禁止，係指雇主與員工簽署之離職後競業禁止約款，目前已被普遍運用於營業秘密之保護。因競業禁止約款涉及雇主財產權與勞動者工作權兩個屬憲法保障權利之衝突，其有效性與判斷標準爭議不斷，一般認為應以雇主有營業秘密等值得保護利益為首要條件，再觀察約定限制之營業種類、地域、和禁止競爭之時間是否合理等四要件加以判斷⁹，然最高法院並未明確統一見解，故實務上仍有不同看法。

準此，立法者為使競業禁止約款有更明確之法源依據，以兼顧工作權與營業秘密之保障，於 104 年 11 月 27 日新增勞動基準法第 9 條之 1：「未符合下列規定者，雇主不得與勞工為離職後競業禁止之約定：一、雇主有應受保護之正當營業利益。二、勞工擔任之職位或職務，能接觸或使用雇主之營業秘密。三、競業禁止之期間、區域、職業活動之範圍及就業對象，未逾合理範疇。四、雇主對勞工因不從事競業行為所受損

6 請參閱行政院勞工委員會編，簽訂競業禁止參考手冊，頁 2，行政院勞工委員會印行，2013 年，<http://www.cla.gov.tw/site/business/414ea820/4899118b/files/data.pdf>，最後瀏覽日期：2018 年 06 月 27 日。

7 請參民法第 562 條。

8 請參公司法第 32 條、公司法第 209 條第 1 項。

9 有關競業禁止約款合理性要件之詳細討論，請參拙作，同註 2，第 5 章。

失有合理補償。前項第四款所定合理補償，不包括勞工於工作期間所受領之給付。違反第一項各款規定之一者，其約定無效。離職後競業禁止之期間，最長不得逾二年。逾二年者，縮短為二年。」規定，將競業禁止約款要件明文化。

由條文內容觀察，可知勞基法對合理性要件採四標準說，且規定四標準欠缺其一則競業禁止約款全部無效。然而，勞基法僅能適用於勞動契約，故委任、加盟連鎖關係等法律關係並不適用，仍應由法院個案判斷¹⁰。

三、出口管制相關規定

若我國廠商技術等營業秘密係受政府補助，或為具軍事國防意義之敏感科技，則我國廠商除可透過營業秘密法或競業禁止約款加以保護外，政府亦得管制各該技術之輸出。

（一）國家安全法

如敏感科技涉及公務上之應秘密事項，依「國家安全法」第 2 條之 1 規定：「人民不得為外國或大陸地區行政、軍事、黨務或其他公務機構或其設立、指定機構或委託之民間團體刺探、蒐集、交付或傳遞關於公務上應秘密之文書、圖畫、消息或物品，或發展組織。」從而該敏感科技不得擅自取得、交付。若意圖危害國家安全或社會安定違反該規定者，依同法第 5 條第 1 項規定，應處 5 年以下有期徒刑或拘役，得併科 100 萬元以下罰金。

10 有關加盟連鎖契約競業禁止之合理性判斷，請參王偉霖、楊孝文，加盟連鎖契約競業禁止條款之研究，華岡法粹，第 62 期，頁 1-47，2017 年 06 月。

（二）貿易法

貨品之輸出入行為及有關事項，如有危害國家安全或對公共安全之保障有妨害者，主管機關經濟部得依「貿易法」第 6 條第 1 項第 2 款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。如涉及戰略性高科技貨品之輸出，需另按「戰略性高科技貨品輸出入管理辦法」規定申請取得許可，並接受定期管控。然而，「貿易法」除第 27 條對違法輸出入戰略性高科技貨品設有刑罰規定外¹¹，其餘僅處行政罰鍰或停止出入口許可。雖貨品包括附屬其上之商標權、專利權、著作權及其他已立法保護之智慧財產權，但「貿易法」僅規範有形貨物之輸出入，不涉及無形技術。

（三）臺灣地區及大陸地區人民關係條例及其子法

依據臺灣地區及大陸地區人民關係條例（下稱兩岸人民關係條例）第 33 條規定，臺灣地區人民、法人、團體或其它機構，得擔任大陸地區法人、團體或其它機構之成員。故臺灣地區人民赴大陸工作，除明令禁止擔任大陸黨務、軍事、行政或具政治性機關、團體職務外，對於影響國家安全、利益之虞或基於政策需要者，原則上必須經主管機關許可。如有違反，依同條例第 90 條規定涉有刑事處罰，如為退休公務員違反者，依同條例第 90 條之 1，將喪失或停止請領退休金之權利。

另該條例第 35 條規定，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

11 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內容，請參經貿資訊網，https://www.trade.gov.tw/Pages/Detail.aspx?nodeID=1005&pid=472604&dl_DateRange=all&txt_SD=&txt_ED=&txt_Keyword=&Pageid=0，最後瀏覽日期：2018 年 06 月 27 日。

一般類，由經濟部會商有關機關訂定項目清單及個案審查原則，並公告之。但一定金額以下之投資，得以申報方式為之；其限額由經濟部以命令公告之¹²。違反者依同條例第 86 條規定得由主管機關命停止並處以罰鍰，屆期不停止，或停止後再為相同違反行為者，處行為人 2 年以下有期徒刑、拘役或科或併科 2,500 萬元以下罰金。

故而，臺灣人民擬前往中國大陸工作者，其許可或禁止之範圍，應另依「在大陸地區從事商業行為應經許可或禁止之事項公告」、「在大陸地區從事投資或技術合作許可辦法」等行政規則之規範，要件及申請方式不一。

反之，如為中國大陸人民來臺投資，按大陸地區人民來臺投資許可辦法之規定，投資人為大陸地區軍方投資或具有軍事目的之企業，應限制其來臺投資。中國大陸軍方以外人士來臺投資者，得投資之業別項目、限額及投資比率，由經濟部會商各中央目的事業主管機關及相關機關擬訂，報行政院核定。投資人所為投資之申請，或投資之經營有經濟上具有獨占、寡占或壟斷性地位；政治、社會、文化上具有敏感性或影響國家安全¹³；對國內經濟發展或金融穩定有不利影響等情形之一者，主管機關得限制或禁止投資申請，已投資經營者得撤銷或廢止其投資¹⁴。

（四）國家機密保護法

如廠商之技術涉及國家機密者，應依「國家機密保護法」規定核定機密等級及保密期限並為維護，如有洩漏者，即視具體情節依該法規定

12 請參經濟部投資審議委員會，https://www.moeaic.gov.tw/businessPub.view?lang=ch&op_id_one=5，最後瀏覽日期：2018 年 06 月 27 日。

13 請參經濟部投資審議委員會，具敏感性或國安（含資安）疑慮之業務範疇及陸資投資資訊產業事業清冊，https://www.moeaic.gov.tw/businessPub.view?lang=ch&op_id_one=3，最後瀏覽日期：2018 年 06 月 27 日。

14 請參大陸地區人民來臺投資許可辦法第 6 條、第 8 條規定。

科以刑罰¹⁵。相關人員未經核准而擅自出境或逾越核准地區者，依該法第 36 條規定，處 2 年以下有期徒刑、拘役或科或併科 20 萬元以下罰金。

（五）科技研發相關規定

我國廠商敏感科技係受政府補助研發所得，因在將敏感科技商業化時，為追求效益之最大化，常有與境外企業合作之必要，如合作對象外國人民，是否可以合作應視「科學技術基本法」之相關規定。惟「科學技術基本法」本文就政府補助研發之敏感科技得否為境外實施並無規範，而是授權各主管機關自行訂立辦法¹⁶，然目前行政院以及轄下各部會就執行單位研發成果運用現行有效之法規命令中，「政府科學技術研究發展成果歸屬及運用辦法」就得否境外實施並無規範，教育部「教育部科學技術研究發展成果歸屬及運用辦法」對境外實施採開放態度，其餘包含經濟部在內之科學技術研究發展成果歸屬及運用辦法多採須報部核准之設計¹⁷，如有違反，該敏感科技將被收為國有¹⁸。

除此之外，受政府補助研發之敏感科技，政府均按科技部 104 年提出之「政府資助敏感科技研究計畫安全管制作業手冊」，與我國廠商於資助契約約定遵守敏感科技保護並防止外洩之方式。其中關於敏感科技項目之增刪，由中央主管機關具明理由提報科技小組決定，並於手冊明列敏感科技項目，包括農業科技、製造業關鍵技術、航太及衛星科技、海洋科技、先進積體電路設計及製程技術等五大類¹⁹。

需特別指出的是，如敏感科技輸出地區為中國大陸，依陸委會「臺

15 請參國家機密保護法第 32 條至第 35 條規定。

16 請參科學技術基本法第 6 條第 3 項規定。

17 請參經濟部辦法第 16 條規定。

18 請參經濟部辦法第 21 條規定。

19 科技部網站，政府資助敏感科技研究計畫安全管制作業手冊，https://www.most.gov.tw/folksonomy/list?menu_id=3010c688-0cca-4d3b-8deb-e0296ddc9cbe&l=en，最後瀏覽日期：2018 年 06 月 27 日。

灣地區科研機構與大陸地區科研機構進行科技交流注意事項」第 2 點規定：「凡法令或國際協議所禁止或管制輸往大陸地區之產品或技術，不得與大陸地區科研機構進行科技合作或技術移轉。」第 3 點規定：「由政府機構資助辦理之科技研究計畫項目，資助機關應約束受資助機構在計畫進行中或計畫完成後二年內，均不得與大陸地區科研機構進行技術移轉。計畫完成二年後，如欲與大陸地區科研機構進行技術移轉，需向資助機關申請許可。」雖此注意事項僅為行政規則，位階劣後於上開所示法規命令，然此注意事項似又可解為特別規範，故於法規適用競合不免產生疑問，然在目前兩岸特殊關係下，仍宜按此注意事項進行較妥。

