2019 TWIGF 座談場次摘要報告

軍方在資安治理的角色

特派員 廖勁燿

■ 座談重點內容

- 主持人引言報告：曾怡碩 / 國防安全研究院助理研究員

  在現行法治架構，如資通安全管理法所定義之公務機關，並不包含軍事與情報機關，然而資安治理 (cybersecurity governance) 中，軍方必然是其中不可忽略的利益攸關者，但礙於種種因素，極少對外說明。如此資訊不透明的情況，對於軍方與民間相互理解並推動合作，十分不易。本次研討希望能透過討論軍方過去與現在於網路安全扮演的角色，了解資安治理脈絡下的軍文關係，並思考未來可能的合作方向。

- 與談人：杜貞儀 / 國防安全研究院博士後研究生

  議題：軍民如何合作?

  首先談到軍方在資安治理的角色，在武裝衝突外，軍方如何保護國家(national)甚至國際(international)的資訊安全(cybersecurity)，是一個極少討論，且缺乏研究的議題，政府應如何將協議保護資訊安全以及關鍵基礎設施的責任，明確的定義且區分出來，肇因為軍方在資訊安全方面很少公開討論資訊也欠缺相關研究，軍方可以算是政府公家機關單位，重點關鍵在基礎設施的保護要如何切入。

  接續從各國軍民合作的面向來切入，以荷蘭、丹麥、愛沙尼亞、捷克等四國作研究，丹麥從 2011 年將資安部門從科技部改隸屬國防部，愛沙尼亞從國防部門移到傳播部門，顯見整體著墨並非以國防

為主要考量，而捷克將資安部門納入國安局管制，另荷蘭由安全與司法部管理資安。在資安管理上的軍民合作研究發現沒有明確的相處模式，可以初步歸納歐洲的共識是軍方參加網路治理必需受到公家或民營單位的指揮領導，尤其對政府部門來說新的政策領域，是常常讓政府部門彼此相互競爭資源的戰場，這個現象很直接地反映在資安戰略上，讓資安政策在指揮系統之責任劃分不夠明確。

那如何改善責任劃分狀況，減少這種問題的產生呢？首先建議軍民辦理共同演訓，由地方政府主導，軍方配合，加上民間及其他單位，讓兩者透過平時演習時，熟悉指揮體制運作，相互瞭解各單位優缺點，可以互相通盤認識及相互支援，其次是軍中與民間、公家與私人部門間進行資安情報分析會議，劃分具體的情報關係及雙方有興趣的議題，相互交流資訊，綿密合作溝通渠道。

- 與談人：謝沛學 / 國防安全研究院助理研究員

  議題： Cybersecurity In Taiwan’s War Games

  個人專業在兵棋推演、賽局分析與軍備競賽層面，試圖來研究在臺灣戰爭競賽中網路安全，過去一年有機會與國安會美國智庫分享兵推過程發生的狀況，首先談到特別是因為決策層面並非攻防實際執行層面上的問題，使得在兵推議題中近一半以上與網路資安議題息息相關，以資安議題來說算是混和性威脅，連結在和平時代與戰爭競爭間的威脅，對攻擊的目標國及藉機入侵的國家而言，假新聞假議題中肯定有網路威脅的現象，包括近年來軍機繞臺頻傳、軍艦不小心橫渡海峽中線、運用時機攻佔太平洋上小島等等都是類似事件，特別是近幾年來遊走在灰色邊緣的威脅更具挑戰，無論是對金融層面、運輸層面、醫療層面等等進行網路攻擊，我們猜測在年底選舉來臨前，中共可能會攻擊我國中選會網站，試圖造成社會動亂，讓政府對危機管理顯得毫無能力。

  以過去的經驗在立法院會期中，委員要國防部長評估，臺灣在對中

國的軍事作戰戰力維持可以支撐多久？到底是一星期或兩星期？我認為應該要把灰色威脅列入考量中。網路攻擊是潛在性的武裝攻擊。這種灰色攻擊到達臨界點時，也就是當社會對這種攻擊的防禦或抵制能力弱化到一定程度後，攻擊國家對目標國家可以產生一定程度的影響。但是網路攻擊並非是傳統的軍事威脅。我們如何將網路攻擊作為認定是一種威脅？這種威脅是很難界定、很難加以判斷的。尤其是對網路攻擊的認知上來說，基礎常識牽涉到網路的基礎設施、潛在的網攻與敵浮有關、受害層面無法評估，指揮體系容易因為政治意志考量影響正確的判斷。尤其在軍隊中政策指揮面的人會想快速處理,馬上做出應對措施,但是網路攻擊沒有實際受害者，僅有危安和國安影響。之前的國際上國家擁有核武，可以保證相互毀滅，可以明確知道哪個國家具有威脅與報復的機制，但是說到網路攻擊與威脅，非常難以歸因與找出哪個國家發動？更難去舉證或證明，特別是網路攻擊無法實際造成人員損害，讓影響與威脅無法上升到國家層面，更難去獲得應有的重視與凝聚力量。

