

# 「混合式威脅」的國安挑戰與因應對策

董慧明

國防大學中共軍事事務研究所副教授

## 摘 要

本文以「混合式威脅」對國家安全的影響為主軸，認為在進入 21 世紀後，隨著資訊網路技術日益成熟，應用層面愈來愈多元，除了帶來便利，特定或不法人士對實體、心理進行攻擊，採用傳統、非傳統手段瓦解國家，亦已成為各國國家安全工作的新挑戰。文中除了從軍事、安全兩個面向界定「混合式威脅」，亦區分網路滲透、網路恐怖主義、網路心理戰、輿論戰、情報戰等面向，說明「混合式威脅」的主要類型和特點。為了能夠有效管控，減少危害，文末提出從教育訓練、危機管理，以及情報合作三方面著手，並且認為儘管「混合式威脅」不易防處，惟若能從安全觀念建立做起，落實政府政策溝通和澄清機制，並且在各單位間保持良好的國內及國際情報合作關係，定能降低威脅。此外，防範「混合式威脅」容易觸及執法正義和基本人權自由爭議，當防禦和反制的安全機制成為常態化的管控重點，均衡法律、政府公共政策和民眾權益，亦為不容忽視之重要課題。

關鍵詞：混合式威脅、網路滲透、網路恐怖主義、情報

# **The National Security Challenges and Respond Countermeasures of “Hybrid Threats”**

**Hui-Ming Tung**

Associate Professor, Fu Hsing Kang College,  
National Defense University

## **Abstract**

The study focuses on the influence of “hybrid threat” to national security. Since the 21st century, with the maturity of information network technology, the application level has become more and more diversified. In addition to bringing convenience, attacks on physical and psychological by specific, illegal personnel, or use traditional, non-traditional means to disintegrate the country, have become a new challenge for national security work. We are not only to define the “hybrid threats” from military and security aspects, but also distinguish between internet infiltration, cyber terrorism, internet psychological warfare, public opinion warfare, and intelligence warfare, indicating the main types of “hybrid threats” and features. In order to effectively control and reduce harm, the study proposes to start from three aspects: education training, crisis management, and intelligence cooperation. Although “hybrid threats” are not easy to prevent, but we could start from the security attitude, implement

government policy communication, clarification mechanisms, and maintain well domestic and international intelligence cooperation between relevant units, that's will be able to reduce threats. Finally, preventing "hybrid threats" easily touches on law enforcement justice and fundamental human rights freedom disputes. When security mechanisms of defense and countermeasures become the control emphasis of normalization, balancing the laws, government public policies and the rights and interests of the people is also an important issue that couldn't be ignored.

Keywords: hybrid threat, internet infiltration, internet terrorism, intelligence

## 壹、前言

國家安全 (national security) 是個多層次且面向廣的工作，向來受到各國高度重視。它既包含了觀念認知、制度設計、運作方式，亦涵蓋傳統威脅中的政治、經濟、軍事、社會方面，以及非傳統安全中文化、生態、環境、能源、科技方面所衍生的各種安全領域。儘管各方對國家安全的見解莫衷一是，惟吾人若將國家安全區分內部和外部的防禦，以及柔性、強硬兩種因應對策，在圖 1 的象限圖中，可見隨著時空環境的遞變，國家安全威脅已從傳統上運用國防軍事硬實力有形力量實現政治或戰略目標的方式，向利用非軍事手段，卻仍然能夠對特定國家的文化認同、價值體系、民眾思想意識發動軟實力的無形力量攻勢。這種「混合式威脅」(hybrid threats) 無論是對實體、心理進行攻擊；採用傳統、非傳統手段瓦解國家，其造成的政治紊亂、經濟動盪、資產損失、社會失序、民眾恐慌等嚴重問題，不僅成為當前世界各國面對國家安全課題時的新挑戰，又因在查處、執法、反制作為方面易涉及介於法律規範和人權自由之間的兩難爭議，至今仍然難有標準答案和共識，突顯出對國安挑戰和因應對策等值得深究問題之重要意義。

「混合式威脅」主要來自於虛擬世界的無政府狀態 (anarchy) 以及失序的假新聞 (fake news)、錯誤訊息 (misinformation)、假訊息 (disinformation) 問題。儘管英國劍橋大學 (Cambridge University) 已於 2017 年 2 月出版《可適用於網路行動國際法的塔林手冊 2.0 版》(Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations)，欲從國際法規範外部的網路威

脅，惟受限於該網路空間國際規則對國家並不具有法律約束力，並無法杜絕網路攻擊活動。<sup>1</sup>其次，儘管各國重視國內資訊和網路安全問題，啟動相關法規的制定和修法工作，惟從實際執行結果以觀，全世界超過 30 億網民 (netizen) 在虛擬世界中傳播各種訊息，往往愈採取限制作為，引起的輿論反彈就愈加激烈。這種現象尤其在民主國家中最為明顯，吾人可從後九一一時期歐美國家設法反恐、解決暴力攻擊事件，或是起始於 2010 年 12 月的茉莉花革命 (Jasmine Revolution) 得到印證。時至今日無論這股推翻威權統治實現民主的運動是否達到當地國家民眾的預期目標，惟在此期間透過網路社群媒體，轉換為具體的公民不服從、示威、罷工、自焚、起義等激烈抗爭，著實震驚全世界。



圖 1 國家安全威脅變遷示意圖

資料來源：作者自行繪製

<sup>1</sup> Michael N. Schmitt ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (London: Cambridge University Press, 2017); Jeff Kosseff, *Cybersecurity Law* (Hoboken, N.J.: John Wiley & Sons, 2019), p. 414.

上述種種從虛擬世界向現實世界進擊的方式，結合當前國際間共同面臨的恐怖主義、資訊安全、金融安全、關鍵基礎建設防護等非傳統安全領域中的威脅，已成為各國的難題。網際網路 (Internet) 發展短短近 30 年的時間，因多元、快速、便利產生的正向效應，已對人類的生活模式產生翻天覆地的改變。然而，負面的違法犯罪行徑，則是對國家治理策略帶來更嚴峻的考驗。由此衍生出的危安問題，不僅對基本的社會秩序安定造成威脅，對於國家政治、經濟、軍事更已構成新型態的安全挑戰。本文採用「公共危機管理」(public crisis management) 研究途徑，<sup>2</sup> 以當前在資訊網路虛擬世界中興起的「混合式威脅」為主要的研究範圍，並且認為這種新興威脅對國家和社會公共安全而言具有「共承風險」(shared risk) 性質，有賴公部門 (public sector)、私部門 (private sector) 以及第三部門 (the third sector) (例如：非營利組織、非政府組織、公益組織等) 合力做出公共反應 (public response)，紓解危機威脅。<sup>3</sup> 研究透過官方文件和相關議題文獻之蒐整分析、比較研究之質性研究方法，適時舉出例證，說明從傳統的國家安

<sup>2</sup> 「公共危機管理」是指政府部門因應自然災害、科技損害、人類衝突、政治動盪等跨越環境、公民、心理、媒體、健康、安全以及政治層面之公共危機事件，在危機的潛在、產生、發展過程中，採取預防、處理、控制、評估、恢復之危機管理對策作法，減少、消除公共危機造成的影響和危害，進而達到避免危機和完善危機管理制度目的。見 Michael J. Hillyard, *Public Crisis Management: How and Why Organizations Work Together to Solve Society's Most Threatening Problems* (Bloomington, IN: iUniverse, 2000), pp. 1-2.; 張永理編，《公共危機管理》（武漢：武漢大學出版社，2015），頁 10-11。

