

美國鋼鐵公司撤回對中國寶鋼公司之營業秘密控訴

陳伶嘉 編譯

摘要

美國鋼鐵公司 (United States Steel Corporation, USS) 於今 (2017) 年 2 月 15 日撤回其依據美國關稅法第 1337 條 (下稱 337 條款) 對中國寶鋼公司所提出之竊取營業秘密控訴。USS 的官方聲明及同業認為, 美國 337 條款儼然未考量日新月異下網路竊盜行為之嚴重性, 尤其是對於涉及國家支持的網路間諜行為。本案的 USS 即因舉證困難, 難以於時限內提出必要證據, 導致其最終選擇撤回控訴。業者建議, 美國政府應重視此議題並改革現行法律, 並與業者合作對抗網路竊盜行為, 以維護市場之安全。

(取材自: *U.S. Steel withdraws trade secrets claim in 337 case against Chinese company*, INSIDE US TRADE, Vol. 35, No. 7, Feb. 15, 2017.)

美國鋼鐵公司 (United States Steel Corporation, USS) 於今 (2017) 年 2 月 15 日向美國國際貿易委員會 (International Trade Commission, ITC) 提交動議, 撤回其依據美國關稅法第 1337 條 (下稱 337 條款), 對中國寶鋼公司所提出竊取營業秘密之控訴, 並表示將繼續致力於另外兩件對寶鋼和其他中國公司的 337 調查, 即偽造產品來源地及共謀定價之指控。

USS 於提交動議之同天於官網上發表聲明¹, 指出受害公司在美國現行法制下, 對於國家支持的網路間諜行為需負擔的龐大舉證責任問題。於網路科技盛行的時代, 網路安全與營業秘密於產業競爭上更具關鍵重要性, 故本次事件相當值得關切與理解。本文將介紹此次 USS 撤回對中國寶鋼公司營業秘密控訴之始末, 首先介紹本事件背景, 即 USS 對於中國寶鋼公司於盜取營業秘密之指控; 並續以 USS 之聲明闡述其於本案訴訟過程中所面臨之困難, 最後提及中美一直存在的網路間諜問題; 最後以相關業者對於本事件之評論作結。

壹、事件背景

依據美國 337 條款, 若進口美國之產品存有盜用營業秘密之情事, 並造成美

¹ United States Steel Corporation, *United States Steel Corporation Announces Action On Section 337 Case*, Feb. 15, 2017, <https://www.ussteel.com/uss/portal/home/newsroom/pressreleases?renderFrame=https://uss.mediaroom.com/index.php?s=32722&item=137111> (last visited Feb. 20, 2017).

國產業之損害，ITC 即可禁止該違法產品進口²；然而，337 條款中並未具體規定何謂盜用營業秘密，故 ITC 通常引用單一聯邦標準，如美國統一營業秘密法典 (Uniform Trade Secret Act, UTSA)，以判定違法行為³。根據 UTSA 第 1 條之定義，「營業秘密」係指包括配方、模式、資訊之編輯、程序、設備、方法、技術或過程之具有獨立經濟價值及秘密性之資訊⁴；「盜用」營業秘密則指在應知或明知的情況下擁有他人以不正當手段獲取之營業秘密，或未經盜取營業秘密之人或有義務保護該營業秘密者明示或默示同意，即揭露或使用該營業秘密⁵；而前述不正當手段又包括盜竊、賄賂、詐欺、違約、引誘使違反保密義務或以電子或其他方式實行之間諜行為⁶。

2016 年 4 月 26 日，USS 向 ITC 指控中國國有鋼鐵公司—寶鋼，盜用 USS 之營業秘密。根據 USS 提交之訴狀指出，2011 年 1 月中國政府曾駭入 USS 之電腦及設備，竊取其製造高強度鋼材之方法。其後，從未生產高強度鋼材的寶鋼公司便開始製造、出口最高等級的高強度鋼材，並影響美國鋼鐵市場，故 USS 認定其生產的鋼材是根據由 USS 盜取之營業秘密所製造⁷。除營業秘密指控外，USS 於去年 4 月 26 日提起的 337 條款指控中，亦包括共謀定價及偽造產品來源地之指控，然該兩件指控均被行政法院法官 Dee Lord 駁回⁸，而唯一未被駁回的營業秘密控訴，卻於今年 2 月 15 日由 USS 自己撤銷。原因是依據現行法律，USS 實際上並無法對抗涉及國家支持的網路間諜行為。

