DOI:10.6915/PMSS.202108_(19).0003
軍事社會科學專刊，第 19 期，頁 7-32 (2021 年 8 月)

我國面臨新型態混合式威脅下軍事情報工作之展望

汪毓瑋*

摘要

混合威脅不容易說清楚，但似乎又是真實存在的，有些時候似乎又呈現出政治作戰之外貌。處理威脅，不能僅從表象上之現況著手，而必須及於整個安全層面之檢討。安全在本質上是被動的，要能夠具有主動性，就必須有情報來支撐。而情報的學理與實踐在「九・一一事件」後就已進行大幅改革，其目的就在於對不斷演化、不易掌握的威脅及有敵意行為者的多樣組合進行有效的回應。相對於臺灣之情報圈，合併了反情報之情報工作並不完整，想要處理混合威脅之軍事情報工作必須有新的思維、目標與工作對象。更重要的是，作為政治作戰領域一環之情報戰，必須補強反情報之內涵，才能完善軍事情報工作。

關鍵詞：混合威脅、軍事情報工作、政治作戰、戰略反情報

* 中央警察大學國境警察學系教授兼任恐怖主義研究中心主任，國立政治大學國發所博士，電子信箱：una254@mail.cpu.edu.tw

DOI:10.6915/PMSS.202108_(19).0003
Publication of Military Social Science, No.19, pp.7-32 (August, 2021)

Prospects for Taiwan's Military Intelligence Work under the New Type of Hybrid Threat

Wang Yuhwoei*

Abstract

Hybrid threats are not easy to clarify, but they seem to be real, and sometimes they appear to be political warfare. Dealing with threats must not only start from the present situation on the surface, but must go to the review of the entire security level. Security is passive in nature. To be proactive, it must be supported by intelligence. The theory and practice of intelligence have undergone substantial reforms after the "September 11 Incident", with the purpose of effectively responding to the constantly evolving threats that are difficult to grasp and the diverse combinations of hostile actors. Compared with Taiwan's intelligence community, intelligence work that incorporates counterintelligence is not complete. Future military intelligence work that wants to deal with hybrid threats must have new thinking, targets, and work object. More importantly, as an intelligence warfare in the field of political warfare, the connotation of counterintelligence must be strengthened in order to improve military intelligence affairs.

Keywords: Hybrid Threats, Military intelligence Work, Political warfare, Strategic Counterintelligence

* Professor, Department of Border Police, Central Police University; & Chair, Terrorism Research Center, Central Police University; Ph.D., Graduate Institute of Development Studies, National Chengchi University; Mail: una254@mail.cpu.edu.tw

壹、前言

情報學是一門專業及綜合性的學術領域，而其實踐又存於隱蔽之國家及國際戰場，其重要性及困難度實不言而喻。情報之需求及多樣化之產品，是一方面源於國家安全與發展的需求；另方面又要嚴防「他方」對我之破壞與誤導。因此，從國家安全思考，此等領域之研究與實踐要不斷的深化、外展與精進。

安全的感受是來自於威脅，混合威脅是源於美國及歐洲國家對於俄羅斯演化中威脅的形容，並舉出多個案例來論證；但是相對於俄羅斯所言，混合威脅才正是西方侵蝕與顛覆不同於其民主政體之途徑，亦舉例反證美歐國家對其與中共之此等作為。但對於混合威脅及其接續引發之混合衝突與混合戰爭之光譜系列之進程，似又與傳統軍事作戰外之政治作戰有其雷同之處。因此，本文首先分析混合威脅與政治作戰，也希望藉此喚醒我傳統政治作戰重要性之目的。