<sup>3</sup> 詹中原、朱愛群、李宗勳、鄭錫鏞，《政府危機管理》（臺北市：國立空中大學，2006），頁 44。

全威脅向資訊時代國家安全威脅變遷中，頻發在國家內部的網路滲透、網路恐怖主義，以及網路心理戰、輿論戰、情報戰等「混合式威脅」的類型、特點、危害，以及可行的因應對策。

## 貳、「混合式威脅」的涵義

「混合式威脅」可以從軍事和安全兩個領域加以界定。前者主要是指國家對因應戰爭衝突型態的一種新觀察；後者則是政府公部門對處理國家公共安全事務的一種新體認。由於「混合式威脅」的發動者往往同時採取常規和非常規的綜合運用攻勢手段，其影響層面和危害程度往往超越傳統或非傳統安全單方面的威脅。

### 一、軍事領域的緣起和界定

「混合式威脅」緣起於美國歷經反恐戰爭所提出的安全威脅辭彙。美軍基於反恐戰爭實際經驗，認為對手採取的威脅類型通常包括：常規戰爭、非常規戰術、恐怖主義活動、無差別暴力攻擊、強制行為、犯罪行為等多種衝突形式。為了能夠取得戰場優勢，減少美軍傷亡，美國國防事務專家自 2000 年起開始呼籲要重視「混合式威脅」的研究。<sup>4</sup> 此外，美國國防部等部門亦在國防和軍事戰略報告等文件中主張必須對新型態戰爭衝突中的「混合

---

<sup>4</sup> 例如：2007 年，美國軍事學者霍夫曼 (Frank Hoffman) 在其《21 世紀的衝突：混合戰爭的興起》著作中，首次探討「混合戰爭」。他指出現代戰爭形態正在改變，從傳統的大規模正規戰爭、小規模非正規戰爭，逐步轉變為一種戰爭界限更加模糊、作戰樣式更趨統合的「混合戰爭」。見 Frank G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars* (Arlington, VA: Potomac Institute for Policy Studies, 2007), pp. 17-33.

式威脅」建立正確認知。首先，依據 2005 年 3 月公布之《美國國防戰略報告》(The National Defense Strategy of the United States of America 2005)，認為美國必須面對來自傳統的 (traditional)、非正規的 (irregular)、災難性的 (catastrophic)，以及破壞性的 (disruptive) 挑戰。<sup>5</sup> 其次，再檢視 2006 年 2 月的《四年防務評估報告》(Quadrennial Defense Review Report, QDR)，其內容亦指出美軍在 21 世紀除了要在傳統戰爭中保持優勢外，亦須進行改革，以解決非傳統、不對稱的挑戰，其中即包括非常規戰爭、災難性恐怖主義，以及破壞性威脅。<sup>6</sup> 而在美國 2010 年《四年防務評估報告》中，正式以「混合」(hybrid) 一詞來說明戰爭衝突的複雜性，並且指出美軍必須在面對多元安全威脅、衝突方面做好準備。<sup>7</sup> 2015 年 6 月，美國參謀長聯席會議 (Joint Chiefs of Staff) 公布《美國國家軍事戰略》(The National Military Strategy of the United States of America 2015)，正式提出「混合式衝突」(hybrid conflict) 是美軍必須有效因應的威脅重點（如圖 2 所示）。<sup>8</sup> 2018

<sup>5</sup> U.S. Department of Defense, *National Defense Strategy*, March, 2005, pp. 2-3, available on: <<https://www.hsdl.org/?view&did=452255>> (2019 年 10 月 15 日查詢)。

<sup>6</sup> U.S. Department of Defense, *Quadrennial Defense Review Report*, February 6, 2006, p. 3, available on: <<https://archive.defense.gov/pubs/pdfs/QDR20060203.pdf>> (2019 年 10 月 15 日查詢)。

<sup>7</sup> U.S. Department of Defense, *Quadrennial Defense Review Report*, February 1, 2010, p. 8, available on: <[https://dod.defense.gov/Portals/1/features/defenseReviews/QDR/QDR\\_as\\_of\\_29JAN10\\_1600.pdf](https://dod.defense.gov/Portals/1/features/defenseReviews/QDR/QDR_as_of_29JAN10_1600.pdf)> (2019 年 10 月 15 日查詢)。

<sup>8</sup> U.S. Joint Chiefs of Staff, *The National Military Strategy of the United States of America 2015*, June, 2015, p. 4, available on: <[https://www.jcs.mil/Portals/36/Documents/Publications/2015\\_National\\_Military\\_Strategy.pdf](https://www.jcs.mil/Portals/36/Documents/Publications/2015_National_Military_Strategy.pdf)>



年 1 月，在美國國防部公布的《國防戰略報告》(2018 National Defense Strategy of the United States of America) 中，直指恐怖份子以美國為目標，試圖對公民個人、經濟、國防、政府關鍵基礎設施進行攻擊，而當數位化已經連結民眾的生活和商業活動，其中的安全漏洞，也成為美國在衝突中遭受敵方進行政治和資訊顛覆活動的弱點，必須優先防範。<sup>9</sup>

檢視上述官方國防和軍事戰略報告文件，可以綜整出：「混合式威脅」的主體可以是國家，也可以是非國家行為者 (non-state actors)，<sup>10</sup> 他們為能達成特定的政治或經濟目標，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運用手段，以出人意料之外的方式，鎖定對手進行有形和心理層面的打擊。美國不僅將「混合式威脅」視為新型態的戰爭或衝突型態，更重要的是在這種新思維中，無論是作為敵國對手、非國家行為者，針對特定目標進行有形、無形和實體、虛擬的攻

---

(2019 年 10 月 15 日查詢)。

<sup>9</sup> U.S. Department of Defense, *National Defense Strategy*, January, 2018, p. 3, available on: <<https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf>> (2019 年 10 月 15 日查詢)。

<sup>10</sup> 依據英國牛津英語辭典對「非國家行為者」之定義是：具有重要政治影響力，惟並未與任何特定國家或地區結盟的個人或組織。這個概念通常指涉國際關係研究領域，各學派亦有各自不同的見解。例如：理想主義者將「非政府組織」視為「非國家行為者」，且是全球化時代挑戰國家威權主義的新興力量；現實主義者則是將「非國家行為者」視為破壞國家體系穩定和民族團結的潛在的革命者。本文檢視之美國官方和軍方報告內容，主要偏向現實主義者的觀點。見 Daphné Josselin and William Wallace, “Non-state Actors in World Politics: A Framework,” in Daphné Josselin and William Wallace eds., *Non-state Actors in World Politics* (London: Palgrave Macmillan, 2001), p. 1.