此外，若我國廠商與外國人民從事商業活動或是學術交流，也需自行依行政院頒佈之「科技資料保密要點」規定區分密等、採取保密要領及補救維護措施²⁰。

參、美國等國家及國際防範涉及國家安全、產業發展 關鍵技術和科技外流及人才挖角的法規及作法

美國等主要國家就商業間諜之防範，也是透過營業秘密法相關法規為之；在人才挖角方面，各國廠商也係以簽署競業禁止約定之方式加以預防，但各國就競業禁止合理性之規範與我國不盡相同。至於國際間防範涉及國家安全、產業發展關鍵技術和科技外流及人才挖角之作法則莫衷一是。本文以下將分別就美國等主要國家防範商業間諜、競業禁止，以及出口管制之規定為初步說明。

20 請參科技資料保密要點第 4 點至第 7 點條文。

一、美國與歐盟營業秘密法制

（一）美國

1. 民事規範

美國早期就營業秘密之民事保護，主要由各州以普通法（Common Law）中的不正競爭禁止原則、契約不履行及侵權行為予以處理²¹，後逐步形成 1939 年侵權行為法整編第 1 版、1979 年統一營業秘密法（Uniform Trade Secret Act, UTSA）、1995 年反不正競爭法整編第 3 版，對營業秘密定義與侵害行為均有規範²²，均認為只要行為人有以不正當方法取得、使用或洩漏他人營業秘密者，即構成營業秘密之侵害，且營業秘密所有人可以尋求禁制令之保護²³。

2. 經濟間諜法案

美國在 1980 年代末期共產主義解體之後，因鼓勵產業從事研發活動而成為商業間諜之主要目標，對美國經濟產生嚴重影響，後美國政府更發現許多商業間諜背後是外國政府及機構支持²⁴。為遏止商業間諜活動，美國國會終在 1996 年 10 月通過經濟間諜法案（The Economic Espionage Act of 1996，下稱 EEA），以聯邦刑法之方式保護營業秘密，列編為美國聯邦法典第 18 編刑法第 90 章，章名為「營業秘密之保護（Protection of Trade Secret）」。

21 請參王 奎，美中商業秘密內涵的思考，政法論壇（中國政法大學學報），第 25 卷，第 3 期，頁 101，2007 年 05 月。

22 請參王 奎，同前註，頁 101-102。

23 請參拙作，同註 2，第 6 章第 4 節。

24 請參劉博文，美國經濟間諜法簡介，2013 年 02 月 17 日，經濟部智慧財產局，<https://www.tipo.gov.tw/ct.asp?xItem=207083&ctNode=6740&mp=1>，最後瀏覽日期：2018 年 06 月 27 日。

EEA 第 1831 條定有經濟間諜活動罪²⁵，主要適用於外國政府、機構以及其代理人所支持之目標為竊取美國企業營業秘密之間諜行為。在本條規定之下，只要能證明行為人有裨益（Benefit）外國政府或機構之意圖或明知之犯意即可，至於該外國政府實際上是否獲取利益則非所問。本條之法定刑為 15 年以下有期徒刑，得併科 500 萬美元以下罰金；如果行為人為法人，得處 1,000 萬美元以下罰金或竊取營業秘密所得利益 3 倍罰金，包括因此所減免之研究發展費用或其他回復營業秘密之成本。

另第 1832 條規定竊取營業秘密罪²⁶，本條適用於任何與外國政府無關之商業機密竊取行為，著重於美國國內或跨國之一般竊取營業秘密案件，本罪主要規範者，為對於任何人故意或意圖將與州際或外國商務所製造或儲存之商品相關營業秘密，轉化為該營業秘密所有人以外之任何人之經濟利益之行為；惟需注意，只有行為人具意圖或明知其犯行將損傷營業秘密所有人之主觀犯意時始有本條之適用，且本條所指裨益（Benefit）僅限於經濟上的利益²⁷，故起訴的要件較經濟間諜活動罪嚴苛。本條之法定刑為 10 年以下有期徒刑，得併科 25 萬美元以下罰金；如果行為人為法人，得處 500 萬美元以下罰金或竊取營業秘密所得利益 3 倍罰金，包括因此所減免之研究發展費用或其他回復營業秘密之成本。

3. 2016 年保護營業秘密法（Defend Trade Secrets Act, DTSA）

雖美國多數州已有各自之營業秘密法，然各自州法時套用 UTSA 之模式立法時多有修改，從而各州法仍欠缺統一性²⁸，故營業秘密訴訟當

25 18 U.S.C. § 1831.

26 18 U.S.C § 1832.

27 William J. Edelman, *The “Benefit” of Spying: Defining the Boundaries of Economic Espionage Under the Economic Espionage Act of 1996*, 63 STAN. L. REV. 447, 468-474 (2011).

28 請參益思科技法律事務所，營業秘密法制之研究，頁 52，2003 年 12 月 31 日，經濟部智慧財產局，<https://www.google.com.tw/url?sa=t&rct=j&q=&esrc=s&source>

事人仍然要面臨各州相互衝突之法律標準以及不同訴訟程序規定之麻煩，美國法界遂有仿專利法、著作權法與商標法之模式制訂聯邦法之聲浪興起，後美國總統歐巴馬最終於 2016 年 5 月 11 日簽署 DTSA，正式將營業秘密納入聯邦法之規範範疇內²⁹。

依 DTSA 正式條文，DTSA 並未取消或排除各州州法對營業秘密民事訴訟之管轄權，且 DTSA 之主要框架並未跳脫 UTSA，諸如兩者間對於營業秘密之定義、以及金錢賠償、不當獲利、禁制令救濟、合理權利金、故意侵害（Willfully and Maliciously Misappropriate）他方營業秘密情形下之兩倍懲罰性賠償以及合理律師費等規定；然而，DTSA 對營業秘密之定義較廣³⁰，且增加部分創新之規定，如得單方聲請扣押不當取得之營業秘密³¹、吹哨者豁免條款³²，在損害賠償方面規定可請求 2 倍懲罰性賠償及律師費用³³，且有域外效力，使得企業或自然人在美國境外之侵權行為因 DTSA 受到追究³⁴。

（二）歐盟

歐盟就營業秘密之保護，原本係由各會員國自行立法，後歐盟議會為調合歐洲內部市場營業秘密規範以保護創新環境，維持歐洲企業競爭優勢，遂研擬營業秘密指令草案。後該草案於 2016 年 4 月 14 日通過，同年 7 月 5 日施行（Directive on the Protection of Undisclosed Know-How

=web&cd=2&cad=rja&uact=8&ved=0ahUKEwiKksbLv5jQAhWCWrwKHQMaDgAQFgghMAE&url=https%3A%2F%2Fwww.tipo.gov.tw%2Fdl.asp%3FfileName%3Df0f9aebef969-462b-8184-aaec45f0af56.pdf&usq=AFQjCNERBqrYinYVFL09KD3chucuz3y4dA&sig2=sEDM8fdNd0TDicjV9zCRpA，最後瀏覽日期：2018 年 06 月 27 日。

29 18 U.S.C. §§ 1836-1839.

30 18 U.S.C. § 1839.

31 18 U.S.C. § 1836(b)(2)(A).

32 18 U.S.C. §§ 1836(b)(3)(A)(i)(I), 1836(b)(3)(A)(i)(II).

33 18 U.S.C. §§ 1836(b)(3)(B), 1836(b)(3)(C), 1836(b)(3)(D).

34 18 U.S.C. § 1836(b)(1). 18 U.S.C. § 1837.

and Business Information (Trade Secrets) Against Their Unlawful Acquisition, Use and Disclosure，下稱營業秘密指令)，使各會員國據以立法落實指令要求，完善營業秘密之保護³⁵。

在營業秘密指令中，第 2 條就營業秘密之定義係採取與 TRIPS 一致之規定³⁶，第 16 條規定會員國得就侵害營業秘密之行為施加罰則³⁷，然較為特別的是，營業秘密指令第 3 條有明確規定不被視為侵害營業秘密之行為³⁸：「1. 營業秘密被視之為合法取得之情形，包括：(1) 獨立

35 完整指令內容，<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0943>，最後瀏覽日期：2018 年 06 月 27 日。

36 For the purposes of this Directive, the following definitions shall apply:

(1) ‘trade secret’ means information which meets all of the following requirements:

(a) is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;

(b) has commercial value because it is secret;

(c) has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.

37 Member States shall ensure that the competent judicial authorities may impose sanctions on any person who fails or refuses to comply with any measure adopted pursuant to Articles 9, 10, and 12. The sanctions provided for shall include the possibility of imposing recurring penalty payments in the event of non-compliance with a measure adopted pursuant to Articles 10 and 12. The sanctions provided for shall be effective, proportionate and dissuasive.

38 1. The acquisition of a trade secret shall be considered lawful when the trade secret is obtained by any of the following means:

(a) independent discovery or creation;

(b) observation, study, disassembly or testing of a product or object that has been made available to the public or that is lawfully in the possession of the acquirer of the information who is free from any legally valid duty to limit the acquisition of the trade secret;

(c) exercise of the right of workers or workers’ representatives to information and consultation in accordance with Union law and national laws and practices;

(d) any other practice which, under the circumstances, is in conformity with honest commercial practices.

2. The acquisition, use or disclosure of a trade secret shall be considered lawful to the extent that such acquisition, use or disclosure is required or allowed by Union or national law.