貳、USS 撤回營業秘密控訴之原因

美國 337 調查程序是於 ITC 立案後，由各方開始蒐集證據，並得以要求對方給予案件相關之資訊，從而獲取必要證據並於時程內提交⁹。本件營業秘密控訴之調查引起政府、鋼鐵業和法律界之關注，因蒐證過程中極有可能一窺中國政府之作為。根據消息指出，本案之證據蒐集可能能夠取得之貿易相關資訊，包括

² Warren S. Heit & James P. Gagen, *Litigating Trade Secret Misappropriation At The ITC*, LAW 360, May 24, 2016, <https://www.law360.com/articles/795109/litigating-trade-secret-misappropriation-at-the-itc> (last visited XX); 19 U.S.C. § 1337 (a) & (d).

³ Warren S. Heit & James P. Gagen, *supra* note 2.

⁴ 18 U.S. Code § 1839 (3).

⁵ 18 U.S. Code § 1839 (5).

⁶ 18 U.S. Code § 1839 (6).

⁷ United States Steel Corp. v. Hebei Iron and Steel Group Co. et al., Complaint under Section 337 of the Tariff Act of 1930, as Amended, at 2-3, *available at* <http://www.itcblog.com/images/ussteelcomplaint.pdf> (last visited Feb. 20, 2017).

⁸ 另兩件指控之相關爭議可參考：李旺達，「中國請求美國 ITC 駁回 USS 公司於 337 調查中反托拉斯及偽造產地之指控」，政治大學國際經貿組織暨法律研究中心經貿法訊，201 期，頁 16-21，網址：<http://www.tradelaw.nccu.edu.tw/epaper/no201/3.pdf> (最後瀏覽日：2017 年 2 月 20 日)。

⁹ 經濟部國貿局，「美國 337 條款調查流程簡介」，2015 年 9 月 30 日，頁 18-19，網址：<https://goo.gl/2PRIKA> (最後瀏覽日：2017 年 2 月 20 日)；李建歡，「美國關稅法 1337 條款所引發貿易規範適用的問題」，政治大學國際經貿組織暨法律研究中心經貿法訊，198 期，頁 18-31，網址：<http://www.tradelaw.nccu.edu.tw/epaper/no198/2.pdf> (最後瀏覽日：2017 年 2 月 28 日)。

生產成本、關係人身份、分銷商和終端消費者等具體事實。然而，中國政府並非本案之被告，故其拒絕 USS 要求之資訊並不會受到任何制裁；再者，由於 337 條款相對一般訴訟更講求效率，時程安排甚為緊湊¹⁰，而 USS 自寶鋼公司取得的資訊又大多為中文文件，更加劇蒐證程序之困難。因此，USS 決定自行撤回控訴。

USS 於其官方聲明中指出，在這個產業高度互聯、以數據為中心的時代，企業更加容易受到網路竊盜所害，被竊取的資料可能會是營業秘密、商業策略或消費者個人資訊等等，而若網路攻擊是由政府支持所完成的，受害公司在 337 條款的調查程序下負擔過於沉重的舉證責任，這將對國家的經濟健全造成威脅¹¹。其更認為，337 條款雖使美國公司得針對不公平競爭行為尋求相關救濟，但這項 50 年來未考慮過任何技術進步的舊法，並無法阻止其他國家竊盜企業營業秘密，間接導致針對美國公司的網路盜竊及犯罪行為日益猖獗。

參、美國業者面對的中國網路間諜問題

自 21 世紀初以來，網路間諜問題便愈發加深美國與中國之間的緊張關係¹²。儘管所有國家均可能涉及間諜行為，但中國可說是犯行最大且最持久者¹³。2011 年，ITC 報告指出美國企業因中國盜用營業秘密之行為，於 2009 年損失約 11 億美元；2009 年到 2013 年間，20 件依經濟間諜法（The Economic Espionage Act）起訴的刑事案件中，中國即涉及 17 件¹⁴。2014 年，美國司法部更直接對 5 名中國官員提起網路盜竊營業秘密之控訴，竊取對象包括 USS、美國鋁業公司（Alcoa）、太陽能世界工業公司（SolarWorld）等 6 家美國公司¹⁵。對此，中國外交部表示該指控十分荒謬且反映出美國對中國的雙重標準，並未配合美國調查¹⁶。

¹⁰ See American Bar Association, *Introduction to Section 337 Investigations*, at 3-4, available at http://apps.americanbar.org/abastore/products/books/abstracts/5370203%20intro_abs.pdf (last visited Feb. 20, 2017).