擊或破壞，已成為當前各國必須嚴陣以待的安全威脅課題。

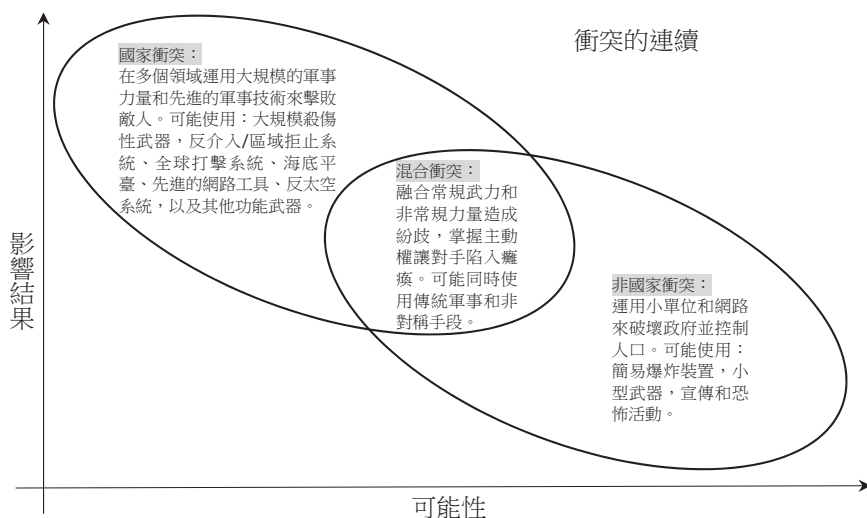


圖 2 衝突的連續：國家、非國家和混合衝突示意圖

資料來源：U.S. Joint Chiefs of Staff, *The National Military Strategy of the United States of America 2015*, June, 2015, p. 4

## 二、安全領域的延伸和界定

「混合式威脅」主要根源於國家安全威脅的複雜性以及現代科技的發展。伴隨資訊科技、社群網路環境的成熟和廣泛運用，「混合式威脅」已從國家的戰爭衝突威脅，向國內公共安全問題延伸。其中，備受關注討論的案例，就是發生於 2013 年底俄羅斯介入烏克蘭東部軍事衝突，以及在 2015 年 9 月 30 日出兵敘利亞空襲「伊斯蘭國」(ISIS) 極端恐怖組織，結合常規和非常規性戰爭特性之軍事行動。當時俄軍除了運用高科技武器於戰場，亦結合外交、網路輿論、心理、法律、經濟等非常規戰法，進而取

得戰略上的優勢與成果。<sup>11</sup> 這種混合交錯運用戰術戰法的作戰模式，除了讓各國體認到未來的戰爭型態已不再是槍林彈雨，兩軍的對陣攻防，更重要的是這種「兵不見血刃」的威脅，已隨著世界各國的相互關聯、日益緊密，而延伸至每個國家內部，攸關民眾的生活和國家安定。

基於上述的觀察，又可以歐盟近年來對於內部和外部安全環境的因應方式作為例證。首先，對於歐盟而言，先後看見發生於 2010 年 12 月在中東和北非地區的「阿拉伯之春」(Arab Spring)、敘利亞、利比亞等國的內亂、「伊斯蘭國」猖獗的恐怖活動等失序的國家和區域治理情事。而難民潮、恐怖攻擊造成的「雙生危機」(twin crisis) 亦大幅改變了歐盟內部的安全戰略環境。<sup>12</sup> 依據歐盟於 2016 年 6 月公布之《共享的願景、共同的行動：建設更強大的歐洲—歐盟外交和安全政策全球戰略》(Shared Vision, Common Action: A Stronger Europe A Global Strategy for the European Union's Foreign and Security Policy) 報告，指出歐盟的內部和外部都存在著危機，包括恐怖主義、混合式威脅、經濟動盪、氣候變遷，以及能源危機已危及到聯盟的人民和疆域。為了確保歐盟本身的安全，必須優先採取務實行動鞏固歐盟內部團結，並

<sup>11</sup> Roman Rukomeda, "Russia's Hybrid War Against Ukraine: The Latest Developments and Trends," *Centre for Integrity in the Defence Sector*, September 28, 2018, available on: <<https://cids.no/2018/09/28/russias-hybrid-war-against-ukraine-the-latest-developments-and-trends/>> (2019 年 10 月 15 日查詢)。

<sup>12</sup> Stephen Fidler, "A Perilous Year for European Unity," *The Wall Street Journal*, January 4, 2016, available on: <<https://www.wsj.com/articles/a-perilous-year-for-european-unity-1451817767>> (2019 年 10 月 15 日查詢)。

且要加強遏阻外部威脅的能力。<sup>13</sup>

2018 年 6 月，歐盟公布《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，內容直指歐盟各成員國必須提升網路攻擊追蹤能力，一方面要阻止潛在的攻擊者，也要增加對當事者究責的可行性。包括強化情報共享機制作法在內，亦被認為是制止混合威脅的有效方式。<sup>14</sup> 歐盟認為，混合威脅包括一切傳統和非傳統、軍事與社會心理層面活動，意圖製造混淆，以達到特定政治目的。其中，不僅是單純的軍事攻擊，在交戰前，更包含了外交、經濟、科技領域之輿論戰、心理戰、法律戰、資訊戰的混合運用，以取得致勝先機。<sup>15</sup> 而歐盟將「混合式威脅」定義為：由國家或非國家行為者混合外交、軍事、經濟、技術等手段進行的脅迫性和非傳統活動。他們能夠靈活運用這些

<sup>13</sup> European Union Global Strategy, “Shared Vision, Common Action: A Stronger Europe a Global Strategy for the European Union’s Foreign And Security Policy,” *European Union*, June 2016, available on: <[http://eeas.europa.eu/archives/docs/top\\_stories/pdf/eugs\\_review\\_web.pdf](http://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf)> (2019 年 10 月 15 日查詢)。

<sup>14</sup> European Commission, *Report on the Implementation of the 2016 Joint Framework on Countering Hybrid Threats and the 2018 Joint Communication on Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats*, May 28, 2019, available on: <[https://eeas.europa.eu/sites/eeas/files/report\\_on\\_the\\_implementation\\_of\\_the\\_2016\\_joint\\_framework\\_on\\_countering\\_hybrid\\_threats\\_and\\_the\\_2018\\_joint\\_communication\\_on\\_increasing\\_resilien.pdf](https://eeas.europa.eu/sites/eeas/files/report_on_the_implementation_of_the_2016_joint_framework_on_countering_hybrid_threats_and_the_2018_joint_communication_on_increasing_resilien.pdf)> (2019 年 10 月 15 日查詢)。

<sup>15</sup> Georgios Giannopoulos, “Introduction to the concept of Hybrid Threats,” *European Energy - Information Sharing & Analysis Centre*, September 7, 2017, available on: <<https://www.ee-isac.eu/hybrid-threats>> (2019 年 10 月 15 日查詢)。

方法，在低於正式對他國宣戰的門檻下，實現其具體目標。

## 參、虛擬世界中「混合式威脅」的主要類型和特點

從對「混合式威脅」的界定中可知，全球化和資訊網路技術成熟加速了全世界經濟、社會和文化的連結互動，縮短了人與人之間聯繫的距離。然而，造成部分國家和地區的分化與失衡發展，導致利益衝突加劇卻也是不爭的事實。對於當事國政府或是當地民眾而言，利用資訊網路、社群媒體傳播訊息的方式、速度已遠遠超過傳統媒體，所有對於公平正義不滿現狀的情緒也在虛擬世界中尋求宣洩。網民之間唇槍舌劍進行激烈的言辭交鋒，甚至號召網路群眾匯聚抗爭行動力量，而少數極端激進和不法份子亦利用網路招募成員，煽動仇恨，找出資訊防護弱點進行攻擊破壞。這些在虛擬世界中進擊，進而扭轉原本在現實世界中居於劣勢的「混合式威脅」正是安全環境日益複雜的主因。

### 一、網路滲透

在民主國家中，網路是自由開放的空間，其隱蔽的性質更提供使用者能夠隱姓埋名，表現網路的個性行為。然而，當這種自由與權利遭到敵對勢力、犯罪或不法份子利用時，便成為「混合式威脅」的一種主要形式。從學理上而論，網路滲透是一種利用網路進行價值觀和意識形態輸入的過程，它可以做為一種攻勢手段、一種資訊攻擊技術，也是操作分化、離間和製造國家內部紛亂無序的方法。網路滲透者透過對特定議題的價值觀輸出，利用虛擬世界中多元的傳播管道詆毀國家制度，編造、傳播謠言混淆視聽，進而在無形之中影響對象國家人民，質疑政府政策，甚至