發現或創造者；(2) 對於已供公眾可取得之產品、或合法取得營業秘密之人就持有之營業秘密進行觀察、研究、拆解或進行測試；(3) 受雇人或勞工代表於符合法令及習慣下，行使資訊與諮商之權利者；(4) 符合商業誠信之行為。2. 依法律規定取得、使用、洩漏營業秘密者，視為合法。」此或可稱之為營業秘密之合理使用，為以成文法保護營業秘密國家之首見。

二、美國等主要國家就競業禁止之規範

世界各國就競業禁止規範亦多採合理性判斷標準，其要件大同小異，復因國情不同，對各標準認定之比重亦有不同，分述如下。

(一) 日本

在日本，競業禁止是否合理全由法院於個案中認定，而日本法院則明白地指出離職後競業禁止條款，應就合理之範圍，須在僱傭契約中約定。所謂合理應考慮的因素包括：1. 企業或雇主是否有競業禁止條款約定之必要性。2. 勞工在原雇主或企業之職務與地位。3. 限制勞工就業之對象、期間、區域及職業活動範圍。綜合判斷是否有無必要填補勞工因競業禁止損害之代償措施³⁹。然則並未硬性要求代償措施必需限於競業禁止期間內給付始足當之，除非綜合考量結果發現競業禁止之結果對員工造成的不利益，比起企業主應予保護的利益顯得不合理時，該條款即可能被認定為違反公序良俗而無效⁴⁰。

有關營業秘密指令草案之介紹，請參陳世傑，歐美營業秘密保護立法趨勢與對我國法制之啟示，科技法律透析，第27卷，第2期，頁66，2015年02月。

39 邱駿彥，競業禁止特約有效性認定基準之法理探討，華岡法粹，第48期，頁34，2010年11月。

40 請參謝銘洋、古清華、丁中原、張凱娜，營業秘密法解讀，頁91，月旦，1996年。

（二）德國

德國在民法與勞工法裡並沒有明文規範勞工離職後競業禁止契約之原則，反在德國商法（*Handelsgesetzbuch, HGB*）第 74 條以下就商人間競業限制有相當詳盡的規定⁴¹。然依照德國聯邦勞工法院判決及學者意見，德國商法之規定就受僱勞工之競業禁止約款也能適用⁴²。而依德國商法第 74 條、第 75 條之規定，德國商法對離職後競業禁止契約，有下列限制⁴³：1. 書面及交付受僱人為必要；2. 雇主應於競業禁止期間支付受僱人補償金，競業禁止約定始具拘束力⁴⁴；3. 競業禁止約定係為保護雇主必要之合法商業利益，否則該約定不具拘束力；4. 競業禁止約定不得對受僱人生計造成不公平與困難的情形；5. 競業禁止約定之期間不得超過二年；6. 受僱人離職前一年薪資總額若低於 1,500 馬克者，所為競業禁止約定無效；7. 競業禁止約款不得違反德國民法第 138 條之公序良俗；8. 受僱人為競業禁止約定時未成年人，其約定無效。

當事人間之競業禁止約定與德國商法規定相異，且較不利於受僱人者，僱用人不得對受僱人主張此等不利約定。然而，上開規定僅適用僱傭關係，根據德國商法第 75 條的規定，高薪者和歐洲以外工作之受僱人不適用離職後競業禁止約款和代償措施之間的法律規定。從而經理人等非純為僱傭關係之員工而言，競業禁止之內容與補償之合理性標準並不若一般屬於故傭關係之員工來的嚴格，從而可推知在德國法上，可能認為競業禁止約款之合理性標準可隨當事人間之關係不同而彈性調整。

41 黃程貫，最低服務年限與競業禁止條款，勞動基準法釋意－施行二十年之回顧與展望，頁 228-229，新學林，2005 年。

42 張聖怡、李素華、李雅萍，研究機構研發人員競業禁止問題研析，科技法律透析，第 13 期，頁 46-47，2001 年 03 月。

43 黃程貫，同註 41，頁 229。

44 高蘇弘，勞工離職後競業禁止約款有效性之研究，國立中正大學法律研究所碩士論文，頁 133，2007 年 07 月。

(三) 美國

目前美國大多數州法院認為競業禁止條款若符合「合理原則」(Rule of Reason)，則承認其效力⁴⁵，有幾個州政府如德州、威斯康辛州、佛羅里達州、密西根州、路易斯安那州，以及南塔科達州，則將競業禁止約款的檢視標準納入成文法中⁴⁶。

而不論有無將競業禁止約款合理性標準納入成文法，各州在檢視競業禁止約款合理性時大多均是檢視下列要件⁴⁷：1. 雇主有合法的商業利益（包含營業秘密、機密資訊和商譽）；2. 期間和地域範圍需有合理的限制；3. 有給予合理補償；4. 不違反公共利益。值得一提的是，加州政府對於競業禁止約款的認定相當嚴格，該州商事與職業法（Business and Professions Code）第 16600 條規定：「除本章另有規定外，任何限制契約相對人或第三人從事合法職業、交易、業務之契約無效⁴⁸。」惟本條仍有例外規定，亦即當公司出售、股票出售以及解除合夥關係時，競業禁止約款仍可適用⁴⁹。雖然加州州法如此規定，實務上法院仍會禁止離職員工使用或揭露前雇主的營業秘密⁵⁰。

45 See Jason S. Wood, *A Comparison of the Enforceability of Covenants Not to Compete and Recent Economic Histories of Four High Technology Regions*, 5 VA. J. L. & TECH. 14, 29-44 (2000).

46 Texas Business & Commerce Code § 15. 50., Wis. Stat. Ann. § 103.465., Flo. Stat. Ann. § 542. 335., Michigan Compiled Laws § 445. 774a., Lou. Rev. Stat. § 23:921., S. D. Codified Laws § 53-9-11.

47 See Christine M. O'Malley, *Covenants Not To Compete in the Massachusetts Hi-Tech Industry: Assessing the Need for A Legislative Solution*, 79 B. U. L. REV. 1215, 1219-1221 (1999). *Blue Ridge Anesthesia & Critical Care, Inc. v. Gidick*, 239 Va. 369, 371-2 (Va. 1990). See Michael L. Agee, *Covenants Not To Compete in Tennessee Employment Contracts: Almost Everything You Wanted to Know but Were Afraid to Ask*, 55 TENN. L. REV. 341, 363, 371-378 (1988).

48 Business and Professions Code § 16600.

49 Business and Professions Code §§ 16601-16607.

50 See *State Farm Mutual Automobile Ins. Co. v. Dempster*, 174 Cal. App. 2d 418 (Ct. App. 1959).

三、美國、歐盟、韓國、日本就涉及國家安全、產業發展關鍵技術和科技出口之限制

(一) 美國

美國就涉及國家安全、產業發展關鍵技術和科技出口管制制度的法律基礎為「出口管理法 (Export Administration Act, EAA)」、「武器出口管制法 (Arms Export Control Act, AECA)」、「國際緊急經濟權力法案 (International Emergency Economic Powers Act, IEEPA)」等，主要可以分為以下兩部分：1. 用於軍事或國防目的產品和技術的出口管制（軍事出口管制）；2. 軍民兩用產品和技術的出口管制（商業出口管制）。

其中，軍事出口管制由美國國務院（即外交部門）負責，具體受管制的產品項目，則以國務院頒布「武器國際運輸規則 (International Traffic in Arms Regulations, ITAR)」所包含「美國軍品管制清單」(United States Munitions List, USML)⁵¹。而在商業出口管制方面，主要包括核、生化、電子設備等敏感物項和技術的管制，目前由美國商務部產業及安全局 (Bureau of Industry and Security, BIS) 主導，並以其制定的「出口管理條例 (Export Administration Regulation, EAR)」為法律依據。

在實際運作上，美國商業出口管制主要通過對特定產品和特定對象（包括特定的國家、社團組織、公司、個人）的禁運來進行管控⁵²；而被禁運的產品或對象主要係以 BIS 制定之商業控制清單 (Commerce

51 See <https://www.law.cornell.edu/cfr/text/22/121.1>, last visited 06.27.2018.

52 管制方式的設計上，主要從出口行為所涉及產品來源、最終送達地、最終用途、最終使用者考量，請參華冠國際顧問有限公司，美、日、歐盟對無形技術管制之法令規定、作法及我國推動無形技術管控之可行性研究，2011年03月，<https://www.trade.gov.tw/Pages/Detail.aspx?nodeID=830&pid=320227>，最後瀏覽日期：2018年06月27日。

Control List, CCL) 對出口產品進行分類，主要包含十大行業與包含了大部分商業產品⁵³。如果外國人擬與美國廠商交易清單內物品，需要在取得出口許可證後始可進行交易。惟 BIS 對於各類型產品都有細部的禁運標準，並就每一商品標誌出口管制級別，管制原因與核發許可證之標準。

而在許可證之申請上，主要係由出口商向 BIS 申請許可，其中涉及與技術出口有關的許可證類別，包括視為出口之外國人身分審查 (Foreign National Review for Deemed Export, FNR)、限制類技術與軟體許可 (Technology and Software under Restriction, TSR)、非限制類技術與軟體出口許可 (Technology and Software Unrestriction, TSU)、加密商品軟體及技術許可 (Encryption Commodities, Software and Technology, ENC)、電腦類許可 (Computers, APP)、暫時進出口及再出口許可 (Temporary Imports, Exports, and Reexports, TMP)、航空器及船舶許可 (Aircraft and Vessels, AVS)、附加許可再出口證 (Additional Permissive Reexports, APR) 等⁵⁴。而具體審查程序相當複雜，包括政府部門磋商 (Government-to-Government assurances)、多方審查 (Multilateral reviews) 等，蓋因 BIS 在收受出口申請後，多會將申請案會同其他更加熟悉該產品和技術的相關部門，包括美國國務院、國防部、能源部，甚至美國國家航空局，中央情報局等進行審查⁵⁵。