- 與談人：廖彥棻 / 獨立軍事分析師

  議題：「數位戰士」資安與民防

  現行資安聯防體系執行上相當困難，如同之前羅馬時代軍團的特殊兵種，培養專業與取得兵源非常難以處理。當前為何需要成立單位？首先因為資訊安全人才的不足，包括美國國家安全部、業界、軍方等各方面，因為需要的資安人才頗多，各單位都供不應求，尤其是政府招募資安人員的機制相對僵化，舉一個案例，2015 年國安局召募資訊安全人才,但是最後在資格審查方面,卻因為個人握力不足，未符合資格，導致無法招到資安人才。這個某部分來說，可以說是政府制度所導致的問題，特別是臨時資安事件造成重大損失，例如勒索木馬軟體綁架政府各機構資料，其實在臺灣也時有發生，通常都是私底下處理，究其原因為目前體制不夠周密，造成很多問題狀

況的產生。另外舉部隊的假日戰士制度,最大的缺點在於人數有限，並且受制於現有軍事指揮體系管轄，以資通電軍的單位為例，假日大約只有兩到三人，每年假日戰士會定期接受訓練與資安防護演練，若是部隊要請民間資安公司人才，來加入處理資訊攻擊事件，需要動員令才能啟動資安聯防機制。

在資安危機事件中,通常是網路攻擊事件時找不到可以處理的人，而部隊資安人才太少，無法直接處理網路攻擊事件，權衡的做法是找民間公司幫忙處理。而講到科技動員部分，問題是需要動員令，不然無法招集人才，民間網路人才身分什麼都不是，根本無法介入處理相關問題。舉例來說中國缺乏網路民兵，他們在 2015 年運用軍民合作方式，成立網路戰鬥支援部隊，讓中國網路民兵均勻分布在各個民間公司中，沒有頭銜而有相關組織，觀察網路攻擊事件大部分由民間公司出手。我國國安局很多來自民間武漢大學的網路攻擊，在目前檯面上很少人追蹤這種戰鬥支援部隊，讓戰鬥支援部隊隱藏在民間公司的後面，但是實際上來說，大陸的民營企業是由共產黨來管制與策動的。

愛沙尼亞有成立網路聯盟組織，讓全民皆兵，都可以擔任平民志願兵，讓民防組織人員接受動員令與正常組織一樣，可以有合法身分來執行資安部分的工作。對民間人士來說，頒發動員令的好處是專業培訓可以跟軍隊機關相互接軌，兩者可以取得資源共享，互相支援。但是這種運用動員令的方式，對資安人才來說，相當仰賴榮譽感與個人信念，因為這是無給職的工作。類似我國海巡署單位人員經常需要平時任務與戰時任務相互轉換，在平時具有各自負責的警衛任務，而戰時需要跟海軍一樣負有岸邊警衛任務，對進犯敵軍做初步的打擊與守備任務。參考海巡的作法來參照我國義消義警執勤的方式，從平時執行勤務的方式發想，實施訓練的工作，如果火警與交通勤務時常由義警義消結合警察跟消防隊處理，發布動員令時，義消義警可以非常順利與警察跟消防隊進行任務處置，完全在工作

上沒有窒礙難行的部分。以網路事件來說，發生網路攻擊事件 30 分鐘後，個人電腦內儲存的資料全部都會消失，通常第一線處理的資安人員，會跟受到攻擊的電腦所有人說，先把電腦關機，過五分鐘後，下一步是將電腦重新開機，當然，導致的結果就是所有的資料全部都被網路攻擊所消除。根據此一事件來說，在地人才與區域性的反應相當需要，我們要常常做資安人才培訓工作，尤其是目前最近網路攻擊事件經常發生在暫存記憶體上，對平常資安稽核的人員來說，會發生儲存資料不齊全和資料消失的詭異狀況，就連電腦實際每日操作人員都不會發覺電腦的異常。

在目前軍民合作上，及資安人才招募部分，最重要的原因是工作職缺的誘因，歸因於制度面，軍隊機關與公務機關在薪資及福利措施上，無法超越民間公司，在公家機關的人都知道，民間機構不需要考一些認證考試，不用取得公家機關的證照或專長，不會限制照相手機的使用，也不會限制上班時間用社交軟體等等。另外來說，資方防護與政府體系中存在編制與授權的問題，到底哪個部門來負責呢?以美國為例，資安處、聯二情報、聯六作戰、國土安全部都不知道由誰負責、由誰主導，最重要的是指揮權在誰身上。建議臺灣由國防部機關各處或由立法院來做個體系間的協議。