產生非理性的對抗行為。這種藉由滲透方式產生的威脅，遊走在合法與違法的法律邊緣，挑戰執法權限，卻能對國家安全造成難以彌補的危害，同時耗費鉅額社會成本，嚴格考驗各國的公共治理能力。尤其對民主國家而言，必須兼顧法治和自由人權，無論是在網路立法、政策管理規範方面的難度亦變得更高。

網際網路自 1990 年代興起以來，其自由和無遠弗屆的連結方式提供全世界各種不同的種族、民族、國家之間的思想和文化交流的條件，而當 YouTube、Facebook、Instagram、Twitter、WhatsApp、LINE 等社交媒體逐漸成為人們生活的一部分，開放程度高、傳播速度快、影響範圍廣、滲透能力強等特點，改變長久以來接收外界訊息、閱讀（聽）習慣。網路話語權產生的網路滲透問題正隨著在資訊技術或網路環境掌有優勢的國家、團體能夠影響是非善惡的評價標準，透過實際或培植的政治領袖主導對特定事物、事件的界定權，甚至是對制度、規則的決定權，直接引導受眾或是改變社會主流意識。近年來發生在全世界的「顏色革命」(color revolution)運動，<sup>16</sup> 儘管參與者們皆是以反對現有政

---

<sup>16</sup> 2000 年後，包括有 2003 年喬治亞共和國「玫瑰革命」(Rose Revolution)、2004 年烏克蘭「橙色革命」(Orange Revolution)、2005 年伊拉克「紫色革命」(Purple Revolution)、吉爾吉斯「鬱金香革命」(Tulip Revolution)、2006 年白俄羅斯「牛仔褲革命」(Jeans Revolution)、2007 年緬甸「番紅花革命」(Saffron Revolution)、2009 年摩多瓦「葡萄革命」(Grape Revolution)、2010 年吉爾吉斯「甜瓜革命」(Melon Revolution)、2011 年突尼西亞「茉莉花革命」(Jasmine Revolution)、埃及「蓮花革命」(Lotus Revolution)、巴林「珍珠革命」(Pearl Revolution)、葉門「咖啡革命」(Coffee Revolution)、2011 至 2013 年俄羅斯「大雪革命」(Snow Revolution)、2016 年北馬其頓共和國「多彩革命」(Colorful Revolution)、2018 年亞美尼亞「絲絨革命」(Velvet Revolution)，這些運



權，以擁護自由民主和人權等普世價值為目標，惟在運動期間同時造成的社會失序和犯罪等危安事件，也確實成為國安、情報和執法部門難解的問題。

## 二、網路恐怖主義

恐怖主義最早源於 1793 年 9 月 5 日至 1794 年 7 月 28 日法國大革命的雅各賓派 (The Jacobins) 專政下的恐怖統治時期。後人則是將恐怖主義視為個人或團體從事極端活動和製造社會不安的代名詞。從個人掌權時的恐怖統治 (la Terreur) 到 1960 年代恐怖主義開始出現國際化、科技化和集團式的行為表現，再至 21 世紀初期以美國「九一一事件」後，隨著反恐戰爭發生在各國帶有特定政治意識形態、政治目的激進主張，網路恐怖主義已成為恐怖組織和恐怖份子慣用的運作方式。亦即恐怖份子不只使用網路做為訊息傳遞和串聯的聯繫媒介，其攻擊的目標亦已鎖定目標國家的關鍵基礎建設 (critical infrastructure)、關鍵資訊基礎建設 (critical information infrastructure)。舉凡以實體破壞、入侵攻擊、社交工程攻擊等利用讓資安防護機制失效的方式，造成包括：能源、水資源、通訊傳播、交通、銀行與金融、緊急救援與醫院、中央與地方政府機關、科學園區與工業區等八大領域停擺或大規模故障，<sup>17</sup> 成為「混合式威脅」的另一主要類型。

---

動的參與者在政黨團體或人士領導下，以社群媒體連繫、傳達訊息，持續數月至數年的抗爭，無論是否達到政治訴求，皆造成人員傷亡和國家政局動盪。

<sup>17</sup> 〈國家關鍵基礎設施領域分類〉，2018 年 7 月 30 日，《行政院國土安全政策會報》，<<https://ohs.ey.gov.tw/File/79A79307409FF32C>>（2019 年 10 月 15 日查詢）。

在實際案例方面，包括「伊斯蘭國」、「蓋達組織」(Qaeda)、「博科聖地組織」(Boko Haram)等極端主義運動，近年來在全世界發動規模大小不一的恐怖攻擊活動最為典型。恐怖組織或暴力激進團體利用資訊網路覆蓋全世界，以及和個人、公民社會、政府部門生活、工作相互依賴的特性，以便捷、隱密、高效的方式聯繫分布在世界各地的組織成員，對恐怖活動進行策劃、實施、指揮，進而讓反制預防的難度大幅增加。其次，在虛擬世界中集合了眾人智慧，透過網路科技能夠針對大量資訊進行快速的蒐集、處理和學習。恐怖組織設想各種攻擊手法，同樣毋須耗費高額成本，就能獲得即時、精準的所需訊息，進而能夠輕易地鎖定攻擊目標，製造社會和經濟秩序的恐慌和混亂，達到預設的訴求和政治目的。第三，恐怖組織透過網站架設招募、培訓成員、募集資金、美化和宣揚意識形態，並且利用文明衝突的弱點，增加敵我之間的對立和分化，鼓動支持者採取暴力手段群起反抗，由於其煽動性強，易對年輕族群產生感染共鳴效應，進而導致各國在防治手段上遭遇極大的阻礙。

以德國為例，其「聯邦憲法保衛局」(Bundesamt für Verfassungsschutz, BfV)局長哈爾登旺(Thomas Haldenwang)曾表示在德國境內潛在的「伊斯蘭國」份子約有 2,240 名，主要透過網路和數位化手段進行聯繫、散布極端思想或煽動支持者發動恐怖攻擊。<sup>18</sup>另據德國《星期日世界報》(Welt am Sonntag)報導，德

<sup>18</sup> “ISIS Can Still Launch Attacks, German Intelligence Chief Warns,” *The National*, April 14, 2019, available on: <<https://www.thenational.ae/world/europe/isis-can-still-launch-attacks-german-intelligence-chief-warns-1.848890>> (2019 年 10 月 15 日查詢)。



國政府已無法繼續追蹤 160 多名前往敘利亞、伊拉克兩國加入「伊斯蘭國」支持者的蹤跡。<sup>19</sup> 儘管當前「伊斯蘭國」勢力已遭到瓦解，惟德國安全部門仍須隨時防範流竄他國或返回德國者可能的攻擊。更重要的是，德國政府相當擔心過去支持「伊斯蘭國」民眾的下一代有可能已受到暴力行為影響，而有必要在特定情況下進行修法，對未成年者進行必要的監控，形成極大的安全隱憂。

### 三、網路心理戰、輿論戰、情報戰

除了恐怖組織、恐怖份子外，近年來利用輿論戰搶占特定議題的話語權、心理戰製造社會矛盾、政治分裂，以及情報戰取得攻擊致勝先機，亦成為在虛擬世界中新興的「混合式威脅」主要特點。尤其是以當前臺灣的安全威脅而論，中共就是利用對臺進行混合式威脅，靈活進行網路輿論心理攻勢以及網路情報工作之最佳案例。