如欲有未經允許出口禁運貨品、技術之行為者，得對行為人處以罰鍰、取消出口優先權與命令禁止從事 BIS 相關之代理、會計、諮詢、貨物運送、申請許可等業務。處罰鍰時得同時附加 1 年以下禁止申請或吊

53 詳請參 BIS 網站，<https://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear>，最後瀏覽日期：2018 年 06 月 27 日。

54 EAR § 740.

55 EAR § 750.3.

扣許可證及限制使用除外條款，以及緩期支付等條件⁵⁶。且就明知而違反或企圖違反 EAA、EAR 及所發布的命令或許可者設有刑罰，對行為人科以相當於出口所涉價值 5 倍或美金 5 萬元以下罰鍰（依較高者），或處或併處 5 年以下有期徒刑⁵⁷。如明知而違反或企圖違反 EAA、EAR 及所發布的命令或許可而出口，且知悉出口目的地為管制地區，除對個人出口外，應科以美金 25 萬元以下罰鍰，或處或併處 10 年以下有期徒刑⁵⁸。經依 EAA、EAR 核發許可證對管制國家出口、明知該出口目的為違反許可條件之軍事或情報用途、故意不對國防部報告者應科以相當於出口所涉價值 5 倍或美金 100 萬元以下、或對個人違法者處美金 25 萬元以下罰鍰（依較高者），或處或併處 5 年以下有期徒刑⁵⁹。

然而，在當今商業活動下，欲取得敏感科技者不一定必得透過技術之出口始能達其目的，以跨境投資之方式直接入主擁有敏感科技之廠商亦可。美國為避免外國人士循此途徑損害其國力，於 1988 年通過 1950 年國防製造法 (Defense Production Act of 1950) 第 721 款 The Exon-Florio 修正案，授權政府組成外資投資委員會 (Committee on Foreign Investment in the United States, CFIUS)，審查外資併購交易，並在發現有危及美國國家安全或可能產生損害時向總統報告，讓總統有權阻擋該已提議或進行之美國企業與外國企業之兼併、合併或收購等業務，以防危及國家經濟與軍事安全並致科技技術外流。

總統若欲引用此修正案所賦予之權利，必需在取得已取得「可信證據 (Credible Evidence)⁶⁰」下作為前提，並且表明「若取得控制權的外國利益企業所採取的行動可能會威脅到國家安全 (Foreign Interest Exercising Control Might Take action that Threatens to Impair the National

56 EAR § 764.3.

57 EAR § 764.3.

58 EAR § 764.3.

59 EAR § 764.3.

60 P.L. 100-418, Title V, Section 5021 Aug., 23, 1988; 50 USC Appendix sect. 2170.

Security)⁶¹」，始可暫停或中止該項業務交易，以阻止或解除外國企業、外國公司對美國企業所進行收購交易行為。嗣後，美國在 2007 年簽署「外國投資和國家安全法」(The Foreign Investment and National Security Act of 2007, FINSA)，針對外國投資安全審查項目再為修正，包括加強國家安全概念、完善 CFIUS 審查與監督職責，令 CFIUS 對於退出審查之交易業務持續採取追蹤調查。

在 FINSA 修正通過後，美國刻正研議「外國投資風險審查現代化法案」(the Foreign Investment Risk Review Modernization Act of 2017, FIRRMA)。旨在推展 CFIUS 現代化改革，限制外資對美國科技公司和基礎設施的投資，以維護國家安全，將再擴大 CFIUS 管轄權與權力、及美國關鍵技術與基礎設施投資審查，並令 CFIUS 審查時要增加國家安全風險考量因素，此一修正對政府而言固有正面意義，但仍有批評此將破壞出口審查制度，並將使 CFIUS 不堪重負，且在事事皆審查的情況下，將使外資卻步，進而損害美國追蹤關鍵技術的能力⁶²。

總體而言，美國管制敏感技術機制運作相當有效率，例如中國大陸極力扶植之中興通訊，於 2012 年間被路透社揭露其私下將依美國法應受管制之貨品銷售至伊朗，美國政府隨即進行調查，惟中興通訊於期間不止隱匿資訊、提供偽證與誤導調查，甚至透過第三方持續銷售管制貨品予伊朗、北韓等戰略性高科技貨品管制輸出地帶。嗣後中興通訊更被發現其內部控制幾乎失靈，竟將銷售計劃、規避方案、參與人員以及法律風險等機密文件置於多數員工可下載的位置⁶³。

61 請參鄭嘉文、許祐寧，跨境投資技術保護與營業秘密之法制研析，科技法律透析，第 29 卷，第 12 期，頁 40，2017 年 12 月。

62 請參壹讀網，CFIUS 改革法案因涉嫌出口管制遭到美國商業界反對，2017 年 11 月 30 日，<https://read01.com/nxDk767.html>，最後瀏覽日期：2018 年 06 月 27 日。

63 請參曾志超，從中興制裁案看 SHTC 管制，國政評論，2018 年 03 月 15 日，<https://www.npf.org.tw/printfriendly/18677>，最後瀏覽日期：2018 年 06 月 27 日。另請參美國會通過 CFIUS 擴權 嚴審中資收購，自由時報，2018 年 05 月 24 日，

雖中興通訊後於 2017 年 3 月以繳納近 12 億美金罰款，承諾解雇、處罰涉案員工等條件與美國政府和解，惟事後並未依和解條件履行，美國政府即於 2018 年 4 月禁止中興通訊從美國出口敏感科技，且禁止美國企業向中興通訊提供零件，切斷其關鍵供應鏈，時間長達 7 年。而在中興案後，美國國會通過法案擴大 CFIUS 職權，賦予 CFIUS 更大權力審查任何可能對國家安全帶來威脅的外資收購美國企業案，包括緊縮對中資收購美國敏感科技的國安審查、加強出口管制等。

由以上案例可知，美國對戰略性高科技貨品之輸出入管制向來十分注意，近幾年來更逐步擴散至影響國家、經濟安全之敏感科技，而在 The Exon-Florio 修正案、FINSIA 法案修正後，美國賦予主管機關 CFIUS 之權限更大，更可以即時地對敏感科技管制加以處理。

（二）歐盟

歐盟早在 2000 年 6 月 10 日歐盟 EC 第 1334/2000 號規則即建立關於軍民兩用品及技術出口管制規範，後為促進會員國國內立法與國際間無形技術出口管制的規定接軌，特重新修訂 EC 第 1334/2000 號規則，於 2009 年 5 月 5 日通過 EC 第 428/2009 號規則以取代之⁶⁴。然歐盟各項規則主要內容除聲明出口管制之必要性及定義出口、出口人之內涵外，多著重在會員國間應如何立法以遵循歐盟出口管制目的，以及會員國通報及諮商、協調機制，以免各會員國彼此之出口管制制度衝突。當時歐盟各會員國中以英國之制度較為健全，故以下簡述英國之相關規定。

英國實施出口管制之法源依據為 2002 年出口管制法（The Export Control Act of 2002）」及其子法 2008 年出口管制令（The Export Control

<http://news.ltn.com.tw/news/business/paper/1203235>，最後瀏覽日期：2018 年 06 月 27 日。

64 詳細內容請參同註 52。

Order) 及貨品出口、技術出口及境外技術協助管制令 (The Export of Goods, Transfer of Technology and Provision of Technical Assistance (Control) (Overseas Territories) (Amendment) Order) 等。管制內容為 7 大管制表，歐盟清單亦包括在內⁶⁵。惟英國有特別規定通常科學研究之資訊交換；可普遍由公眾取得之資訊之產出；可普遍由公眾取得之資訊之交換等不得限制⁶⁶。屬公共領域者；或因非屬軍用物品或軟體、及非屬英國管制軍商兩用物品或軟體之安裝、操作、維護或修復所需，申請專利所需，或屬基礎科學研究所需者之最低技術；以及公共領域之軟體或技術出口不受管制⁶⁷。

關於英國管制無形技術出口之範圍，就內容而言，7 大管制表組成之出口管制清單中與技術相關者均屬之；出口的型態包括口頭溝通、電子傳遞、技術協助及一切與技術之發展、使用相關之行為；對象包括任何英國境內外實際進行或掌控出口之自然人、法人、學術研究機構等；至地域方面，全世界均在管制範圍內⁶⁸。

受理無形技術出口許可申請及核發許可或駁回申請之主管機關為隸屬於企業創新技能部 (Department of Business, Innovation and Skills, BIS) 之出口管制組織 (Export Control Organisation, ECO)。決定對申請案件予以准駁前，出口管制組織須先將申請案知會外國事務辦公室 (Foreign and Commonwealth Office, FCO)、國防部 (the Ministry of Defence, MoD) 及國際發展部 (the Department for International Development, DfID) 等機關出具審核意見，再依據審核意見決定許可與否。

65 UK Strategic Export Control Lists, <https://www.gov.uk/guidance/k-strategic-export-control-lists-the-consolidated-list-of-strategic-military-and-dual-use-items>, last visited 06.27.2018.