為了有效應對不斷演化中的威脅，因此作為維護國家安全最重要之情報工具，不論在理論與實踐上已進行不斷的檢討。特別是在美國「九・一一事件」後，學界已對於傳統情報理論進行了大量之論辯與批判；美歐等先進國家甚至中共等國也均從情報體制、法制與運作上進行實踐上之變革，而似引發了所謂「情報事務革命」之實，而為本文分析的第二個部分。針對混合威脅與情報改革分析之論述，導引出本文的第三個部分，就是從大家比較熟知的四項重大危害來論證對於情報運用之影響，特別是新的情報類型與實踐途徑之反思，可藉以引發若是結合此四項危害之混合威脅發生，則情報是否可以提供預警。最後一個部分，則是結合我國現行作為而論證與聚焦軍事情報應有之改善方向；並與第一部分之我國政治作戰相呼應，盼能補強進而指導欠缺之情報理論與實踐。

貳、混合威脅與政治作戰

一、認知安全

「安全」是任何國家常掛在口邊的「話語」，是依於有關法律之當下的「危難」或是「緊急狀態」時，必須依於「非常規」行政手段處理之暫時「現象」。換言之，不會是時刻每日提及的某個「長期」的有企圖之「政治運用」，因為後遺症是「單」方面改變「遊戲規則」且會造成直接或間接或長或短的「對等」回應並總會秧及無辜。而在設計企求「政治利得」時，也常可能會「壓制」人民。因為它涉及的範圍不僅是政、軍、經、心等「國家」政策，更深化於「市民社

會」而及於人民生活的方方面面，才能求得「認同」與支持。但是目前常態化聽到之安全卻已是每日必要之「話術」，它的因果又經常是「常識推論」的想當然耳，因為經常它的「取信」是基於現實案例再加上誇大「想像」之「預防性」而非論證的「證據」驗證，但會藉「情報」來源再輔之「宣傳」則效果大增。這種現象特別是美國川普及接續的拜登政府不斷的攻擊中共可見一斑。

若嘗試從學術上詮釋「話語」，它或許可以稱之為「名詞」，若是再更精確一點，它就是一個引導行動的「概念」，也是哲學脈絡下「方法論」上的最基本去觀察「現象」及進而嘗試「說明」的一個必須釐清的起點。但是到底應該如何去「定義」安全？若努力檢視任何中、外有關安全之相關教科書、或是自詡專家與學者之不同觀點，甚或是政府官員、民意代表、媒體、網民之說法，則是豐富多樣、自我「合理化」、且「各自堅持」，但這個真的是安全嗎？它又到底是怎麼來的呢？這種感知又能夠持續多長？且又真的能夠取得大多數民眾的認同嗎？

「安全」的起點定義，或許可以認知為：「客觀上不存在威脅、主觀上不存在恐懼之交互感覺過程」。且它的指涉客體不一定要與「國家」有關，但必然是與人類的「集體性」有關才能夠取得共鳴，自然也不應該僅是聚焦於軍事能力之限制與否，舉凡影響人類生存與解放的自然環境變化、重大傳染性病、恐怖主義等議題均可能是被關注的議題。也因此安全的指涉，通常是伴隨著新事件或新威脅的出現而產生變化。而若從「辯證邏輯」角度思考，此種從個別主體的主觀認知，上升到主體間的共有認知，再上升到社會的普遍認同，就彰顯出安全問題就是一種「社會建構」的過程，而且具有較大權力者或強勢話術者就具有主導的優勢地位(余瀟楓、王江麗，2006；Buzan, Wæver, Wæver, & De Wilde, 1998; Terriff, Croft, James, & Morgan, 2000)。且在此演進過程中就涉及了「非政治性」、「政治性」、「安全性」三類事物之進程判斷(Collins, 2016)，而安全就被視為是一種極端的政治化，可以是由國家也可能是由非國家行為者發起，並使用「安全的語言」來進行說服(Buzan & Herring, 1998)。若從兼具「唯心」或「唯物」之論爭並加以融合，整體上涉及了努力緩和威脅以保有型塑之價值。並透過有意識的努力，而能以一種可欲的方法達成安全(汪毓瑋，2021)。

二、混合威脅

根據北約型塑「拱頂石概念」(Capstone Concept)所描述之「混合威脅」(Hybrid Threats)，就是「對手」已有能力同時採用「常規」(Conventional)和「非