首先，兩岸心理輿論攻防形勢主要仍以中共採取主動攻勢，爭取、影響臺灣民心的威脅最大；另一方面，儘管我國政府部門極力防阻，甚至針對特定議題進行反制，惟仍然難以阻擋中共對臺心理輿論攻勢，加上國內民意紛歧，導致在匡正視聽之外，影響效應有限。尤其在心理輿論攻勢方面，憑藉特定的傳播手段與方式，傳遞、表達軍事優勢與戰略決心。只要有運作空間，就可見中共藉此針對我國政治、經濟、軍事、社會等重要層面進行心

---

<sup>19</sup> “Germany Loses Track of 160 ‘Islamic State’ Supporters,” *DW Akademie*, June 23, 2019, available on: <<https://www.dw.com/en/germany-loses-track-of-160-islamic-state-supporters/a-49317535>> (2019 年 10 月 15 日查詢)。

理輿論影響。其中，中共利用我國民眾「相對剝奪感」(relative deprivation)之消極情緒，<sup>20</sup>大肆展現軍事實力、戰略意圖，拉攏國內傾中民意，並且製造與本土、傾美、傾日等多元政治意識之間的矛盾與衝突。中共認為心理輿論就像是合奏樂團，可區分為「主奏」與「和聲」兩類，並且強調在運用上不能「齊奏」，因此，採用央媒出擊、多軌管理、觀點引領、追兵群起的策略作法是近年來中共心理輿論攻勢手段之主要特色。<sup>21</sup> 中共利用傳播媒體不同的特性，以與中共官方具有密切關係的媒體為發布權威消息的主奏者，另配合其他主流媒體的聚焦、參與，形成綜合、廣泛的宣傳與討論氛圍，再加上各種非主流的媒體運用，在社會中引起話題、挑動各方見解差異之爭辯，進而達到心理輿論攻勢目標。

其次，在網路情報戰方面，可以此次中共軍改後中國人民解放軍成立的戰略支援部隊作為主要觀察的指標對象。其中，該部隊利用高科技增強對臺電子、電磁、電訊等信號情報的能力已獲得大幅提升。中共將過去分散於總參謀部、總政治部、總裝備部之科技情報單位或職能，統一納入戰略支援部隊，象徵裝備、人員、資源、能量的高度整合與運用，再加上和其他各軍種的協調運作（例如：海、空軍遠海長航訓練），不僅擴大信號情報偵收範圍，也表示中共有意將對臺和對國際間的情報工作推向更加高

<sup>20</sup> 是指某一群體的人口對於自己所處的情境，原本不認為有什麼問題存在，但是在與其他參照團體比較後，覺得自己的情況的確不如別人，與別人的情況存在顯著的差距，於是提出縮短差距具體要求所形成的情境。見吳定編，《公共政策辭典》（臺北市：五南圖書公司，2005），頁234。

<sup>21</sup> 蘇榮才，〈十八大以來官方輿論傳播的新變局〉，《南方電視學刊》，第4期，2013年8月，頁86。

科技的運用領域。此外，過去隸屬總政治部，負責進行心理、輿論和法律戰之 311 基地（61716 單位，駐地：福建福州）在改隸戰略支援部隊後，<sup>22</sup> 仍持續對臺實施心理戰和輿論戰。該基地的功能是運用廣播、電視等影音製作方式推動政治宣傳工作。例如：中國華藝廣播公司 (China Huayi Broadcasting Corporation, CHBC) 為 311 基地對外的掩護名稱，其電波主要覆蓋中國大陸大部分地區，以及臺灣、香港、澳門和東南亞地區、北美洲、大洋洲與歐洲部分地區。另一個同屬「一個機構兩塊牌子」的海峽之聲廣播電臺，同樣面向臺灣和海外進行廣播。

## 肆、國家安全的因應對策

當國家愈發展，對於安全要求的程度也就愈高。包括政治、經濟、軍事等攸關安全防護的層級、範圍、標準愈趨嚴密，才能保障國家得來不易的發展成果。20 世紀以來，人類基於兩次世界大規模戰爭以及數十次中、小規模戰爭的殘酷教訓，除了少數仍陷於族群、宗教、派系爭議而處於內戰狀態的國家外，絕大多數國家對於戰爭多半抱持謹慎、保守的態度。儘管當前世局仍然紛

---

<sup>22</sup> 2015 年 11 月，中共正式啟動「深化國防和軍隊改革」，其中，2015 年 12 月 31 日，成立中國人民解放軍陸軍領導機構、火箭軍、戰略支援部隊；2016 年 1 月 11 日，中共中央軍委會公布軍委機關部門調整方案，原軍委四總部（總參謀部、總政治部、總後勤部、總裝備部）改組為 15 個軍委直屬職能部門，包括總參謀部更名為聯合參謀部、總政治部更名為政治工作部、總裝備部更名為裝備發展部。見陳化水、申群喜編，《形勢與政策》（成都：電子科技大學出版社，2017），頁 123-124；〈梅華波少將調任戰略支援部隊某基地政委，原任空降兵學院政委〉，《澎湃》，2016 年 12 月 21 日，<[https://www.thepaper.cn/newsDetail\\_forward\\_1584288](https://www.thepaper.cn/newsDetail_forward_1584288)>（2019 年 10 月 15 日查詢）。

擾不安，惟各國基於確保國家安全、利益原則下投入國防軍事建設，用意多半反映在國力的綜合展現，並非藉興兵鑾戰攻城掠地。當國家之間的權益爭端尋求以非軍事手段作為解決問題的優先考量，瞭解國家面對敵情威脅與安全形勢，析察在虛擬世界中的「混合式威脅」，保持理性的國家行為和高度警覺，成為最終思考的重點。

### 一、教育面：批判性思考和教育訓練

虛擬世界中「混合式威脅」的主要來源是網路資訊，且和傳統媒體資訊在維繫社會公信力的基礎上具有一定的自律機制性質有所不同。因此，無論是利用網路滲透方式散播危害國家安全的假訊息，或是網路恐怖主義對實體設施安全和意識形態造成的損傷，抑或是特定攻擊採取之網路心理、輿論、情報攻勢，其防範的第一道防線就是透過適當的教育訓練方式和管道，提升網路資訊傳播者和受眾本身的自律機制和事實辨識能力。

根據 2014 年 6 月臺灣資訊工業策進會產業情報研究所公布「網路社群使用現況分析」報告，顯示高達 96.2% 的臺灣網友曾使用「社交網站」。<sup>23</sup> 時至 5 年後的今日，社群媒體已和大多數人的生活緊密相連，即時、迅速亦變成使用者的基本要求。因此，無論是訊息的真假，輿論風向的引導，往往因網路活動難以全面管控，致使在解決之道方面除了在法規方面尋求完備外，更應從教育面著手。以芬蘭為例，面對「數位野火」迅速傳播，虛假訊

<sup>23</sup> 〈96.2% 臺灣網友近期曾使用社交網站〉，《資策會產業情報研究所》，2014 年 6 月 13 日，〈[https://mic.iii.org.tw/IndustryObservations\\_PressRelease02.aspx?squo=364](https://mic.iii.org.tw/IndustryObservations_PressRelease02.aspx?squo=364)〉（2019 年 10 月 15 日查詢）。

息難以遏止，該國主張從學校和社會教育層面著手，不分年齡，強化國民、學生、記者、政治人物的數位能力 (digital capability) 和批判性思考能力 (critical thinking capability)，進而成功遏止假訊息在國內的傳播和傷害。<sup>24</sup>