66 The Export Control Act of 2002 § 8(1).

67 The Export Control order § 18.

68 The Export Control Act of 2002 § 2(2)(6). 另請參同註 52。

英國出口管制之特色在於許可證申請均必須透過專屬網站 SPIRE 辦理線上申請⁶⁹，但無形技術出口方面關於英國境內人彼此間之出口管制技術行為、境外英國人之出口管制技術行為、及管制之技術協助行為，則需以書面向出口管制組織申請許可⁷⁰。且英國有由 ECO 出版發行 Compliance Code of Practice 協助國內企業對出口主管人員實施訓練及增強內部法令遵循⁷¹，然英國在協助企業實施訓練過程中，發現事實上符合應辦理無形技術出口管制的情形較預計中為少，原因在許多無形技術出口情況均屬於除外不需規範的情形。

就無形技術違法出口之裁罰，依據 2002 年出口管制法第 7 條(1)(g) 規定可處以最高 10 年有期徒刑；依 2008 年出口管制令規定，對簡式起訴獲有罪判決者，處罰金或科或併科 6 個月以下拘役；對正式起訴獲有罪判決者，處罰金或科或併科 2 年以下有期徒刑。實務上，英國稅務及關務總署對於違法行為亦可施以沒收、或達成行政和解，以取代檢察官起訴。

而在具體案例部分，目前經主管機關公告可查得之裁罰案例中，所涉之違法情事均為有形物體之違法出口，尚無違反技術出口管制者，故尚難以此觀察實施成效⁷²。

(三) 韓國

韓國曾發生多起敏感科技因外資剝削而外流之事例，礙於國內產業

69 SPIRE 官網，<https://www.spire.trade.gov.uk/spire/fox/espire/LOGIN/login>，最後瀏覽日期：2018 年 06 月 27 日。

70 Guidance on Supplementary Weapons of Mass Destruction End-Use controls, available at <https://www.gov.uk/guidance/supplementary-wmd-end-use-controls#contents>, last visited 06.27.2018.

71 Guidance on Export control: compliance code of practice, 2012/11/23, available at <https://www.gov.uk/government/publications/compliance-code-of-practice>, last visited 06.27.2018.

72 請參華冠國際顧問有限公司，同註 52。

保密技術不足，難以證明技術外流，且無法針對此等行為定罪等主要原因⁷³，在國民強烈要求之下，於 2006 年間制定「防止產業技術外流及產業技術保護法」（下稱產業技術保護法），希望能遏止外資透過併購，或技術交流之名實則竊取韓國企業技術⁷⁴。

在架構設計上，產業技術保護法是授權韓國產業通商資源部組成產業技術保護委員會，主要任務在決定國家核心技術項目。該法所稱國家核心技術為「具備國家與海外市場的經濟價值、或存在高度成長潛力，若是洩漏至海外可能對國家安全與國民經濟發展產生不利之影響⁷⁵」之技術。在認定上是由各中央行政首長得綜合考量國家安全、國民經濟、產業技術的海內外市場比率及相關技術領域之趨勢，在最小必要限度內指定之⁷⁶，換言之，國家核心技術項目並非一成不變，而是處於可由主管機關決定、變更或撤銷之狀態。

韓國產業通商資源部在產業技術保護委員會指定國家核心技術後負責處理之事務有：1. 制訂並執行通盤計劃；2. 指定、變更及取消國家核心技術事項；3. 管制出口的國家核心技術；4. 管制擁有國家核心技術機構的海外收購併購；及 5. 其他防止外流及保護產業技術事項等五大項，目前重點工作項目在管制擁有國家核心技術企業的海外併購。依產業技術保護法規定，擁有國家核心技術的產業機構，不論是主動或被動所為的海外收購或併購，應向韓國產業通商資源部報告；若海外收購併購將嚴重影響國家安全，韓國產業通商資源部得採取必要措施，要

73 請參自由時報，產業關鍵技術審查韓國可當借鏡，2010 年 02 月 22 日，<http://news.ltn.com.tw/news/business/paper/374577>，最後瀏覽日期：2018 年 06 月 27 日。

74 請參顏思妤，跨國惡性關廠的永豐餘集團何以有恃無恐？，2015 年 04 月 06 日，<https://www.tahr.org.tw/news/1577>，最後瀏覽日期：2018 年 06 月 27 日。

75 請參鄭嘉文、許祐寧，同註 61，頁 43。

76 請參詹世榕，國際間關於研發國際化所涉事項之規範研析，科技法律透析，第 23 卷，第 7 期，頁 59，2011 年 07 月。

求中止、禁止或回復原狀，過程應給與陳述並聽取意見。

在實際運作上，產業技術保護法對國家核心技術之管制密度，係以有無受國家補助作為區分。如國家核心技術受有國家補助，則企業若欲向海外出售、移轉此等技術，需事先申請許可；若未受有國家補助，則採事後報備制，但產業通商資源部長有疑慮時，得於會商相關中央行政機關首長，並經產業技術保護委員會審議，要求必須暫緩、禁止輸出或回復原狀。由產業技術保護法僅針對後者賦予向主管機關表示意見之機會，即可知受有國家補助國家核心技術之管制較為嚴格⁷⁷。

如企業違反產業技術保護法規定，經產業通商資源部向產業技術保護委員會提出，查證屬實，並經產業技術保護委員會審議後，得暫緩、禁止技術輸出或回復原狀等措施。而若是以竊盜、詐欺、恐嚇或其他不正方式，取得、使用或洩漏產業技術於公眾之行為，產業技術保護法對此設有刑罰規定⁷⁸。

韓國產業技術保護法於實際執行上如何適用，或許因為議題敏感性較無公開資料可獲得。但由韓國產業通商資源部 2009 年 10 月公佈查獲之韓國人與外國人或與外國企業相關的 21 起科技盜竊案中，以及其後於 2011 年時，由韓國光州地方法院針對韓國三星電子合作公司代表竊取百餘項三星冰箱核心技術，並試圖將這些技術帶往中國大陸之行為判處 1 年 6 個月有期徒刑之態度看來，韓國對於管制敏感科技外流之態度相當積極⁷⁹。

77 請參同前註。

78 請參鄭嘉文、許祐寧，同註 61，頁 45。

79 請參文龍，韓國三星百項核心技術險洩中國，大紀元日報，2011 年 01 月 06 日，<http://www.epochtimes.com/b5/11/1/6/n3134552.htm>，最後瀏覽日期：2018 年 06 月 27 日。

（四）日本

目前日本出口管制法律依據為「外匯與外國貿易法」；日本出口管制事務由經濟產業省管轄，戰略貨品出口管制主要由經濟產業省轄下貿易經濟協力局安全保障貿易管理課負責審核，另由轄下貿易經濟協力局貿易管理部所設安全保障貿易檢查官室辦理企業內部遵循規定諮詢及調查違法出口事宜，藉由審查企業提出之自我檢查表、對企業進行不定期抽查等程序，於發現違法情事，得對發出警告並要求改善，對逾期無法改善者，並得撤銷其三年概括出口許可證。

「外匯及外貿法」第 25 條、第 48 條分別規定管制技術及服務出口與管制貨物出口之原則⁸⁰。至於具體限制項目，則由主管機關訂定政令（Cabinet Orders）及省令（Ministerial Orders）分別規範限制貨物與技術清單及限制品目之詳細規格。

大體上，日本出口管制係將管制對象分為 16 類，採清單管制以及全面管制兩大方面，前 15 類與大規模破壞性武器或與通常武器相關者採清單管制，管制對全球各地之輸出行為。第 16 類則採全面防制，除由經濟產業省判斷後通知提出申請外，出口者在出口前亦需先自行就使用者及使用用途進行評估，若有用於大規模毀滅性武器等開發之虞者即需申請許可⁸¹。從而，既全面管制既然須先由出口人自行判斷應否申請出口許可，故日本政府會提供足夠的支援及資訊，令出口人自行評估，且日本政府有公告輸出對象白名單，故若無用於大規模毀滅性武器等開發之虞且輸往白名單地區者，應不受限制。

80 條文內容請參閱 http://elaws.e-gov.go.jp/search/elawsSearch/elaws_search_lsg0500/detail?lawId=324AC000000228&openerCode=1#289，最後瀏覽期：2018 年 06 月 27 日。

81 請參產業經濟省貿易管理部，日本出口管制制度概要，2015 年 11 月，http://supportoffice.jp/outreach/2015/taipei/pdf/METI_Mr.Shimokawa_C.pdf，最後瀏覽日期：2018 年 06 月 27 日。

而在申請程序上，日本之出口許可程序，無論貨物出口或技術出口，一律向經濟產業省提出申請，並由經濟產業省審核決定是否核發許可，流程尚稱簡便。而出口許可分二大類：一是由經濟產業省審查而逐案取得出口許可的「個別許可」；另一種是出口人經自主管理足可擔負審查時，且屬輸往特定地區的之特定貨物，無須逐案個別許可之「概括許可」⁸²。

如有違法出口之情形，按 2017 年 5 月 17 日通過修正「外匯與外國貿易法」第 69 條之 6 規定，就未經許可就出口需要獲得許可的物品或技術時係採兩罰制。一般人洩漏大規模具破壞性武器者之技術者，最高處 3 千萬日圓或輸出價格的 5 倍；洩漏一般武器技術者，最高處 2 千萬日圓或輸出價格的 5 倍；洩漏其他技術者最高處 1 千萬日圓或輸出價格之 5 倍；至於針對法人則規定針對洩漏大規模破壞性武器最高處 10 億日圓或輸出價格之 5 倍；洩漏一般性武器最高處 7 億日圓或輸出價格的 5 倍；洩漏其他技術則最高可處 5 億日圓或輸出價格之 5 倍。另亦將有 3 年內禁止出口、提供技術之行政處罰⁸³。

與美國相同，日本為了防止與國家安全相關的高端技術流出海外，日本參議院於新修正「外匯與外國貿易法」內規定外資企業等在取得擁有軍事、原子能等領域之高端技術的日本上市或非上市公司逾 10 % 的股份時，有義務向事前向日本政府申告，並接受審查。如有違反，日本政府將強制命令售出已取得的股票，且對違反「外匯與外國貿易法」洩漏高科技至海外公司之董事、代表、經理等從業人員，將禁止其轉任其他公司或獨立從事相同業務⁸⁴。