¹¹ United States Steel Corporation, *supra* note 1.

¹² Gary Brown & Christopher D. Yung, *Evaluating the US-China Cybersecurity Agreement, Part 1: The US Approach to Cyberspace*, THE DIPLOMAT, Jan. 19, 2017, <http://thediplomat.com/2017/01/evaluating-the-us-china-cybersecurity-agreement-part-1-the-us-approach-to-cyberspace/> (last visited Feb. 20, 2017).

¹³ *Id.*

¹⁴ Brian T. Yeh, *Protection of Trade Secrets: Overview of Current Law and Legislation*, CONGRESSIONAL RESEARCH SERVICE, R43714, Apr. 22, 2016, at 15, available at <https://fas.org/sgp/crs/secretary/R43714.pdf> (last visited Feb. 20, 2017).

¹⁵ *U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage*, US DEPARTMENT OF JUSTICE, May 19, 2014, <https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor> (last visited Feb. 20, 2017).

¹⁶ Jonathan Kaiman, *China reacts furiously to US cyber-espionage charges*, THE GUARDIAN, May 20, 2014, <https://www.theguardian.com/world/2014/may/20/china-reacts-furiously-us-cyber-espionage-charges> (last visited Feb. 20, 2017).

僵持不下的中美網路間諜問題，直到 2015 年中國與美國簽訂中美網路協議 (U.S.-China Cyber Agreement) 始露出曙光¹⁷。兩國於協議中同意不會進行或支持網路竊盜智慧財產權之行為¹⁸。然而，美國普遍質疑該協議之實施成效¹⁹，因其後仍有網路安全公司監測到中國官方駭客攻擊²⁰，且中國亦尚未因該協議而做出任何管制行為²¹，甚至有評論擔心中國可能已經發展出更進步的駭客技術，可以避免被偵測。總結來說，中國網路間諜仍持續威脅美國產業利益。

儘管過去美國公司曾於中國營業秘密訴訟中取得勝訴，但該些案件均不涉及中國政府行為。因此，面對高度政府控制的中國市場，美國業者呼籲政府應立即改革現行法律制度以應對國家支持的網路間諜行為，並提供政府資源以協助業者對抗之。業者近一步表示若未能制定產業網路間諜之協調政策，可能會影響相關美國業者使用商業資訊。鋼鐵工人工會 (United Steelworkers) 副主席康維 (Tom Conway) 亦對本案結果表示失望，其認為忽略網路間諜行為嚴重性的法律已然過時，並呼籲政府應提供一套政治解決方案，以解決網路間諜問題。

有鑑於去年 5 月歐巴馬簽署了保護營業秘密法 (Defend Trade Secrets Act)，相對以往 337 調查遵循的聯邦普通法，設立了更多營業秘密行為之統一標準，業者預期將會有更多營業秘密案件於 ITC 進行。USS 於其聲明中表示，儘管美國近來在網路威脅領域已有所進步，聯邦政府和私營部門之間仍需要更多的合作和協調，以有效解決惡意網路犯罪問題，政府亦應提供受害公司尋求救濟之合理法律途徑。若相關法律有積極進展，USS 將進一步評估後續動作。

¹⁷ John W. Rollins et al, *U.S.-China Cyber Agreement*, CONGRESSIONAL RESEARCH SERVICE, IN10376, Oct.16, 2015, available at <https://fas.org/sgp/crs/row/IN10376.pdf> (last visited Feb. 20, 2017).

¹⁸ *Id.*

¹⁹ Scott Warren Harold, *The U.S.-China Cyber Agreement: A Good First Step*, THE RAND CORPORATION, Aug.1, 2016, <http://www.rand.org/blog/2016/08/the-us-china-cyber-agreement-a-good-first-step.html> (last visited Feb. 20, 2017).

²⁰ Joseph Menn, *China Tried To Hack American Companies Since Agreeing To Cyber Pact*, Security Firm Says, THE HUFFINGTON POST, Oct. 19, 2015, http://www.huffingtonpost.com/entry/us-china-cybersecurity_us_56249ed8e4b02f6a900cd0de (last visited Feb. 20, 2017).

²¹ Aisha Chowdhry, *U.S.-China still at odds on cybersecurity issues*, FCW, Mar 31, 2016, <https://fcw.com/articles/2016/03/31/obama-xi-cyber.aspx> (last visited Feb. 20, 2017).