常規」(Non-conventional)的手段進行威脅以達成自己目標(Supreme Allied Commander Europe & Supreme Allied Commander Transformation, 2010)。而在無法鑑定特定國家危害下，這個定義承認了對手的「模糊性」，以及威脅本身的傳統和非傳統的「同時發生」和「結合」的本質。2011 年 5 月，「北約盟軍轉型司令部」(NATO Allied Command Transformation)基於情節結合專家學者與實務單位進行「反制混合威脅」(Countering Hybrid Threats)實驗，[1]以驗證新的《北約戰略概念》(NATO Strategic Concept)中兩個關鍵概念的可行性：一是「混合威脅」；另一就是演變為有效應對混合威脅的屬於多層面本質概念之「全面性途徑」(Comprehensive Approach)，並要求應用外交、軍事、情報、經濟等全面、集體資源以促進協作。2010 年 11 月，北約重申新的「戰略概念」，強調要防範極端主義、恐怖主義和跨國的非法活動，例如販運武器、麻醉品和人員，網路攻擊和其他技術和環境等獨立因素融合及編織一起的新的和不同性質威脅(Aaronson, Diessen, De Kermabon, Long, & Miklaucic, 2011)。

美國海軍陸戰隊更早發展「混合威脅」概念，並見之於 2006 年及 2010 年《四年期國防檢討報告》中。這個概念源於歷史分析和參考了外國學界關於有意混合和模糊「作戰模式」(Modes of Warfare)之思考。因此，使用這個術語來描述衝突的複雜和不斷演化的特質(Hoffman, 2014)。隨後 2010 年 2 月，國土安全部公佈的《四年期國土安全檢討報告》中，再度提醒必須關注此威脅的演化趨勢(汪毓瑋，2021)。若進行美國國防部和相關學術文件的分析，混合作戰在整個衝突範圍內，混雜了常規(Conventional)和非正規作戰(Irregular Warfare)的途徑。例如 2011 年，美國陸軍指出「混合威脅」就是「常規」、非正規、恐怖主義和犯罪能力的多樣化和動態組合，或這些部隊和各種因素的組合以實現互利效果。而美軍聯合作戰司令部則將「混合威脅」定義為：對手在任何時候同時發起的、並在戰役作戰空間中適應性地採用常規、非正規、恐怖主義和犯罪手段或活動的量身定做的混合。並不斷抨擊俄羅斯與中共所造成的此等威脅，以及發動的「混合作戰」(Hybrid Warfare)，且定調是破壞民主國家和民主體制發展的隱晦手段(Department of Defense, USA, 2007, 2009, 2010; Joint Forces Command, USA, 2010)。

除了「混合」的術語之外，美國國防部亦採用了「全光譜系戰役」(Full

[1] 2003 年北約改革時，歐洲盟軍司令部除了在蒙斯的行動指揮部外，位於葡萄牙里斯本原本隸屬於大西洋盟軍司令部的行動指揮部也被劃分給了新的盟軍作戰司令部。而大西洋盟軍司令部的剩餘部分，則在重組後成為了盟軍轉型司令部(Allied Command Transformation)。

Spectrum Operations)一詞來代替「混合」術語。例如在《第 3-0 號陸軍野戰手冊-戰役》(Army Field Manual No. 3-0, Operations)中，就將「全光譜系戰役」定義為一種「戰役概念」(Operational Concept)，部隊結合了攻擊、防禦和穩定或民事支援作戰而作為相互依賴的聯合部隊的一部分，抓住、保留和利用創意，接受謹慎的風險，以創造取得決定性成果機會。2010 年《陸軍姿態聲明》(2010 Army Posture Statement)除了使用混合威脅外、還使用「全光譜系戰役」描述當前和未來的軍事行動(Department of the Army, USA, 2008)。均顯示「混合威脅」之不同說明的嘗試。

