〈本文轉載自清流雙月刊 106 年 5 月號〉

反情報工作為國家安全之守門員

中央警察大學恐怖主義研究中心主任　汪毓瑋

在金融等投資領域，風險常是用以評估報酬的一種方法，亦即若一項投資的風險很低，那麼預期回收很大利潤的可能性就不會太高。若把此低風險卻高利潤的思考類比於情報工作，就可以了解為何情報之行動與分析人員會採取相對較低風險之行動以獲取更多的機密資訊；惟若計畫與配套措施得宜，對手又有失誤，仍然可以成功獲取高品質情報。

反情報工作之必要性

在現實情況中，低風險與高報酬，不論是在情報領域或是金融領域皆不易獲得，但風險卻是可以被逐步減緩的。而此降低風險的工作在國家安全領域中即為反情報工作，亦即反情報工作能保障採行情報工作行動的安全。

在維護國家安全脈絡下結合風險管理之思考，則任何實體，不論是個人、公司、軍方或甚至是整個政府，都需要反

情報來保護其安全與利益。因為反情報支撐著情報各個方面運作之表現，而情報則支撐著政策的不斷完善及理性的發展。進一步比擬，若情報活動是一場國與國間的運動比賽，那麼執行反情報技巧的工作人員就是守門員，若沒有這些反情報工作人員，則我們的對手將從開放且不設防的目標獲得無止盡的分數。

美國電郵門案例

美國總統大選落幕以來，對於可能來自於俄羅斯針對美國實體與網路目標的情報作為以企圖影響美國國內政治之發展，已不斷地被媒體、甚或「維基解密」爆料。不僅造成美國民主與共和兩黨之政爭，進而引發已當選之川普總統對情報機構的不信任，且竟涉及英國情報機構可能不當介入監聽的指控，以及美國中央情報局在德國建構駭客基地大肆對歐洲監聽等不法行為。此等情事反映美國反情報工作之缺失，亦引發各國警惕。

初起之時，是在總統競選期間，作為川普唯一競爭者─前國務卿希拉蕊在任內時，對於資訊安全不當處理之「電郵門事件」，當時川普就曾經公開「邀請」俄羅斯駭客入侵競選

對手希拉蕊的電腦，再去尋找「電郵門」事件中消失的3萬多封郵件。而媒體報導，俄羅斯將其入侵獲取的機密資訊，即郵件和資料，透過「中間人」提供給「維基解密」和其他受控制的網站；彼等出於各自不同目的，立即將這些機密資訊公布。接著就爆發了俄羅斯駭客是在普丁總統直接授意下，持續駭入民主黨重要人物電郵及竊取大量機密文件之指控。

此亦導致了主要負責「人員情報」之中央情報局、負責國內安全亦即「反情報」之聯邦調查局、及負責「電訊情報」之國家安全總署，在去年向仍在任之歐巴馬總統和甫當選之川普總統分別提交了一份《評估俄羅斯在近期美國總統大選中的活動與意圖》的報告，同時開放公開版本供媒體和大眾下載查閱。總結是相信俄羅斯利用駭客和情報行動干擾2016年美國總統大選，破壞大眾對民主進程的信心，且傷害了另一名總統候選人希拉蕊，並幫助川普當選。

然而是否真是駭客駭入行為讓川普當選，還是因為所揭露的「機密資訊」確實使一般民眾普遍認為希拉蕊之虛偽，實際上是兩個不同層次的問題，不應混淆。一方面，對於民

眾而言，基於「知的權利」，他們只想要瞭解所要選擇總統之品格及行事作風是否足以帶領美國及使國家更加的安全。因此，儘管所讀到的洩漏資訊來源不合法，但已足以判斷應該選擇誰。