其次，教育訓練更是政府國安情報單位不容忽視的重點。據相關報導顯示，利用網路做為情報通報管道，透過 Skype 與從事對臺情報工作人員聯繫亦曾有案例可循。<sup>25</sup> 在臺灣，國人喜好運用網路通訊軟體建立人際溝通模式，各式各樣的通訊軟體，交往平臺，已成為情報工作人員暗中傳遞情報資料，或是與工作對象進行聯繫之秘密管道。因此，不只要持續完善國家情報統合機制，更需要透過不同層級、反覆的教育訓練時機，讓各情報機關（構），以及國安、國防、社會治安等相關單位、部門能夠在交流互動平臺上，熟稔統合作法，將規定落實於實務工作中。

在教育訓練設計方面，主要區分法規、技術與實務三大部分。首先在法規教育方面，必須釐清我國情報機關遂行情報工作之所有法規依據，尤其側重於情報統合機制之法規或行政命令，使各級承辦人員能夠充分瞭解作業機制。其次，在技術訓練方面，可朝向建立國家安全情報資訊系統為構想，在國內各情治機關（構）統合機制運作下，以強化各級人員技術操作與運用為訓練重點。另考量情報作業首重安全、保密，因此在各機關的使用權限方面，

<sup>24</sup> 陳崢詒編譯，〈不只抓到了，還打贏了？芬蘭如何對抗假新聞之戰〉，《天下雜誌》，2019年5月27日，<<https://www.cw.com.tw/article/article.action?id=5095369>>（2019年10月15日查詢）。

<sup>25</sup> 〈經商掩護情報工作，4人判刑〉，《中央通訊社》，2017年6月25日，<<http://www.cna.com.tw/news/asoc/201706250159-1.aspx>>（2019年10月15日查詢）。

須有賴網管人員確實設計掌控，避免情資遭不當運用，衍生後遺。因此，其訓練方式雖較不具學理性，卻是教育過程中最為重要部分。第三，是要採取實際交流參訪互動方式，使各情治機關（構）瞭解情報工作現況與因應各種安全威脅所做的準備、需求，並且熟悉各單位之間作業模式，增進彼此互動與信任，相互借鏡，使統合機制得以深化。

## 二、危機管理：政策溝通和澄清機制

主要是指將公共危機管理方面強調的政府政策溝通和澄清機制，作為阻止假新聞、錯誤訊息、假訊息等「混合式威脅」常見態樣損害國家安全的第二道防線，必須減輕對國家和社會安全的衝擊。其中，有效的溝通和協調機制往往是危機能否「轉危為安」的關鍵，亦是遏阻網路滲透行為和網路輿論戰、心理戰攻勢的有效方式。主要包括政府與民眾、政府與新聞媒體、政府部門之間，以及民眾之間四大面向。必須建立制度化的資訊公開和發布制度，同時有效引導對民眾資訊傳播，防止各種政策消息的誤傳和謠言流傳。<sup>26</sup> 在實際的作法方面，除了必須重視跨層級、跨部會、跨社會部門的行動協調外，同時運用資訊網路做為危機管理的溝通和澄清手段亦為當前電子化政府、網路行政發展的趨勢。政府應用傳播媒介將即時、正確、最新的資訊向民眾傳達，透過網路傳播讓民眾建立對政府部門的正面認知，更可藉由大數據分析技術，掌握輿情動態，及時發現立場偏差、資訊錯誤等可能造成誤解等增加危機處理困擾的問題，<sup>27</sup> 進而有效管控「混合式威脅」

<sup>26</sup> 詹中原、朱愛群、李宗勳、鄭錫鎔，《政府危機管理》，頁 201。

<sup>27</sup> 詹中原、朱愛群、李宗勳、鄭錫鎔，《政府危機管理》，頁 252、265。



造成的危害。

政府部門為了能夠即時、準確傳達施政內容，建立可信賴的訊息發布源頭和傳播通路，我國行政院於 2018 年 6 月建置「即時新聞澄清專區」，各部會除了針對民眾誤解的訊息提出正確說明，針對重大政策不實的訊息或是網路流傳之假新聞，亦須即時因應處置。<sup>28</sup> 此外，行政院亦和在臺灣月活躍用戶超過 2,100 萬人的通訊軟體 LINE，合作成立「行政院澄清專區」，用戶可迅速檢視由政府各部會於第一時間澄清所有關於國安、民生、災防等重大訊息。<sup>29</sup> 其中，「LINE 訊息查證」官方帳號亦與「MyGoPen」、「CoFacts 真的假的」、「蘭姆酒吐司」、「臺灣事實查核中心」等國內 4 個單位合作打擊假新聞。<sup>30</sup> 有關假新聞、假消息對世界各國政經局勢和社會安定造成的危害，已成為政府相關部門極為重視的議題。因此，檢視世界上其他有名的通訊服務的業者（例如：Facebook、Google、Twitter），亦可發現分別採取不同的查證措施識別假新聞和轉發的訊息。<sup>31</sup> 可見，當各種真假訊息充斥

<sup>28</sup> 〈賴揆：政院建置新聞澄清專區，即時、精準澄清正確施政訊息〉，《行政院》，2018 年 5 月 10 日，<<https://www.ey.gov.tw/Page/9277F759E41CCD91/f33464e4-409a-4a81-9580-f05adcb1d742>>（2019 年 10 月 15 日查詢）。

<sup>29</sup> 黃筱晴，〈全球首發！「LINE 訊息查證」平台今上線，一個動作辨真偽〉，《聯合新聞網》，2019 年 7 月 22 日，<<https://udn.com/news/story/7266/3943382>>（2019 年 10 月 15 日查詢）。

<sup>30</sup> 楊又肇，〈協助打擊假新聞的 LINE 訊息查證上線，LINE 是如何做到的？〉，《聯合新聞網》，2019 年 7 月 22 日，<<https://udn.com/news/story/7086/3943236>>（2019 年 10 月 15 日查詢）。

<sup>31</sup> Jane Wambui Waweru Muigai, "Understanding Fake News," *International Journal of Scientific and Research Publications*, Vol. 9, No. 1 (January 2019), p. 29.

在虛擬世界，且影響日常生活中的每一個人，適時做好溝通與澄清的工作，成為公私部門合作的重點。

### 三、情報合作：跨部門領域構建國家安全網

防控「混合式威脅」的第三道防線，就是透過情報合作方式，建立跨領域的國家安全網。無論是國家安全情報機關或是執法治安單位，對於任何可能對國家或社會安全造成危害的危安情資必須依職權分工詳察評估。尤其「混合式威脅」來源涵蓋境外和國內的資訊網路，無論是欠缺正確網路使用觀念的網民、利用網路犯罪的犯罪份子，或是惡意攻擊、竊取機密資訊的網路駭客、敵對勢力，最終必須由代表政府公權力的國安情治單位依法查處。其中，有效掌握正確情報，強化政府部門間協調合作，提升相關安全部門防處能力，更是有效降低多數「混合式威脅」的關鍵。

以網路恐怖主義威脅為例，當前臺灣面臨的是國際現實的外交處境，尤其是當美國、日本成為國際打擊「伊斯蘭國」聯盟的主要國家，無論是出錢還是出力，臺灣在國際反恐的立場上只能做出支持的選擇，共同和其他 70 多個國家和國際組織發揮反恐聯盟作用。另一方面，在面對現階段潰散的「伊斯蘭國」成員改採獨狼或狼群式的攻擊手法，平時察覺不易，因此需要在國際間加強警察、特種作戰、外交、情報、資安等領域間的活動參與和交流合作。

再以 2019 年 4 月 21 日起，發生在斯里蘭卡造成該國民眾和印度、日本、美國、英國、中國大陸等多國外籍人員傷亡之連環爆炸恐怖攻擊事件為例，敲醒世界各國繼續在反恐議題方面的合作意願。除了成立跨部門聯合作戰中心，並和國際刑警、美國聯



