恐怖分子就在你身邊？——談生物檢測

胡湘玲

「遭受恐怖攻擊」──這個一向被保險業者評估為發生機率微乎其微的風險，在911之後已經成為「日常」的危險。每次發生飛機墜毀、火車相撞、高樓傾倒的意外，「是不是又一次的恐怖攻擊事件？」已成為例行的問題。當意外變成可能，高科技範疇中長久以來受到忽視的安全問題，瞬間被凸顯與認識。突然之間我們才發現，原來這個處處繁華的昇平景象這麼脆弱。

紐約世界貿易大樓倒塌是一個轉捩點。之前，風險評估大約可以憑經驗與專業判斷。例如，芝加哥發生大地震的機率小於洛杉磯，佛羅里達州遭颶風侵襲的機率大於美國內陸。之後，風險將以完全不同的概念計算，也以脫離常軌的方式認知。什麼樣的經驗與專業可能評估：哪裡會是恐怖分子下一個攻擊目標？遭恐怖攻擊的風險有多大？可能造成多嚴重的損失？這是一個完全缺乏資訊的領域。

全世界與風險相關的研究團體目前正專注於一個問題：我們該如何保護自己？

航空公司加強安檢措施、機場增添更先進的掃描儀器、化學工廠把圍牆加高、核能電廠要求遠離飛航航道。不過，這些都不及德國內政部長席利（Otto Schily）的「好主意」──把恐怖分子揪出來。〔註〕

2001年11月7日，席利向聯邦內閣提出「反恐怖攻擊」的應對方案。在這個備受爭議的安全措施中，計劃在未來所有的身分證件，不管是德國人或外來移民，都要植入電子晶片以儲存指紋、面容與手形掃描資料，也就是透過生物檢測來辨識與確定持件人身分。一旦確定持件人與恐怖組織的關連，外國人將被遣送出境，本國人將受法律審判。在這個方案中，人身安全被列為第一優先。

因為，沒有安全，自由也就不存在了

然而，一個自由民主的社會，究竟應該為免於恐怖攻擊的恐懼付出多大代價？這牽涉到風險的認知與評估，也就是在「恐怖攻擊」與

【註】在這裡稍做背景說明，以免讀者誤會這項安全方案意味著德國軍國主義、極右派國家監視系統的抬頭。德國聯邦內政部長席利在1980-1989年為綠黨成員，1989年退出綠黨加入社民黨，一向擁有另類政客及社會主義者的社會形象。他1971年曾擔任左派恐怖組織「紅軍陣線」（Rote-Amee-Fraktion, RAF）成員馬勒（Horst Mahler）的辯護律師。而現任德國總理施洛德也於1978年為這位「恐怖分子」辯護。因此，誰是「恐怖分子」，恐怕沒有確定的定義，而跟社會政治情境絕對相關。不過，德國知識界一向強調「寧願極左，也不要極右」。所以，席利這項違背憲法人權精神（個人資料不公開）的安全方案，不僅引起討論風暴，也為他這個公民權利維護者及個人資料隱私權保護者「贏得」2001年「超級老大哥」的難堪稱號。參見：德國明鏡周刊， Oct. 29， 2001及歐威爾的小說《1984》。