但俄羅斯卻認為不論是「混合威脅」或是「混合衝突」(Hybrid Conflicts)或是「混合戰爭」(Hybrid War)，這些名詞實際上都是西方故意「曲解」或是「甩鍋」給俄羅斯的。其總參謀長格拉西莫夫(Valeri Vasilyevitch Gerasimov)將軍曾經指出：在 21 世紀的戰爭與和平界限已較以往更趨於模糊，戰爭已經不再宣布就開始了，而且是根據與以往完全不同的、且傳統上並不熟悉的戰略模板(Template)，透過混合之與時俱進的戰術設計來實踐的。並警告要注意來自「西方工具箱」的間接攻擊，及蠶食不同體制與文化國家之「舒適領域」與影響既有或固有領土的間接和非對稱性方法，例如「顏色革命」之分階段政權轉變，透過政權調整等破壞、控制或影響國家及跨國性相互連接關鍵基礎設施項目，包含網路空間的資訊流動等。且這些非軍事手段，包括虛假旗幟行動，例如支持反叛分子使用化學武器卻歸咎於敘利亞政府，經濟制裁和強迫政權更迭。不斷侵蝕俄羅斯勢力範圍、反對中國大陸「一帶一路」戰略倡議等。而俄羅斯的「間接和非對稱性方法」就被西方詮釋發展成「混合戰爭」的概念(汪毓瑋，2018a)。

雖然從 2006 年以來，「混合威脅」、「混合衝突」、或是「混合戰爭」等之名詞不斷被美歐官方與學者提及並各自賦予其定義，且不斷有相關反制「實踐」；而常與此等名詞混用的亦有「灰色地帶」(Gray Area)的說詞與對類似事件的形容等不勝枚舉，尤其是美國的智庫且政府樂於配合宣傳，但是迄今仍然沒有一個共同接受的內容。既使美國國防部內部各軍種單位，對於此等定義也不一致。而綜整目前西方國家已是基於保護的民主價值與意識型態、主宰不容挑戰的國際規範、或基於安全環境動變現實，大概均是根據上下文義而引用這些名詞，特別是當不易歸類，無法提出明確證據，但隱含威脅或危害的斷言，且基於必須型塑之安全感，這些名詞就常掛在口邊(汪毓瑋，2018b)。有趣的是，近期自俄羅斯總統

盧卡申科(Alexander Lukashenko)為迫使一架飛往立陶宛的客機改降落在明斯克之辯解，也指責西方國家發動了「混合戰爭」(Hybrid War)以「扼殺」他們(自由時報，2021)。

雖然西方政府部門、智庫與學者專家之定義分歧，但進而分析與排比這些定義，似仍可以概定其內容：混合威脅通常運作於低於戰爭界限之灰色地帶，是發生在整個衝突頻譜中的每一個「區間」，而不是頻譜上獨立的衝突類型。可以被定義為：「模糊性」的國家或是非國家行為者，不受以往遠近「地理」或主權「疆界」概念的限制，而「同時」在不同的戰場與市民社會之含實體與虛擬的多樣化「空間」中，混合採用了「單方面」或是結合「可調適」和「系統性」之「量身定製」的傳統武器、非常規戰術、恐怖主義和犯罪行為等之既「不易歸類屬性」、又能夠悠遊於合法與非法之「灰色地帶」的隱而不顯作為，以追求具有更大算計之政治目標。因此，可能包括了經濟和金融行為在內的合理施壓或是制裁手段，包括創造或隱蔽的利用貿易聯盟；顛覆性的政治作為；透過情報與反叛組織的隱蔽行動；利用非政府組織；訴求人道主義援助；運用社會壓力；施展恐怖攻擊；誘發犯罪與失序；或是使用虛假網站和植入錯誤資訊(汪毓瑋，2020a)。