然因日本「外匯與外國貿易法」甫修正，目前尚無從查知其運作成

82 同前註。

83 請參經濟產業省，http://www.meti.go.jp/policy/anpo/kojinyushutsu_chinese.html，最後瀏覽日期：2018 年 06 月 27 日。

84 請參鄭嘉文、許祐寧，同註 61，頁 39-40。

效，有待日後觀察。

（五）小結

據以上所述各國實施無形技術出口管制之方式，可以發現各國對於技術出口管制，均有完整之規範體系，美國、英國係就技術出口管制各項細節分別制定法律位階之規範，而日本及韓國則是分別制定「外匯與外國貿易法」、「防止產業技術外流及產業技術保護法」為管制技術交易之母法，在據此授權機關訂定子法規範相關細節。

此外，各國就技術出口管制之範圍較貨物出口管制為廣，幾乎涵蓋所有可能的輸出入行為態樣，且管制之內容涵蓋技術與軟體。而在管控目的上，各國均兼具國家安全與國家利益之目的，其中國家利益部分，重在考量保護國內技術優勢與經濟競爭力。

而在具體運作上，各國均設置專責單位來統籌敏感科技之管制業務，諸如美國的 CFIUS、英國的 ECO、韓國的產業通商資源部及日本的經濟產業省，而由各該專責單位來橫向連結其他業務主管機關來進行出口許可證之核發、出口管制執法、違法查緝等管制業務。至於出口許可審查方式，則多採單一窗口之方式處理。

在處罰行為上，美國、日本、英國均採行政罰與刑罰兩罰體制，可分別由行政機關處罰或經由司法機關審理後判決。

準此，可知世界各國就敏感科技均有採取管制措施，以維護國家安全與經濟，其作法雖各有不同，應係因各國環境背景不同所致，無關優劣，我國日後制定相關法律時，均可做為借鏡。

肆、我國因應作為與修法建議

如上所述，我國與世界各主要國家為防止技術外流，在制度設計上不外乎採防止直接竊取，出口管制及投資審查等方式。就前者而言，各國均係透過營業秘密法制給予保護，而就後者，則依賴出口及投資審查

等相關法規處理。以下將分別針對我國相關法制設計衍生之問題加以說明，並提出建議。

一、我國營業秘密法制之相關問題與因應作為

首先，在營業秘密相關法制方面，我國營業秘密法固賦予營業秘密所有人有對包含以違反競業禁止約款等不正方法侵害營業秘密者提起民事救濟之權，且得提出刑事告訴，雖營業秘密法之規範意旨甚佳，但營業秘密所有人在實務上獲得保障之效果不明顯，原因主要在於舉證責任，營業秘密刑事規範要件不明確，既有刑事規範未能有效規範域外犯罪之故，分述如下。

首先，當營業秘密所有人就侵害營業秘密行為發動民刑事訴訟時，法院或檢察官在審酌被告所為是否該當各該民刑事責任構成要件前，必先令營業秘密所有人證明遭侵害之營業秘密存在，且法院將依營業秘密法第 2 條規定判斷營業秘密所有人所主張之資訊是否具備秘密性⁸⁵、價值性、以及合理保密措施等要件⁸⁶。而在營業秘密所有人證明營業秘密存在之後，就需要證明所受損害之範圍為何。

由現可查得之法院見解觀察，法院對證明營業秘密存在之審酌重點多在是否具有秘密性⁸⁷，並進而推斷是否具有價值性，故營業秘密所有人證明秘密性之難度，將影響侵害者應否負責之機率。因營業秘密秘密性係指「非一般涉及該類資訊之人所知者」，此一要件屬於消極事實，

85 秘密性要件並非指營業秘密需前所未見，而是只要處於秘密狀態，非一般涉及該類資訊之人所之即可，拙見以為應稱新穎性較為妥適，然未避免與專利新穎性混淆，故本文以秘密性稱之。詳細說明請參拙作，同註 2，第 2 章第 2 節。

86 請參拙作，我國營業秘密法刑事規範的再思考，法令月刊，第 68 卷，第 5 期，頁 66-69，2017 年 05 月。

87 臺灣士林地方法院 102 年度自字第 14 號刑事判決，臺灣新北地方法院 103 年度聲判字第 124 號刑事裁定，臺灣苗栗地方法院 104 年聲判字第 6 號刑事裁定。

於舉證責任之分配上，主張消極事實之當事人並不需證明消極事實存在，而應是由對造舉證證明消極事實不存在。從而慮及營業秘密秘密性要件之特性，認為只要營業秘密所有人能舉證證明該當秘密性之表面事實，即應由侵害者就已為「一般涉及該類資訊之人所知」負舉證責任，以調和營業秘密所有人之保護。

在民事訴訟中，此一舉證責任之調整並無太多爭議，但在刑事訴訟若調整只要求告訴人或檢察官證明營業秘密之秘密性、價值性存在之表面事實，即說明該營業秘密為何不為一般涉及該類之人所知，並因此推定具有價值性，不要求證明秘密性及價值性確實存在，或許將與刑事訴訟法有所抵觸，因此如同不要求告訴人或檢察官去證明確有受侵害之營業秘密存在。蓋因營業秘密所有人或檢察官依刑事訴訟法之規定需負積極之舉證責任，或其指出證明之方法⁸⁸，否則基於無罪推定之原則，不得推斷行為人有犯罪行為。然本文以為縱然為如此調整，營業秘密所有人或檢察官就行為人有不法意圖之主觀要件以及其他客觀構成要件之存在仍須負積極之舉證責任，故此一調整實質上並未陷行為人於不利之地位，且可增加法院認定營業秘密存在之空間，而將訴訟攻防之重點移轉至主觀意圖與行使、洩漏等行為態樣之討論，對我國營業秘密刑事規範之發展將有助益，故此一舉證責任之調整未必不是可考慮之方向。

而在損害賠償計算方面，雖我國營業秘密法第 13 條定有請求損害賠償之計算方法，包含所受損害與所失利益、受害前後使用營業秘密所獲得利益之差額、侵權人侵害行為所得利益，以及懲罰性違約金等四種⁸⁹。然而，此四種損害賠償計算方式各有利弊，未必準確也未必能反映營業秘密所有人遭侵害當下受損之嚴重程度，且若營業秘密所有人就損害程度舉證不足，甚有可能出現法院以無損害駁回請求之窘境。惟對照美國 DTSA 規定，法院在計算營業秘密所有人之損害時，除得按實際損

88 請參刑事訴訟法第 154 條、第 161 條第 1 項規定。

89 有關侵害營業秘密損害賠償計算方法之詳細內容，請參拙作，同註 2，頁 107-112。

失、不當得利計算外，亦可以用合理權利金計算營業秘密所有人之損害範圍⁹⁰。亦即營業秘密所有人無法證明有實際損害或不當得利存在，但可證明侵害者已將竊取之營業秘密用以改善製程，或尚未因竊取營業秘密而得利時，法院可判決侵權人應支付營業秘密所有人合理之權利金⁹¹。本文以為，DTSA 規定得以合理權利金計算損害賠償，將使營業秘密所有人求償及法院判決內容更有彈性，也能適當調整營業秘密所有人就受損範圍之舉證程度。因此認為 DTSA 以合理權利金計算損害賠償之設計，值得作為我國營業秘密法第 13 條未來修正之參考。

其次，營業秘密法第 13 條之 1 有構成要件不明確，有處罰過廣之疑慮，可能使法官本於「刑法謙抑」之原則，於涵攝構成要件時偏向採取對被告有利之解釋，進而難生嚇阻商業間諜行為之效。如營業秘密法第 13 條之 1 第 1 項第 1 款雖定有「竊取、侵占、詐術、脅迫、擅自重製」等行為，但僅為例示規定，若法院於具體個案中發現侵害營業秘密之人所使用之方法雖非為本項例示之行為，但屬於「不正方法」者，仍有本條之適用，惟不正方法範圍過廣，難以定義。就此等問題，基於刑法法律明確性之要求，應盡量避免使用「其他不正方法」等不確定法律概念適用之機會，故建議應仿上開 EEA 第 1832 條(a)項第 1 款至第 3 款之規定，盡量特定應予刑罰之行為態樣或為嚴格或限縮解釋，以符合刑罰明確性之要求，降低爭議⁹²，故以為於未來修正時似可將本條第 1 款「重製或其他不正方法」修正為「未經授權而重製、複製、筆記、描繪、攝影、下載、上載、刪改、毀損、影印或其他不正方法」，藉以大幅降低使用不確定法律概念之機會，使營業秘密行為規範禁止之行為更為明確，令法官於判決時有所依歸，避免侵害者因構成要件不明確而獲益於

90 18 U.S.C. §§ 1836(b)(3)(B), 1836(b)(3)(C), 1836(b)(3)(D).

91 *See Linkco, Inc. v. Fujitsu Ltd.*, 232 F. Supp. 2d 182 (S.D.N.Y. 2002).

92 Robin D. Ryan, *The Criminalization of Trade Secret Theft Under The Economic Espionage Act of 1996: An Evaluation of United States v. Hsu*, 40 F. Supp.2d 623 (E.D. Pa. 1999), 25 DAYTON L. REV. 243, 259 (2000).