另方面，美國情報部門的報告也指出，在2016年之大選期間，俄羅斯駭客對於民主黨與希拉蕊之攻擊與竊密早在「電郵門」事件之前即已開始，但到了最後民主黨大會才找了專業的網路安全公司對其系統安全進行評估與補救，顯示對於攸關資訊安全之網路空間管理並沒有投入太多心力。也反映網路時代，立法者和政治家必須跟上網路技術發展，認知先進的間諜技術實已脫離情報部門掌控，而落入商業機構與個人駭客手中。

俄羅斯之「駭客間諜門」事件尚未完全結束，川普總統近期又透過其「推特」社交媒體，公然指控前總統歐巴馬透過「國家安全總署」之途徑，間接藉由英國「政府通訊總部」（GCHQ）對其進行竊聽。導致「政府通訊總部」不得不立即發表強烈聲明抗議，將美國白宮聲稱其協助歐巴馬竊聽川普的指控，斥為「無稽之談」。同時，英國首相梅伊(Theresa

May）的發言人也表示，已經收到美方不會再有人提起此事的保證。

此外，「維基解密」又再度加碼爆料，揭露了8000份有關美國中央情報局駭客襲擊的檔案─Valut 7，暗示該局利用美國駐德國法蘭克福領事館作為掩護，暗中管理其駭客基地，駭入歐洲重要國家與官員之網路資訊系統。德國首席聯邦檢察官辦公室已公開表示，將仔細審閱「維基解密」文件，以了解中央情報局在當地的活動是否違法，強調如果看到具體犯罪行為或明確犯罪人士的證據，將會展開調查工作。

2017 年 3 月 20 日，聯邦調查局局長柯米在「眾院情報委員會」聽證會上表示，川普對歐巴馬前總統的指控毫無根據，也證實了該局正在調查去年川普選戰團隊與俄羅斯有無不當聯繫，及俄國政府是否想要干預去年總統大選。調查的重點包括：與川普陣營有關的個人和俄國政府之間任何關係的性質，以及川普陣營與俄方的行動之間是否有任何的協調。當然聯調局調查團隊在去年即已著手調查川普或他的親信是否觸犯《海外反腐敗行為法》（Foreign Corrupt Practices Act），以及是否與遭美國或國際金融制裁的俄羅斯人聯繫或曾進行交易，調查仍會持續地進行。美國國會亦

積極啟動應有之監督權責，強化對於進行中之外國情報有關作為及本國人可能涉及間諜行事之調查行動，並意圖補強反情報之不足。

我國反情報工作之可行方向

美國作為世界強權之一，尚不免持續遭受來自於外國之情報作為，且必然已投入大量資源，惟分工較明確之反情報工作仍然有不足之處，必須持續地加以改善。因此，我國在檢視這些具體案例時，相對於與美國反情報能力之比較，必須更加警惕，是否也可能碰到此等情事？是否已經發生了但並不知情？又應該如何因應？且能夠推動更佳事前預防之準備呢？當然反情報工作之建構並非一蹴可幾，但有幾個步驟應可先明定而依序或併行之，包括了：

第一、

重新檢視從民國38年以來之相關情報概念，是否真的清楚認識與定義，並進而能夠操作，且與時俱進地與國際接軌，而有利於未來之國際情報合作。其中包括了情報、反情報、間諜、反間諜等；且若是保防之傳統概念已漸有民意需求或反彈聲浪，亦應該勇於調整。

第二、

必須專業地整合及瞭解反情報、反間諜、安全與執法等不同實踐層面之真實關係，並進行明確之功能區隔，進而強化教育與訓練。否則實踐上必然會混淆，任務重疊、浪費資源，又不知或無感可能有更大效率之可能性；並或可以對現有體系之分工與統合進行全面檢視。

第三、

反情報之本質是「戰略性的」，而非僅是抓間諜之「戰術性的」，縱然方便而可以區隔成「攻擊性反情報」與「防衛性反情報」，但均必須服膺於戰略性目的；亦即先建構理論後，再進行可具體化之實踐行動。