三、政治作戰

2014 年 3 月之克里米亞之危機顯示，涉及了分裂主義者、俄羅斯超民族主義者、代理戰士以及俄羅斯「總參謀部情報局」人員等在內，已經不再適合西方類型的「戰爭」認知(汪毓瑋，2018b)。且在某種意義上，兩國的衝突更像是一場內戰，也像是一場代理戰爭(Proxy War)。目前的準則(Doctrine)試圖將這兩個國家的衝突分為常規和非正規作戰的兩個框架。也有學者將此系列的行動，就稱之為「政治作戰」(Political Warfare)，使用這個名詞來描述歸於「戰爭」(War)知識架構之外的不明確和模糊的衝突(Nebulous Conflicts)，且在此過程中，涉及了必須贏得民心、且要整合秘密行動(Covert Actions)以針對重要的外國機構介入；或是涉及了減少暴力作為和最大化國家影響力的手段等之思考與實踐。

在一般定義思考，政治作戰是在一個國家的指揮下，為了實現其國家目標而採取的一切手段。這些戰役(Operations)是公開(Overt)和秘密(Covert)同時進行的。其範圍是從政治聯盟、經濟措施和「白色」宣傳等之秘密運作(Covert Operations)到隱蔽(Clandestine)支持「友好」(Friendly)的外國因素、進行「黑色心理作戰」(Black Psychological Warfare)，甚至於是鼓勵或以有用資源暗助敵對國家的地下抵

抗運動(Kennan, 1948)。但是若戰爭的自身目的本來就是政治性的，則與政治作戰的內涵又有什麼不同呢？其次，對於軍事學者而言，「作戰」(Warfare)這個詞是描述解決戰爭的實體行為(Physical Conduct)，或是戰爭的戰鬥(Fighting)和暴力(Violent)方面。但是這些沒有暴力或致命武力的「政治活動」，有利「秘密運作」的「白色」宣傳，作為對於「友好」外國要素之隱蔽支援；「黑色」心理作戰，甚至鼓勵在敵對國家進行地下抵抗運動等等作為或是運作，不也是我們所熟知的政治作戰在政治與經濟領域中的活動嗎？這就是為什麼混合戰爭與政治作戰這兩個名詞內涵並非完全矛盾與牴觸的原因。

亦有給予「政治作戰」最廣泛的定義，指的是：在一個國家指揮下，使用所有不及於戰爭的手段，以實現其國家目標。但是「所有手段」的使用，已將定義擴展到超出政治或外交部分之外。其次，這種作戰模式只限於「不及於戰爭」的脈絡，但如果是不到戰爭的程度，那麼就不是戰爭了，也難以現有規範與措施應對，因此這也和常態下「混合威脅」之運用雷同。此外，「政治作戰」列出的清單只是不及於戰爭嗎？實際上也並不是那麼的清楚，這又涉及「混合作戰」之模糊邊界。此外，當戰爭正式開始時，這些所謂的許多活動，例如宣傳、制裁、顛覆等都不會停止且是內化於戰爭間的，因此不易切割是什麼時候「開始」的，檢證 2013 年美國入侵伊拉克就是如此。所以相較於政治作戰，混合戰爭這個術語或許不利於常態的理解，且似乎也不符合傳統之作戰邏輯(汪毓瑋，2018b)。

1957 年起，我國政治作戰就有所謂「六種作戰方式」，分別是心理戰、思想戰、情報戰、組織戰、群眾戰與謀略戰，且延用至今。然而從美、歐先進國家甚至中共之「戰爭」與「作戰」學理與教戰守則之檢討等以觀，均已與時俱進的發展。而若僅是「概述」中共為例，早就把政治作戰的內涵深化及外延為法律戰、輿論戰與心理戰，且不斷實踐及熟練運用於「國際社會陣線」，不僅因此在國際上依法的有憑有據進行其合理行動，且不斷爭奪「國際話語權」，而不僅限於軍事並且轉而為「國家戰略」服務；又除了體制上原有之公安與國安系統外，政戰體系的情報戰與謀略戰一部分併入戰略支援部隊；組織戰與群眾戰則聯接並深根到最底層之「街道辦事處」、「村兩會」，且調動大學生、各行業志願者到第一線擔任書記而直接掌控等，並透過「調研」掌握問題與民心，這些都是日常運作且是軍民協作而非只能「軍管軍」、「民管民」而已。因此，我政戰的所謂六種作戰方式之「方式」的定位框架狹窄，很容易聯想只是「技巧」或「戰術」層次，不