刑法謙抑性。

此外，我國營業秘密法第 13 條之 2 固規定：「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。」雖名為域外侵害營業秘密之處罰，但除「意圖在外國、大陸地區、香港或澳門使用」之主觀要件，其餘構成要件與第 13 條之 1 並無不同，已有論者指出本條並非域外侵害營業秘密罪之立法模式，因該條客觀構成要件並非針對域外使用之行為⁹³，由罪刑法定主義來解釋，本條實際上僅能處罰意圖於外國、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。另本條並非最輕本刑三年以上之重罪，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⁹⁴，故本規定似亦未能針對國際經濟間諜犯罪。從而我國宜另設域外侵害營業秘密之規定，以填補漏洞⁹⁵，目前已有論者提出我國版經濟間諜法之草案，應可作為日後修法參考⁹⁶。

除以上原因外，我國民刑事訴訟時間冗長也是營業秘密所有人難以透過營業秘密法或競業禁止約款取得適當保護的原因之一。據司法院統計，民事案件於 106 年度之平均結案日數，以智慧財產法院 228.4 日最長，其次依序為高院 185.1 日、最高法院 39.9 日、地院 33.1 日。刑事案件在不計入檢察官偵查時間下，106 年度平均結案日數以智慧財產法院 131.4 日最長，其次依序為高院 80.9 日、地院 77.5 日、最高法院 29.2 日⁹⁷。由此觀之，營業秘密所有人如欲透過司法訴訟途徑取得終局確定

93 請參王銘勇，「域外侵害營業秘密罪法制研析」，2014 年第 18 屆全國科技法律研討會論文集，國立交通大學，新竹，2014 年 12 月 08 日。

94 請參中華民國刑法第 7 條規定。

95 請參王銘勇，同註 85，頁 105。

96 請參曾勝珍，我國有關經濟間諜立法必要性之探討—以參考美國經驗為主，人文及社會科學集刊，第 19 卷，第 2 期，頁 305 以下，2007 年 06 月。

97 請參司法統計，106 年司法業務概況，<https://www.judicial.gov.tw/juds/106all.pdf>，

判決，平均時間至少需要一年以上，三五年者亦在所多有，就技術外洩所帶來之立即實害而言實緩不濟急。從而，未來立法者在研議修法時，亦應將如何使營業秘密所有人得適時取得保障納為重要思考方向。

目前我國經濟部智慧財產局刻正研議營業秘密法之修正，惟目前之修正要點在於將域外犯罪自非告訴乃論修改為告訴乃論，增訂未經認許之外國法人得作為訴訟主體，增訂偵查程序營業秘密資料之閱覽限制，及外國人營業秘密保護之互惠原則等技術性事項，尚無促進營業秘密所有人保障效果之內容⁹⁸。故若有其他法律規範可補營業秘密法之不足，亦為可研議之方向。

二、出口管制及投資審查法制相關問題與因應措施

在出口管制方面，目前我國針對貨品與技術的直接輸出雖有相關法規，但散見於不同法律之中，無統一制度與標準。又我國貿易法僅管制物品之出入口，如僅為技術輸出，除非該技術為「戰略性高科技貨品輸出入管理辦法」規定應申請許可並接受定期管控者外，否則似無從依貿易法規定加以管制。另國家安全法、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亦有規範，然若敏感科技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，然如前所述，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敏感科技。

最後瀏覽日期：2018年06月27日。

98 請參經濟部智慧財產局，營業秘密法部分條文修正草案總說明，<https://www.tipo.gov.tw/ct.asp?xItem=621644&ctNode=7452&mp=1>，最後瀏覽日期：2018年06月27日。

另就外資來臺投資部分，我國均由經濟部投資審議委員會（下稱投審會）進行審核，目前除中國大陸投資我國需受兩岸人民關係條例、大陸地區人民來臺投資許可辦法等規定限制⁹⁹，且在投資審議時需先參考具敏感性或國安（含資安）疑慮之業務範疇外，其他外資投資我國時僅需受外國人投資條例限制，而依該條例，外資除對國家安全、公共秩序、善良風俗或國民健康有不利影響之事業、法律禁止投資之事業¹⁰⁰，以及經濟部公告禁止及限制僑外人投資業別項目外¹⁰¹，其餘事業應均屬准許投資之範疇。換言之，我國既有投資審議法制除對中國大陸外，似乎未能充分預防外資投資我國廠商而致技術外流之情形。

由我國上述出口管制以及投資審查的相關法規觀之，可知我國缺乏對敏感科技管制的相關體系規範，直言之，我國在技術輸出管制上存在法規漏洞，非無檢討改進之必要。而目前已有建議提出未來在設計審查體制上，宜仿效「歐美國家主要以國家安全或經濟安全為審查原則」作為審查啟動因素¹⁰²，對外資投資我國企業所涉技術保護機制作為全面性規範。

參照上開美國、英國、日本就技術輸出之管制，其體系設計均是採由專責主管機關負責，同時明定管制技術類別並配合主管機關間之定期檢討修正，令人民清楚知悉輸出前應先申請審核之技術為何，而不致妨礙廠商技術輸出與併購計畫之擬定。從而我國在研議修正相關法律制度時，應著重在敏感科技管制法制的統整與明確化，使得政府補助或我國

99 同前註 13、14。

100 請參外國人投資條例第 7 條。

101 請參經濟部投資審議委員會，僑外投資負面表列－禁止及限制僑外人投資業別項目，https://www.moeaic.gov.tw/businessPub.view?lang=ch&op_id_one=1，最後瀏覽日期：2018 年 06 月 27 日

102 請參經濟部投資審議委員會，105 年 07 月 29 日僑外投資條例修法與投資審查制度改革座談會會議記錄，https://www.moeaic.gov.tw/businessPub.view?lang=ch&op_id_one=1，最後瀏覽日期：2018 年 06 月 27 日。

廠商自行研發之敏感科技受有完整保障。

然而，美國政府在研議「外國投資風險審查現代化法案」時，亦有批評密度過高之審查機制將破壞既有審查制度，同時將損害產業追蹤關鍵技術的能力。故我國在設計相關法制度時，亦應留意此問題之發生。換言之，在敏感科技保護法制化之同時，除著重專責機構之設計，敏感科技定義，與建立公開透明審查機制外，亦要避免扼殺我國從商業活動中追蹤關鍵技術之能力，方能促進我國技術管制機制之完善。

三、我國敏感科技保護法草案

承上所述，我國既有營業秘密法制、出口管制以及投資審查之規範在敏感科技之管制保護有所不足，我國政府鑑於創造更有利於國內科技之經營與發展環境等重要科技政策，擬對於國家安全及公共利益有重大影響之敏感科學技術，採取積極管理措施，避免國安核心技術流失，致影響我國科技實力，爰針對敏感科學技術保護機制之建立與執行制定「敏感科技保護法」加以規範，相關草案已由立委提請立法院議決¹⁰³。

該草案首先定義敏感科技為保護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，同時必須符合：非一般涉及該類資訊之人所知、因其秘密性而具有實際或潛在之經濟價值、權利人已採取合理之保密措施等條件¹⁰⁴。

敏感科技之項目與輸出國家及地區，將由科技部應定期會同其他各目的事業主管機關訂定後報請行政院公告，認定上應以確保國家安全及公共利益，且確具必要性為原則，認定過程中應遴聘(派)有關機關(構)

103 請參立法院，立法委員蘇治芬等 24 人提出之敏感科學技術保護法草案，https://lci.ly.gov.tw/LyLCEW/agenda1/02/pdf/09/03/15/LCEWA01_090315_00036.pdf，最後瀏覽日期：2018 年 06 月 27 日。

104 請參敏感科技保護法草案第 2 條。

人員、專家、學者及產業界人士參與¹⁰⁵。經核定敏感科技之公開許可與輸出由主管機關科技部審查¹⁰⁶。

就未經許可而輸出或公開敏感科學技術者，違反者並處 7 年以下有期徒刑、拘役或科或併科新臺幣 3 千萬元以下罰金¹⁰⁷；若其行為出於意圖或明知其行為有利於其他國家或地區之政府、機構或其派遣之人所為者，將加重其刑¹⁰⁸。特別之處在於，若敏感科技所有人發現有受不法侵害之情事，致敏感科技有輸出或公開之虞者，有主動通報相關目的事業主管機關之義務，且相關目的事業主管機關得進行協調並協助防止侵害擴大¹⁰⁹。

最後，為避免本法之規定破壞既有出口管制法規與國家安全法規之體系，爰明定敏感科學技術相關資料除應適用國家機密保護法之規定採取保密措施者外，有未核定為國家機密而有保密之必要者，應予保密，相關辦法由相關目的事業主管機關會商定之¹¹⁰；科技貨品輸出入，仍依現行貿易相關法律及法規命令規定辦理¹¹¹。

由以上草案內容，可知我國就敏感技術保護已經有完整與明確化之規劃，且在敏感科技所有人發現有不法侵害情事時，令主管機關有主動介入防免損害擴大之法源依據，並已注意到既有出口管制法規與國家安全法規相容性之問題，應有助於在現行營業秘密法制，出口管制規範與科研相關法規就非政府補助研發敏感科技保護不足之情形下，對敏感科技為有效管理，此項草案立法應予支持。然而，此項草案對於敏感科技之定義與我國法就營業秘密之定義如出一轍，雖有加上應經主管機關指

105 請參敏感科技保護法草案第 4 條。

106 請參敏感科技保護法草案第 5 條。

107 請參敏感科技保護法草案第 11 條。

108 請參敏感科技保護法草案第 12 條。

109 請參敏感科技保護法草案第 14 條及第 15 條。

110 請參敏感科技保護法草案第 16 條。

111 請參敏感科技保護法草案第 17 條。

定之要件，但在理論上有可能發生得受營業秘密法保障者即受敏感科技法草案拘束的情形，不無引發政府過度管制人民財產權之疑慮。

因此，建議立法者應仿韓國經驗，在法條內要求主管機關指定敏感科技時，除衡量國家安全、國民利益外，亦應一併衡量產業技術國內外市場比率，相關技術領域趨勢，且在最小必要限度內指定之原則。而在審查體制之發動，宜仿效以上美國等國家作法，以國家安全或經濟安全作為審查啟動的首要因素。至於作業流程上，未來就許可申請亦可仿英國作法，設計專屬網站開放網路申請，同時設置專責機關協助產業導入申請流程及法規遵循，協助產業進行人員訓練。

