數學的曼哈頓計畫

不沾俗塵的散仙，還是鴕鳥

自從 2013 年起，經由史諾登（E. Snowden）所流出的大量機密文件揭露出美國國安局（NSA）的各種情蒐和監視行為，造成各界莫大的震撼。隨後陸續揭發的資料更表明國安局情蒐範圍的廣泛和全面，已達到前所未有的程度。似乎我們的一切都被監控、被窺伺，再也沒有隱私可言。其中值得注意的是，數學在此所扮演的角色。

舉凡資訊的加密與傳遞、情報的蒐集與分析，都與數學密切相關。國安局的各項技術是建立在數學知識上的，它的運作也需要大量數學家支援，所以長久以來都有「國安局是數學家第一大雇主」的說法。也因此，有些數學家自然會問：他們手上的工作是否在不知不覺中被用於摧毀他們所信仰的人性價值？他們是否該採取更積極的行動來阻止數學的誤用與濫用？

率先發難者之一是芝加哥大學的貝林森（A. Beilinson），他投書給美國數學學會（AMS）的 *Notices*，呼籲學會切斷與國安局的一切關係，他的來信在 2013 年 12 月號的 *Notices* 刊出。之後，艾克隆大學的佛西（S. Forcey）與匹茲堡大學的黑爾斯（T. Hales，克卜勒猜想的證明者）也主動投稿表達意見。其中黑爾斯的文章是針對被批評設有「後門」的橢圓曲線加密演算法（參見本刊第二期，〈橢圓曲線：增強或減弱資訊安全的雙面刃〉）探討破解密碼的可行性。黑爾斯的實作證明，利用後門可以輕易破解密碼，將加密的資訊還原。而且即使不知道具體的後門為何，只要具備適當的數學知識，便可以自行找出後門所在。

以此為契機，AMS 便規劃了以 *Notices* 作為論壇，邀請各方數學家發表意見。AMS 這麼做有其必要性，誠如貝林森的文章所云，AMS 和國安局之間存在著共生關係——國安局是數學研究的重要金主，他們透過 AMS 招募數學家，AMS 也經管國安局的某些贊助計畫。AMS 沒有理由置身事外。

一年多以來，*Notices* 上已刊出十餘篇相關文章和來信，大部分是對國安局及其監控行為的批評意見，願意為國安局辯護的人並不多（可能是因為相關人士都簽有保密協定）。在這些支持意見裡，最值得注意的是今年二月號所刊出的〈加密法與國安局在制定國際標準時的角色〉，作者魏特海默（M. Wertheimer）在撰文時是掌理國安局研究部門的主管。對於引發爭議的 Dual_EC_DRBG 加密標準的制定原委，他承認國安局在獲悉演算法的瑕疵後處理不當，但其中絕無陰謀；至於情蒐行為，則一切都是合法的，也並未侵犯美國民眾的權益。他的說法雖有避重就輕之嫌，而且只是以個人名義發言，但因為難得見到國安局一方的說法，所以仍引起多國媒體的關注與報導。

儘管 AMS 努力促成討論風氣，但是即將卸任的學會會長佛根（D. Vogan）坦言，絕大多數數學家的態度還是漠不關心，他們認為研究的價值在於研究本身，這與它們是否被濫用無關。即使他身為會長，也難以推行像是發表公開聲明之類的進一步行動。

在史諾登事件之前，我們都難以想像抽象、純粹的數學可以成為欺騙、為惡的工具。難道以後拿起筆來做數學，竟也要像醫學或生化實驗一樣，考慮道德問題？面對這個處境，人們不免聯想到參與曼哈頓計畫的物理學家，例如柏克萊的數學家弗倫科（E. Frenkel）便說道：「在這個新時代，數學已變成一項強力的武器。當核子彈建造時，……理論物理學家被迫要面對深刻的倫理問題。如今發生在數學上的，或許也有類似的深遠影響。」

把數學與核子武器相提並論，究竟是實情抑或只是誇張的修辭，還有待時間來驗證。然而可以確知的是，數學再也不是（也許從來都不曾是）像哈第（G. Hardy）所以為的那樣一門與世隔絕的學問。（編輯室）

本文參考資料請見〈數理人文資料網頁〉http://yaucenter.nctu.edu.tw/periodical.php