邦調查局合作調查、防堵安全罅隙。<sup>32</sup>

鑒於當前國際恐怖組織、極端主義團體善於利用網路作為聯繫平臺，可見加入國際間在資訊網路安全的防範管控機制亦為重要突破口。以「伊斯蘭國」的網路週報《新聞》(al-Naba)為例，其刊登之文章就在告知聖戰士如何避免和敵人面對面衝突，並詳細指導他們發動游擊戰的方式，在避免遭受損失情況下削弱敵人。此外，恐怖組織或極端主義份子透過網路社群媒體作為聯繫管道，其在網路上留下的數位線索，更是追緝恐怖份子、避免恐怖攻擊事件發生最重要的依據。這些在虛擬世界的恐怖攻擊訊息，有賴強化資訊情報之蒐集、分析和即時通報。在防範作法方面，更須強化資安管控、阻斷，甚至制止網路恐怖主義攻擊。相關技術和人才的建置，皆須透過國際化的交流訓練與合作，可做為更進一步的思考。

從人道主義角度而論，我國政府部門仍應透過友盟在國際間發聲，支持臺灣建立和國際刑警組織之間的情報合作機制，抑或是採取低調作法，派員參與國際反恐和區域安全之活動、聯合訓練，強化實質性的安全情報訊息傳遞與分享。以近期「國際反恐和安全專業人士協會」(The International Association of Counterterrorism and Security Professionals, IACSP) 東南亞區域主任 Andrin Raj 指出，存在於印尼的「狼群式」恐怖攻擊手法，可

---

<sup>32</sup> “US Warns of More Attacks in Sri Lanka by Active Members of Terror Group Still at Large,” *The Economic Times*, April 30, 2019, available on: <<https://economictimes.indiatimes.com/news/international/world-news/us-warns-of-more-attacks-in-sri-lanka-by-active-members-of-terror-group-still-at-large/articleshow/69118536.cms?from=mdr>> (2019年10月15日查詢)。

透過 Telegram 即時通訊軟體告知另一「狼群」，在其他國家或區域發動攻擊。就算「狼群」之間沒有直接見面聯繫，仍然可以即時掌握每個「狼群」的動向。<sup>33</sup> 可見臺灣在國際反恐機制中，必須設法在公私部門領域加入相關組織，方能充分掌握國際反恐最新且正確之安全動態資訊，避免成為恐怖份子境管跳板或從事非法活動的漏洞。

## 伍、結論

資訊網路在帶給人類福祉的同時，同樣也顛覆了傳統的國家安全觀念。本文以「混合式威脅」在虛擬世界中快速增長為主要觀察，認為包括網路滲透、網路恐怖主義，以及網路心理戰、輿論戰、情報戰等種種態樣的轉變，已對傳統上認知的國家安全威脅來源、行為主體及其行為活動方式等方面產生重大影響，且成為各國政府掌理國家安全工作嚴峻的難題。2010 年 5 月，美國前總統歐巴馬 (Barack Obama) 執政期間曾公布《2010 年國家安全戰略報告》(National Security Strategy 2010)，內容即指出網路安全威脅是最嚴重的國家安全、公共安全和經濟挑戰之一。<sup>34</sup> 時至 2017 年 12 月，美國總統川普 (Donald Trump) 主政後，亦公布新的國家安全戰略，內容同樣提到當前網路空間已提供國家和非國

<sup>33</sup> “Wolf Packs a Common Trend in I.S.,” *New Straits Times*, May 15, 2019, available on: <<https://www.nst.com.my/news/crime-courts/2019/05/488526/wolf-packs-common-trend-counter-terrorism-expert>> (2019 年 10 月 15 日查詢)。

<sup>34</sup> U.S. White House, *National Security Strategy 2010*, May, 2010, available on: <[https://obamawhitehouse.archives.gov/sites/default/files/rss\\_viewer/national\\_security\\_strategy.pdf](https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/national_security_strategy.pdf)> (2019 年 10 月 15 日查詢)。

家行為者能夠在毋須際跨越國界的情況下，便可針對美國政治，經濟和安全利益發起反抗運動。網路攻擊為敵方提供低成本的良機，他們可以嚴重破壞美國關鍵基礎設施，削弱美國企業實力，侵害美國聯邦政府網路，並且攻擊美國人每日用於交流和推展工作的工具和設備。<sup>35</sup>

臺灣面臨的國家安全「混合式威脅」的程度並不亞於外國。其中，以中共對臺心理輿論攻勢為例，包括：宣傳、謀略、干擾、欺騙、嚇阻、恐嚇、情感等類型，皆是利用電子、網路方式達成其戰略意圖影響常見的手法。而檢視其攻勢之內涵，是以能夠達到自己有口不說，不需聲言令色，卻能造成製造對方內部紛亂。中共將輿論視為武器，裝載包括政治、軍事、外交、經濟等各種議題，掌握：先聲奪人，先入為主；集中造勢，形成強勢；抨擊要害，重點突破；滲透引導，爭取人心，以及因勢利導，趨利避害原則。<sup>36</sup> 此外，臺灣同樣面臨網路滲透嚴重影響國家安全的問題，除了有賴政府相關部門制定周延的法規外，更須思考教育紮根作法，透過課程設計、議題宣導，不僅要建立網路使用的正確態度，養成良好的資訊安全意識，更要訓練批判性思考能力，提升辨別假新聞和減少訊息「病毒式內容傳播」造成的負面影響。

世界之大，讓人可以從各種不同角度觀察各種事物。有人從金錢的角度認為這個世界是有財力之人的世界；有人從權力的角

<sup>35</sup> U.S. White House, *National Security Strategy of the United States of America*, December, 2017, available on: <<https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf>> (2019 年 10 月 15 日查詢)。

<sup>36</sup> 楊春長、盛和泰，《信息時代政治指導員工作》（北京市：長征出版社，2006），頁 310。

度認為這個世界是有權勢之人的世界。若從國家安全的角度而論，這個世界應是有人心機之人的世界。其中，作為安全維護者，須以國家和眾人生存的安全利益為優先考量；反之，作為破壞者則是處心積慮找尋國家制度的弱點、民心輿論的缺口趁虛而入。因此，在良善和變惡之間，不可諱言的是在執法正義和公理所須審慎因應的人權自由問題。尤其當虛擬世界中的「混合式威脅」朝向現實世界進擊，其防禦和反制的安全機制成為常態化的管控重點，而包括限制和糾舉作法容易觸及到一般守法民眾的言論自由、秘密通訊自由、集會及結社自由，以及請願、訴願權利等基本人權而引起爭議。然而，從我國憲法和國安角度而論，民眾的自由及權利必須不妨害社會秩序公共利益，政府部門則是為了避免國家緊急危難、維持社會秩序，增進公共利益而須制定適當的法律規範。因此，為了能夠均衡法律、公共政策和民眾權益之間的關係，更應著重充分的政府政策溝通和公民教育。「混合式威脅」對國家安全帶來新挑戰，政府和全民之間建立合作共識以及協調運作機制則是有效因應的關鍵，實不容忽視。

(收稿：2019 年 12 月 12 日；第一次修正：2020 年 3 月 30 日；  
接受：2020 年 7 月 14 日)