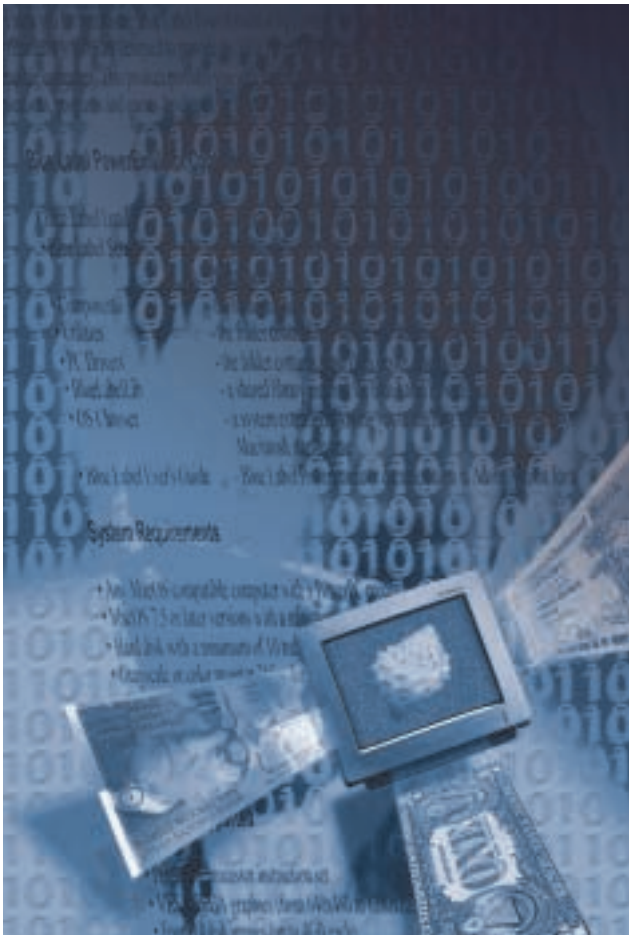
「老大哥」之間做個衡量。不過，在這個我們隨時可以聽聞「高科技保障安全」的論述中，技術發展的邏輯，往往未必保證民眾的接受(國內最典型與最熟悉的例子可能就是「以核能使用保障電力供給的安全」)。同時，今天保障安全的科技，明天可能就成為風險的來源。

讓我們先談談「生物檢測保障安全」的技術邏輯

許多身體特徵不具有重複性，也就是在兩個人身上不會發現完全相同的特徵。而且，終其一生，這些特徵也不會改變。這是自然本身就設定好的身分系統。身分證件可能被偽造，密碼可能遺失，可是自己的身體一直由自己帶著，我們不會搞丟，也不會把自己的身體交給其他人。所以，從技術的面向，生物檢測提供一個簡單與舒適的可能—我們只需「出示」個人的身體特徵，就可以認證身分。

用一個掃描器，可能是攝影機或者是指紋影像掃描器，來判讀身體特徵，是所有生物檢測的基本概念。指紋經由掃描成為數據化的圖像，再透過電腦程式辨識特徵，最後這個身體特徵將簡化為數值，即所謂的數值模組。也就是說，儲存在電腦或電子晶片裡用來確認身份的，不是指紋或者相片，而是這個簡化的最終數值。而且，這個數值模組，不可能倒轉還原為掃描前的圖像，這個特質提供原始資料不會被加工處理的安全保證。

加註生物資訊據稱可以提高人身的安全。因為，不但身分證件不容易被偽造，同時也使政府部門間可以進行快速的線上資料交換、確認與判斷，也就是透過電子化政府來杜絕恐怖分子間的連結，進而迫使他們現身。這是在席利安全方案中，生物檢測技術承擔的重責大任。



也因為身分證件上的電子晶片儲存了個人的身體特徵，例如指紋與眼球虹膜的掃描數值結果。這些數值經由電腦的確認，等於確認使用者個人的身分。在電子化政府的連線中，持卡人也就可以經由生物檢測資訊的確認，獲得進入資料世界的通行證。如果這個方式可行，那麼就可以省掉拜訪公家機關所花費的時間與精神，坐在家裡的電腦前就可以報稅、報戶口，還可以向監理所重登汽車資料。我們也可以想像，在自動提款機之前不必再苦思密碼，只要伸出指頭就可以領錢。公司的打卡鐘也不再吃卡片，反而定定地瞧著員工的眼睛，彷彿在說：「你可別想幫別人代打啊！」

然而，一項技術能不能受到廣泛接受與落實，不僅僅決定於技術本身的發展。儘管眼球虹膜辨識技術的可靠性已經獲得相當高的評價，但並不代表一般民眾會願意把站在辨識器前，讓光線照入眼睛以