- 與談人：曾怡碩 / 國防安全研究院助理研究員

  議題：網路作戰人力需求與資安產業人才培育

  資訊人才在部隊面臨兩個問題，第一是晉用的問題，資安人才知道什麼是網路攻擊，與電腦部門如何進行防禦作為，在網路課程上，有相當多的網路防禦課程可以學習，從一開始的 DOS、C 語言、R 語言、Python 等等，資安人員需要的背景知識庫相當龐大，在資安人員的評比上，無法衡量學習舊程式語言的比較強，還是學習新電腦語言的比較強，資安人才間無法相互對比能力的高低，因為齊頭上的平等與基準點。第二是留用的問題，國安會網路作戰人才的需

求，跟民間資安產業的人才需求一樣多，在薪資考量與福利措施部分，大多數的資安人才會選擇民間企業，比較少會留在部隊機關中。

因為臺灣是資安與通訊大國，在一般人的想法中，第四軍通資電軍資安人才的兵源是不虞匱乏，但是以臺灣資安人才來說，就薪資做第一考量，通常會先去科學園區，接續是法人資策會、工研院、科技部等等，另一部分也是因為工作環境的關係，公家機關可以準時上下班按表操課，就已經是非常幸福的單位，而民間機關可以彈性上班，也可以視訊上班，相對來說，完全沒有可比性。根據經驗法則來說，建議軍方、公家機關與民間企業可以交流，在部隊具有網路攻擊時經驗的人，退伍後到民間企業上班，可否回到部隊中擔任顧問與工作交流，讓高手在民間、軍中有能手，並透過考試院規劃制度，讓軍中的規範跟民間規範一樣。

■ 座談結論

- 共識

軍方與民間相互理解並推動合作，十分不易。希望能透過討論軍方過去與現在在網路治理上扮演的角色，試圖瞭解資安治理脈絡下的軍文關係，並思考未來可能的合作方向。

- 歧見

對政府部門來說網路治理算的上新的政策領域，是常常讓政府部門彼此相互競爭資源的戰場，這個現象很直接地反映在資安戰略上，讓資安政策在指揮系統之責任劃分不夠明確，在軍民關係上對兩者影響頗大。

- 建議

一、首先建議軍民辦理共同演訓，由地方政府主導，軍方配合，加

上民間及其他單位，讓兩者透過平時演習時，熟悉指揮體制運作，相互瞭解各單位優缺點，可以互相通盤認識及相互支援，其次是軍中與民間、公家與私人部門間進行資安情報分析會議，劃分具體的情報關係及雙方有興趣的議題，相互交流資訊，綿密合作溝通渠道。

二、對網路攻擊的認知上來說，基礎常識牽涉到網路的基礎設施、潛在的網攻與敵浮有關、受害層面無法評估，指揮體系容易因為政治意志考量影響正確的判斷。尤其在軍隊中政策指揮面的人會想快速處理，馬上做出應對措施，但是網路攻擊沒有實際受害者，僅有危安和國安影響。所以建議相關部門應明確定義網路攻擊影響層面與因應措施，讓介入層級能符合實需。

三、資方防護與政府體系中存在編制與授權的問題，到底哪個部門來負責呢?以美國為例，資安處、聯二情報、聯六作戰、國土安全部都不知道由誰負責、由誰主導，最重要的是指揮權在誰身上。建議臺灣由國防部機關各處或由立法院來做個體系間的協議。

四、建議軍方、公家機關與民間企業可以交流，在部隊具有網路攻擊時經驗的人，退伍後到民間企業上班，可否回到部隊中擔任顧問與工作交流，讓高手在民間、軍中有能手，並透過考試院規劃制度，讓軍中的規範跟民間規範一樣，相互間可以交流與回流。

■ **心得感想**

軍隊在資安治理 (cybersecurity governance) 中，可謂多方利益關係人之一，能在保密原則與較為封閉的制度下，參加民間網路治理論壇實屬難能可貴，藉由政府、民間、軍方在同一平臺上進行對話，從網路設施建構、資訊軟體管制、實體與虛擬管理等層面進行經驗交流，相信對軍隊資安政策健全、資安人才培訓與管理、網路攻擊危機處理流程等等實務經驗上，都能有所改變與潛移默化的影響。

目前軍隊中仍存在不可改變的制度與環境限制，對資安人員、軍民關係、網路治理上，都具有相當程度的侷限性，若能讓管理階層持續跟民間對話，相信可以逐步改善所面對的問題跟挑戰，畢竟網路攻擊事件或資安危機都是與時俱進，時刻不停歇，需要大家共同面對。