雖目前草案內未納入美國、日本、韓國針對投資審查之部分，似不能對藉投資取得敏感科技之問題加以預防，惟因商業活動對關鍵技術發展之追蹤至為重要，對我國而言更是如此，故是否應在就投資審查部分為規範，宜在草案通過後視具體施行情況加以調整。

伍、結論

保護敏感科技向來為我國政府之重點政策，但目前尚無正式法律規範與制度，而既有營業秘密法、出口管制相關法規，國家安全與科研相關法規有所不足。例如我國砷化鎵晶圓代工產業知名企業穩懋半導體股份有限公司遭遇中國大陸人士以不正當手法竊取技術文件資料等事件，穩懋公司縱可以依法對該技術文件資料主張營業秘密法所有之各項權利，並向法院聲請對被挖角之員工聲請定暫時狀態處分，避免其任職於競爭對手。

然而，提起營業秘密民刑事訴訟審理時間過長，營業秘密所有人舉證責任又重，且定暫時狀態處分在實務上可以反供擔保免於執行，無法及時防堵營業秘密外洩；另穩懋公司所有技術資料雖為國際民生有關之敏感科技，若非與國家安全或國防有關，又非屬受政府資助之研發成果，我國各行政主管機關縱有協助防堵之心，於法亦無從介入，且該技

術與被挖角之人員並非實體貨物，不能以出口管制法規相繩，是我國對敏感科技管制存有法規漏洞，實有檢討改進之必要。

然而，參照世界各主要國家如美國、日本、韓國之相關制度，敏感科技輸出或公開之審核通常由專責機關負責，且定期就敏感科技項目與輸出地區等為檢討，以確保科技交易秩序之維護，達成有效管理之目的，故若我國不採統一立法，而僅就既有法制逐一修正，仍無法改善現行規定過於分散，定義不清，各主管機關權責混淆之問題，對於敏感技術之管理恐缺乏效率。

準此，我國刻正研議之「敏感技術保護法」草案實有助於在相關法制對敏感科技保護不足之情形下，建立敏感科技管理機制。該法施行後，如再出現其他類似之受害者，相關目的事業主管機關於收受受害者通報後，得別於司法訴訟外先行介入，與各機關進行協調並協助防止侵害擴大，避免敏感科技或相關人士外流，應有助於對敏感科技為有效管理，提升科技競爭優勢，並確保國家安全與利益。二方面也可以保障受害者不因冗長訴訟而難以伸張權利。惟目前敏感科技之定義與營業秘密法之定義並無不同，為免發生受營業秘密法保障即受敏感科技法拘束之情形，進而引發政府過度管制人民財產權之疑慮，建議草案中宜增加主管機關指定敏感科技時，除衡量國家安全、國民利益外，亦應一併衡量產業技術國內外市場比率，相關技術領域趨勢，且在最小必要限度內指定之原則。而在具體實施上，建議仿以上美國等國之經驗，以國家、經濟安全為啟動審查之首要因素，未來亦可仿英國作法開放網路申請，並設置專責機構協助產業訓練人員，一方面可以普及敏感科技管制制度，二來可以協助產業遵循法規。

至於我國營業秘密法制部分，則應針對舉證責任，營業秘密刑事規範要件不明確，既有刑事規範未能有效規範域外犯罪等致營業秘密所有人難以主張權利之問題進行修正。建議可適當調整舉證責任之程度，另營業秘密所有人在訴訟上只需先證明秘密性與價值性之表面事實，由被

告舉證系爭營業秘密並非「一般涉及該類資訊之人所知」；將營業秘密法第 13 條之 1 第 1 項第 1 款行為態樣進行修正，使營業秘密行為規範禁止之行為更為明確，避免侵害者因構成要件不明確而獲益於刑法謙抑性；現行法並無針對域外犯罪加以規範，日後修法時宜增設真正規範域外侵害營業秘密之規定。

參考文獻

中文

一、專書

王偉霖，營業秘密法理論與實務，元照，2017年2版。

王銘勇，域外侵害營業秘密罪法制研析，2014年第18屆全國科技法律研討會論文集，國立交通大學，2014年。

黃程貫，最低服務年限與競業禁止條款，勞動基準法釋意－施行二十年之回顧與展望，新學林，2005年。

謝銘洋、古清華、丁中原、張凱娜，營業秘密法解讀，月旦，1996年。

二、期刊論文

王 奎，美中商業秘密內涵的思考，政法論壇（中國政法大學學報），第25卷，第3期，2017年05月。

王偉霖，我國營業秘密法刑事規範的再思考，法令月刊，第68卷，第5期，2017年05月。

王偉霖，論我國引進營業秘密法不可避免揭露理論（Inevitable Disclosure Theory）之可行性與適用限制，萬國法律，第203期，2015年10月。

王偉霖、楊孝文，加盟連鎖契約競業禁止條款之研究，華岡法粹，第62期，2017年06月。

邱駿彥，競業禁止特約有效性認定基準之法理探討，華岡法粹，第48期，2010年11月。

高蘇弘，勞工離職後競業禁止約款有效性之研究，國立中正大學法律研

究所碩士論文，2007年07月。

張聖怡、李素華、李雅萍，研究機構研發人員競業禁止問題研析，科技法律透析，第13期，2001年03月。

曾勝珍，我國有關經濟間諜立法必要性之探討—以參考美國經驗為主，人文及社會科學集刊，第19卷，第2期，2007年06月。

詹世榕，國際間關於研發國際化所涉事項之規範研析，科技法律透析，第23卷，第7期，2011年07月。

鄭嘉文、許祐寧，跨境投資技術保護與營業秘密之法制研析，科技法律透析，第29卷，第12期，2017年12月。

三、其他資料

益思科技法律事務所，營業秘密法制之研究，2003年12月31日，
<https://www.google.com.tw/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=0ahUKEwiKksbLv5jQAhWCWrwKHQMaDgAQFgghMAE&url=https%3A%2F%2Fwww.tipo.gov.tw%2Fddl.asp%3FfileName%3Df0f9aebef969-462b-8184-aaec45f0af56.pdf&usg=AFQjCNERBqrYinYVFL09KD3chuucz3y4dA&sig2=sEDM8fdNd0TDicjV9zCRpA>，最後瀏覽日期：2018年06月27日。

華冠國際顧問有限公司，美、日、歐盟對無形技術管制之法令規定、作法及我國推動無形技術管控之可行性研究，2011年03月，
<https://www.trade.gov.tw/Pages/Detail.aspx?nodeID=830&pid=320227>，最後瀏覽日期：2018年06月27日。

劉博文，美國經濟間諜法簡介，2013年02月17日，
<https://www.tipo.gov.tw/ct.asp?xItem=207083&ctNode=6740&mp=1>，最後瀏覽日期：2018年06月27日。

英文

Agee, Michael L., *Covenants Not To Compete in Tennessee Employment Contracts: Almost Everything You Wanted to Know but Were Afraid to Ask*, 55 TENN. L. REV. (1988).

Edelman, William J., *The “Benefit” of Spying: Defining the Boundaries of Economic Espionage Under the Economic Espionage Act of 1996*, 63 STAN. L. REV. (2011).

O’Malley, Christine M., *Covenants Not To Compete in the Massachusetts Hi-Tech Industry: Assessing the Need for A Legislative Solution*, 79 B. U. L. REV. (1999).

Ryan, Robin D., *The Criminalization of Trade Secret Theft Under The Economic Espionage Act of 1996: An Evaluation of United States v. Hsu*, 40 F. Supp.2d 623 (E.D. Pa. 1999), 25 DAYTON L. REV. (2000).

Wood, Jason S., *A Comparison of the Enforceability of Covenants Not to Compete and Recent Economic Histories of Four High Technology Regions*, 5 VA. J. L. & TECH. (2000).

Abstract

Though small in geographic area, with its advancement on the production process and research and development, for decades, Taiwan has played an indispensable role in the global supplying chains in the high-technology industry. While such technology mostly serve for commercial purposes, some of which, known as “Sensitive Technology,” simultaneously possess significant value on the aspects of national economy and military security. With high-technology industry from China on the rise, it is evident that Taiwan’s role in the industry is challenged by what’s called “Red Supply Chain.” It is not uncommon that events such as events like Chinese companies misappropriating Taiwan’s technology or Sensitive Technology of the Taiwanese companies occur in recent years. Under the circumstances, protecting the technology and Sensitive Technology developed by Taiwanese companies become a timely and imminent issue. However, no legal system governing the intangible technology is currently in place in Taiwan, wherefore, establishment of a proper legal system is imperative.

This article will review the existing acts and regulations that are intended to prevent foreign companies, mainly Chinese companies, from misappropriating technology or poaching talents from Taiwan and make comparison to those from the United States and other countries. This article will show that Sensitive Technology Protection Act, which is being drafted as of now, does help structuring a system which provides control over Sensitive Technology. Nevertheless, the proposed definition of Sensitive Technology substantially overlaps with that of trade secrets. Consequentially, to refrain that all trade secrets would be subject to Sensitive Technology

Protection Act, leading to excessive control over rights to property , this article suggests another provision - that is, on top of national safety and public interests, when labeling Sensitive Technology, the authorities must take into account a technology's market shares in both foreign and domestic markets, consider the trends in relevant industry, and exercise highest scrutiny when designating a technology as Sensitive Technology.

Keywords: Trade Secret, Sensitive Technology, Commercial Espionage, Non-Compete, Export Control