確認身分這件事情，變成日常生活的一部分。雖然在技術上可行，但要發展到讓自動提款機經由指紋辨識，或者看到美麗的眼睛就吐出錢來，還要看這項技術能不能日常生活化。同時，在安全性的考慮上，生物檢測在金融界的應用，也可能給消費者帶來全新的問題。例如，在提款卡遺失而被盜領的案例中，因為密碼可能一起被偷，是銀行承擔損失的原因。但是，一旦生物檢測引入，銀行可能在類似的案例中指責顧客「漫不經心地管理自己的指紋」。因為「被偷」的指紋，很可能是在某一家餐廳所用過的某一只杯子上，輕易取得的。那麼，其他的身體特徵，例如容貌與眼睛，應該不會被偷了吧？生物檢測的確因為個人生物資訊的特殊性，而提供不易偽造的安全保證。但是，「私有化的身體特徵」並不保證可免於電腦駭客的入侵。

可以想像有人想竊取你的容貌或者眼睛嗎？不必像〇〇7影片中，大張旗鼓血腥暴力地取人眼珠。只要接一條電線到容貌或者虹膜的生物檢測系統中，電腦駭客可以從電子化政府的設計，即席利在安全措施中強調的資訊連線傳遞過程中，直接攔截個人身體特徵資料。這聽起來或許還像是科幻小說的情節，不過這類駭客入侵生物檢測系統的情事已經有了專有名詞——再現攻擊（replay-attack）。

在一項由德國聯邦資訊科技安全處（BSI）主導的研究計劃下，弗勞恩霍夫圖像資訊處理研究所（Fraunhofer-Institut, IGD）的研究人員，可以毫無困難地破解一連串從網路攔截下來的商用生物檢測資料。在這個過程中，不只是「再現攻擊」可以攔截與盜用傳輸的資料。令人驚訝的是，研究人員發現，在這個過程中甚至可以重寫系統中比對資料的「界限值」。這個問題源自技術本身的邏輯。因為，就算是在同一個人身上進行固定特徵的重複掃描，也不會每一次都辨識出相同的數值模組。所以，在生物檢測的過程中，必須靠數學運算相當程度地決定，兩組數值模組的「相似性」是不是足夠大到被接受為「相同」。在這個點上，電腦駭客就可以試圖重寫這個讓整個系統容忍的「界限值」。因此，到目前為止，利用生物資訊進行身分辨認的技術，雖然在商業上號稱已經完成，但是在安全的控制上卻還停留在實驗室的階段。

同時，以偽造的方式來入侵生物檢測系統雖然的確有相當的困難，可是基本上仍是可以辦到的。不靠駭客，用矽膠製的指紋模型來欺騙辨識系統，早已經不是新聞。雖然，新一代的指紋檢測系統已經加裝了以紅外線測試組織反射程度的設計，用來分辨「死的手指」與「活的手指」。然而，如果整個生物檢測的設計不能提供安全保證，這類加裝的設計其實只能治標，而無法提供治本方案。

從使用者的角度出發，今天如果有人忘記了密碼、遺失了卡片，只要再申請一個新的就好了。可是，如果有一天，右手拇指的生物資訊（指紋）被偷了呢？這個身體特徵從此以後就「沒有用」了。因為生物資訊給偷了，就是給偷了，什麼也要不回來了。

一個自由民主的社會，究竟應該為免於恐怖攻擊的恐懼付出多大的代價？這個代價也包含願意接受什麼樣的安全措施。德國聯邦議會在「恐怖分子就在你身邊」的風險認知下，於2001年12月20日通過席利「反恐怖攻擊」的安全方案。

然而，就如德國聯邦議會議長梯爾斯（Wolfgang Thierse）遺憾地強調：沒有百分之百的安全措施，除非我們拿自由當代價。

在生物檢測監視下的民主社會，民眾能享受到什麼樣的安全保障？問題的答案不僅存在於科技發展與民眾接受的機制裡，個人生物資訊被盜取與濫用的風險，同時成為安全措施下的另一個問題。畢竟，生物檢測系統辨認的是「身體」，而不是「個人」。 □

胡湘玲
德國Bielefeld大學「科學與技術研究中心」研究員