## 參考文獻

### 一、中文部分

#### (一) 期刊論文

蘇榮才，2013/08。〈十八大以來官方輿論傳播的新變局〉，《南方電視學刊》，第4期，頁86-87。

#### (二) 專書

吳定編，2005。《公共政策辭典》。臺北市：五南圖書公司。

張永理編，2015。《公共危機管理》。武漢：武漢大學出版社。

陳化水、申群喜編，2017。《形勢與政策》。成都：電子科技大學出版社。

楊春長、盛和泰，2006。《信息時代政治指導員工作》。北京市：長征出版社。

詹中原、朱愛群、李宗勳、鄭錫鍇，2006。《政府危機管理》。臺北市：國立空中大學。

#### (三) 網際網路

不著撰人，2014/06/13。〈96.2% 臺灣網友近期曾使用社交網站〉，《資策會產業情報研究所》，<[https://mic.iii.org.tw/IndustryObservations\\_PressRelease02.aspx?sqno=364](https://mic.iii.org.tw/IndustryObservations_PressRelease02.aspx?sqno=364)>。

不著撰人，2016/12/21。〈梅華波少將調任戰略支援部隊某基地政委，原任空降兵學院政委〉，《澎湃》，<[https://www.thepaper.cn/newsDetail\\_forward\\_1584288](https://www.thepaper.cn/newsDetail_forward_1584288)>。

不著撰人，2017/06/25。〈經商掩護情報工作，4 人判刑〉，《中央通訊社》，<<http://www.cna.com.tw/news/asoc/201706250159-1.aspx>>。

不著撰人，2018/05/10。〈賴揆：政院建置新聞澄清專區，即時、精準澄清正確施政訊息〉，《行政院》，<<https://www.ey.gov.tw/Page/9277F759E41CCD91/f33464e4-409a-4a81-9580-f05adcb1d742>>。

不著撰人，2018/07/30。〈國家關鍵基礎設施領域分類〉，《行政院國土安全政策會報》，<<https://ohs.ey.gov.tw/File/79A79307409FF32C>>。

陳埤詒編譯，2019 年 5 月 27 日。〈不只抓到了，還打贏了？芬蘭如何對抗假新聞之戰〉，《天下雜誌》，<<https://www.cw.com.tw/article/article.action?id=5095369>>。

黃筱晴，2019/07/22。〈全球首發！「LINE 訊息查證」平台今上線，一個動作辨真偽〉，《聯合新聞網》，<<https://udn.com/news/story/7266/3943382>>。

楊又肇，2019/07/22。〈協助打擊假新聞的 LINE 訊息查證上線，LINE 是如何做到的？〉，《聯合新聞網》，<<https://udn.com/news/story/7086/3943236>>。

## 二、外文部分

### （一）期刊論文

Muigai, Jane Wambui Waweru, 2019/01. “Understanding Fake News,” *International Journal of Scientific and Research Pub-*

lications, Vol. 9, No. 1, pp. 29-38.

## (二) 專書

Hillyard, Michael J., 2000. *Public Crisis Management: How and Why Organizations Work Together to Solve Society's Most Threatening Problems*. Bloomington, IN: iUniverse.

Hoffman, Frank G., 2007. *Conflict in the 21st Century: The Rise of Hybrid Wars*. Arlington, VA: Potomac Institute for Policy Studies.

Josselin, Daphné and William Wallace, 2001. "Non-state Actors in World Politics: A Framework," in Daphné Josselin and William Wallace eds., *Non-state Actors in World Politics*. London: Palgrave Macmillan. pp. 1-20.

Kosseff, Jeff, 2019. *Cybersecurity Law*. Hoboken, N.J.: John Wiley & Sons.

Schmitt, Michael N. ed., 2017. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. London: Cambridge University Press.

## (三) 網際網路

Anonymous, 2019/04/14. "ISIS Can Still Launch Attacks, German Intelligence Chief Warns," *The National*, available on: <<https://www.thenational.ae/world/europe/isis-can-still-launch-attacks-german-intelligence-chief-warns-1.848890>>.

Anonymous, 2019/04/30. "US Warns of More Attacks in Sri Lanka by Active Members of Terror Group Still at Large," *The Economic Times*, available on: <<https://economictimes.india->

times.com/news/international/world-news/us-warns-of-more-attacks-in-sri-lanka-by-active-members-of-terror-group-still-at-large/articleshow/69118536.cms?from=mdr>.

Anonymous, 2019/05/15. “Wolf Packs a Common Trend in I.S.,” *New Straits Times*, available on: <<https://www.nst.com.my/news/crime-courts/2019/05/488526/wolf-packs-common-trend-counter-terrorism-expert>>.

Anonymous, 2019/06/23. “Germany Loses Track of 160 ‘Islamic State’ Supporters,” *DW Akademie*, available on: <<https://www.dw.com/en/germany-loses-track-of-160-islamic-state-supporters/a-49317535>>.

European Commission, 2019/05/28. *Report on the Implementation of the 2016 Joint Framework on Countering Hybrid Threats and the 2018 Joint Communication on Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats*, available on: <[https://eeas.europa.eu/sites/eeas/files/report\\_on\\_the\\_implementation\\_of\\_the\\_2016\\_joint\\_framework\\_on\\_countering\\_hybrid\\_threats\\_and\\_the\\_2018\\_joint\\_communication\\_on\\_increasing\\_resilien.pdf](https://eeas.europa.eu/sites/eeas/files/report_on_the_implementation_of_the_2016_joint_framework_on_countering_hybrid_threats_and_the_2018_joint_communication_on_increasing_resilien.pdf)>.

European Union Global Strategy, 2016/06. “Shared Vision, Common Action: A Stronger Europe a Global Strategy for the European Union’s Foreign And Security Policy,” *European Union*, available on: <[http://eeas.europa.eu/archives/docs/top\\_stories/pdf/eugs\\_review\\_web.pdf](http://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf)>.

Fidler, Stephen, 2016/01/04. “A Perilous Year for European Unity,” *The Wall Street Journal*, available on: <<https://www.wsj.com/articles/a-perilous-year-for-european-unity-1451817767>>.



- Giannopoulos, Georgios, 2017/09/07. "Introduction to the concept of Hybrid Threats," *European Energy - Information Sharing & Analysis Centre*, available on: <<https://www.ee-isac.eu/hybrid-threats>>.
- Rukomeda, Roman, 2018/09/28. "Russia's Hybrid War Against Ukraine: The Latest Developments and Trends," *Centre for Integrity in the Defence Sector*, available on: <<https://cids.no/2018/09/28/russias-hybrid-war-against-ukraine-the-latest-developments-and-trends/>>.
- U.S. Department of Defense, 2005/03. *National Defense Strategy*, available on: <<https://www.hsdl.org/?view&did=452255>>.
- U.S. Department of Defense, 2006/02/06. *Quadrennial Defense Review Report*, available on: <<https://archive.defense.gov/pubs/pdfs/QDR20060203.pdf>>.
- U.S. Department of Defense, 2010/02/01. *Quadrennial Defense Review Report*, available on: <[https://dod.defense.gov/Portals/1/features/defenseReviews/QDR/QDR\\_as\\_of\\_29JAN10\\_1600.pdf](https://dod.defense.gov/Portals/1/features/defenseReviews/QDR/QDR_as_of_29JAN10_1600.pdf)>.
- U.S. Department of Defense, 2018/01. *National Defense Strategy*, available on: <<https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf>>.
- U.S. Joint Chiefs of Staff, 2015/06. *The National Military Strategy of the United States of America 2015*, available on: <[https://www.jcs.mil/Portals/36/Documents/Publications/2015\\_National\\_Military\\_Strategy.pdf](https://www.jcs.mil/Portals/36/Documents/Publications/2015_National_Military_Strategy.pdf)>.
- U.S. White House, 2010/05. *National Security Strategy 2010*, available on: <<https://obamawhitehouse.archives.gov/sites/default/>>

files/rss\_viewer/national\_security\_strategy.pdf>.

U.S. White House, 2017/12. *National Security Strategy of the United States of America*, available on: <<https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf>>.