當前「混合式威脅」對我國家安全的衝擊和因應

國防大學中共軍事事務研究所副教授　董慧明

資料來源：本文轉載自法務部清流雙月刊 109 年 3 月號

《摘要》

「混合式威脅」(Hybrid Threat）是一種隨著安全環境變遷所產生的新興安全威脅，正對各國帶來嚴峻挑戰。從攸關國家生存發展的政治、經濟、軍事、外交等傳統安全領域，到影響民眾生計、社會安全、金融秩序、恐怖攻擊、暴力犯罪、資訊網路安全等等，「混合式威脅」同時涵蓋了傳統和非傳統安全議題，跨越了虛擬和實境空間。當攻擊者對目標國家、民眾採取無預警的威脅攻勢，無論是政府部門或是社會大眾，皆應對這種新形態威脅建立正確認知，並且審慎因應，以確保國家和民眾最大安全福祉。

「混合式威脅」的源起和特性

緣起於美軍在中東反恐戰場上對新形態戰爭的體驗，「混合式威脅」相關概念於 21 世紀初就相繼在美國國防部、參謀首長聯席會議公布之《國防戰略報告》(The National Defense Strategy of the United States of America)、《四年防務評估報告》(Quadrennial Defense Review Report, QDR)、《美國國家軍事戰略》(The National Military Strategy of the United States of America）中被提出。學者 Frank Hoffman 在《21 世紀衝突：混合戰爭的興起》(Conflict In the 21st Century: The Rise of Hybrid Wars）著作中亦呼籲美國正視混合形態的威脅。綜合美國官方和學者的論述觀點，吾人可將「混合式威脅」界定為：

“國家或非國家行為者為實現政治目的、達到經濟目標，在戰場上同時採用常規武器、非常規戰術、恐怖主義、犯罪行為等一系列結合先進科技和武裝力量之複雜組合手段，以出乎意料的方式，鎖定對手進行有形和心理層面的打擊。”

由以上定義可知，「混合式威脅」的特性是進擊「多源」、方法「多元」。無論是外部安全或是內部安定，攻擊者交織運用傳統和非傳統安全威脅的複合型手段，針對特定目標進行有形、無形和實體、虛擬的攻擊或破壞，成為當前各國面對的國家安全難題。

「混合式威脅」的主要類型和對國家安全的衝擊

儘管「混合式威脅」的態樣眾多，當前最受到關注且最難以防範的類型就是結合資訊網路之科技應用威脅。例如：網路恐怖主義、網路滲透，以及網路輿論戰、心理戰、法律戰。攻擊者不僅將資訊網路視為募集成員、發動攻勢的媒介工具，必要時更將資訊網路當作攻克癱瘓的目標。

一、「混合式威脅」的主要類型

（一）網路恐怖主義

以興起於 2014 年 6 月的「伊斯蘭國」（Islamic State in Iraq and Syria, ISIS）宗教極端組織為例，除了積極在敘利亞、伊拉克發動武裝攻擊，擴張勢力據點外，為加大對全世界穆斯林的影響力，透過建立網站、發行網路宣傳刊物《達比克》（Dabiq）、《新聞》（al-Naba）、散發文宣、下達恐怖活動指令，該組織亦利用資訊網路在全世界召募成員。雖然「伊斯蘭國」領袖巴格達迪（Abu Bakr alBaghdadi）的死訊重創聲勢，惟殘餘勢力並未銷聲匿跡。其成員流竄全球各地，並且活躍於網路世界聯繫訊息，伺機攻擊，成為國際反恐更加難以防範的潛在威脅。

（二）網路滲透

以 2014 年俄羅斯合併克里米亞半島案例最受關注。2013 年 11 月，烏克蘭爆發「親歐」、「親俄」兩股勢力之群眾示威和支持集會活動，造成國家政局動盪。位在烏國東部的克里米亞半島，亦因俄羅斯從外交、軍事、網路輿論、心理、法律、經濟等途徑介入「克里米亞歸屬公投」，影響「親俄」烏克蘭民眾政治態度，被視為成功運用混合戰法之典型案例。俄羅斯同時運用軍事和非軍事手段達到政治目的的方式，除了將「混合式威脅」的場域從戰場延伸至議場，也讓各國警覺這種透過資訊網路對特定對象輸入政治主張，進而改變該國內部主流民意和影響投票的作法，成為必須設防的重點。

（三）網路輿論戰、心理戰、法律戰

以中共對臺進行之「三戰」攻勢最為明顯。中共在軍事教材中，明確指出：「輿論戰是心理戰和法律戰的實施平臺、心理戰是輿論戰和法律戰的根本落腳點、法律戰為輿論戰、心理戰提供法理依據」。另外，中共亦將「三戰」視為配合國家政治、外交、軍事鬥爭的重要形式。以此檢視中共近年來對臺進行之文攻武嚇，以及打壓臺灣國際活動空間、強奪臺灣邦交國等舉動，除了不利於兩岸關係實質發展，更可印證臺灣當前遭受來自中共利用假新聞、虛假訊息進行輿論和心理攻擊，已成為誤導和分化社會內部和諧之主要危害。可見 利用資訊網路進行網路「三戰」，亦為維護國家政局安定和社會安全之防範重點。

二、「混合式威脅」對國家安全的衝擊

「混合式威脅」開始在國內受到關注的主要原因，是因為這種同時包括正規和非正規攻擊的行為，正利用像臺灣主張民主自由和尊重基本人權等類型國家的國情相對開放、透明等特點，進行無煙硝的輿論和心理分化影響。這種過去較常在政局動盪國家才會出現的政治現象，隨著資訊科技、網路技術、媒體傳播能力的躍進提升，在近年來亦成為民主化國家遭到假新聞、虛假訊息等惡意攻訐、滲透分化常見的慣用手法。

基於前述對目前「混合式威脅」主要類型之概略介紹，可見各國當前面臨的

安全威脅來源，主要來自特定國家或非國家行為者，從虛擬世界向現實世界的目標對象發動之綜合性攻擊。對此，歐盟於 2018 年 6 月公布《增進應對混合威脅能力和恢復力》(Joint Communication Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats) 報告，呼籲各成員國必須提升網路攻擊追蹤能力，不僅要阻止潛在攻擊者，也要追究責任。歐盟認為「混合式威脅」的攻擊者毋須對他國宣戰，便能靈活運用外交、軍事、經濟、科技等方法製造混淆，以實現特定政治目的。因此，「混合式威脅」的危害程度，輕則造成國家內部紛亂無序，重則亡國亡民，對國家安全的危害毫不亞於傳統的軍事武力威脅，或是單一層面的非傳統安全危害。

全民應有的防範意識

「混合式威脅」盛行於 21 世紀資訊時代，是多領域的綜合性較量，必須建立聯防機制。從國家安全的面向以觀，吾人追求的是國家處於外部沒有威脅且內部團結安定的狀態，因此，必須確立主權、領土、政治、經濟、軍事、資訊、科技、文化、環境和國民的總體安全。然而，「混合式威脅」已成為當前國家安全、國防安全、國土安全和民事安全最主要的危害，且因同時包括軍事和非軍事、常規與非常規，以及傳統和非傳統手段的綜合運用，故在防範作法方面須仰賴政府權責相關部門和全體民眾共同建立公務協調、公私夥伴的安全合作意識。

(一) 政策面

首先是安全規範的制定。當前包括美國、歐盟、澳洲等諸多民主法治國家皆因發現「混合式威脅」對於國家安全構成嚴重危害，正著力完善國家法規以有效確保國家安全利益。臺灣亦應從國情和安全兩個面向著眼，置重點於杜絕境外威脅和境內影響公共安全情事，研訂相關法規制止惡意傷害國家安全等危安行為，並且保護勇於檢舉不法之吹哨者(Whistle Blower)。其次，政府部門亦須兼顧政策溝通，使民眾了解國家面對安全威脅做出的因應對策，化解疑慮，方能形塑全民防範「混合式威脅」共識。

(二) 執行面

包括政府部門對假新聞、虛假訊息的即時查證和澄清，以及強化國安情治單位各層級之間的交流、經驗互鑒，並且建立危安預警情報之相互通報機制。就現況而論，我國行政院除了建置「即時新聞澄清專區」，即時澄清各部會遭到誤解之政策訊息，亦和國內社群通訊軟體 LINE 合作成立「行政院澄清專區」。此外，包括「資訊工業策進會」、「臺灣事實查核中心」等財團法人、基金會等民間機構亦著力於打擊假訊息等資訊安全技術精進，運用公私夥伴作法，進而大幅降低安全威脅。

(三) 教育面

主要是指將正確的網路使用態度和行為規範，以及對於真假訊息的批判思考方式納入各級學校教育和社會教育。檢視公開資料可以得知，位在北歐的國家—芬蘭，政府為了防止假訊息介入國內選舉事務，除了從教育層面

強化國民、學生、記者、政治人物的數位能力外，亦著重強化批判性思考能力，亦即從養成查證事實的日常生活態度著手，減少不實訊息的傳播。臺灣亦應重視資訊網路安全和倫理教育，培養民眾健康上網、合理使用網路習慣，遏止網路亂象對國家安全的衝擊。

結語

隨著國家安全的威脅種類愈趨複雜，資訊科技、社群網路環境的成熟以及廣泛運用，「混合式威脅」這種新形態的安全威脅正從國際問題向國內公共安全事務領域延伸。檢視各國案例和典型的威脅種類可知，「混合式威脅」已嚴重阻礙民主法治國家制度運作，造成國家利益和人民生命財產損耗、關鍵基礎建設破壞，以及社會動盪不安等情事。當前各國政府不僅高度警覺，且積極著手防範。

臺灣，由於堅守民主自由法治，包容多元族群、尊重文化，讓國家在世界上獲得民主友盟的認同和支持。然而，臺灣珍貴的民主價值在當前亦面臨嚴峻的「混合式威脅」。以維護國家安全為設想，必須全面提升全國策應各種安全威脅的綜合能力。因此，政府相關部門亦應以政策為導向、以公私夥伴為務實作法，並且以教育作為預防之道，建立政府和民間攜手合作防範共識，共同防禦安全威脅。