僅沒有知識累積之效，也可能只是步驟的遵循卻無法「創新」，而更嚴重的是自我侷限於政戰兵科卻不為其它兵科所完全認同進而給予更多支持，結果就是沒有國人重視，也沒有更多學者願意投入研究。或許應該更努力的正名為六大作戰「領域」，才可能及於國家安全之戰略層次並漸進內化於國土安全之關鍵基礎設施防護的不同領域，換言之，平時整個國家「工具箱」就應運行政治作戰，而到危機或戰時之作戰階段，實際上因為早已「先行」而奠基成功的必然條件，這也是前述混合作戰與政治作戰分際模糊的論辯焦點。

參、國家情報之改革趨勢

一、情報學理與實踐之論辯

「情報」源於「資訊」與「資料」，傳統的情報概念認為，資訊應該針對於來源和方法進行組織，且依法而基於嚴格的國內與國外區別去執行，亦即「情報」與「反情報」有其不同之任務重點與限制。但是美國 2004 年的《情報改革與恐怖主義預防法》(Intelligence Reform and Terrorism Prevention Act)則重新定義了「國家情報」(National Intelligence)，試圖超越以往舊的情報概念，而更是強調及時性(Timeliness)和準確性(Accuracy)，且呼籲在實踐上，應該是圍繞於議題(Issues)或問題(Problems)去組織情報，而不再只是針對資訊的來源(Sources)和出處(Provenance)去組織。亦強調政府內外資訊分享的重要性，且應檢討以往機密(Secrecy)概念之「有用性」。該法的變化程度，也導致學術與實務界開始重新思考及論辯情報圈(Intelligence Community)是否終於要啟動「情報事務革命」(Revolution in Intelligence Affairs)以因應新威脅。

學理上之檢討，已分別從情報的定義，探索理論之歷史方面、數學方面和心理方面，「反事實思考」(Counterfactual Thinking)之現實需求，討論了情報到底應該做什麼？情報理論到底是要解釋「是什麼」(What Is)？抑或只是要描述「應該是什麼」(What Ought To Be)等以往不認為是問題的問題？且情報理論也需要審思情報循環、反情報、秘密行動和問責制之執行與成效。且不能一直痴迷於資料(Data)，卻犧牲了判斷力(Judgment)，避免將神秘(Mysteries)變成拼圖(Puzzles)的誘惑(Treverton, 2003)，亦要求情報必須關切的中心問題，就是如何平衡的思考資料和技術的主導地位、情報與政策分離的路線、獨特的情報官僚和民主、軍事與政治目的情報間的衝突，以及對情報圈創造性思維能力的限制。

實踐上，情報的哪些假設是有用的，又有哪些應該被推翻？情報在本質上究竟是一個國家主權或是國家企業(National Enterprise)而只為國家的高層服務，還是也應該為其他有需求的消費者服務？情報僅能是「關於」這個數位時代的秘密資訊(Secret Information)和/或秘密活動(Secret Activities)嗎？且真的存有一個接續的情報「循環」(Cycle)，還是在「蒐集」、「分析」和「分發」之間的界限是如此模糊，以至於需要一個新的模型(Model)？是基於消費者的需求還是資訊層級？假如情報與任何其他資訊之間有所區隔，則什麼樣的資訊才是對於決策者是有用的？是否應該有一個情報消費者或是資訊的「等級制度」(Hierarchies)？情報圈受到不同蒐集部分如何管理的影響所造成的不良後果有那一些，且是否可以解決？可以有來自「情報測量」的結果嗎？測量行動與戰術情報之指標(Metrics)可以發展出來嗎？因此，可以有新的「情報典範」（Intelligence Paradigm）嗎？

雖然「人員情報」等傳統之五種情報來源主要鎖定國家行為者之「軍事」發展，仍然是發展傳統基於國家應對威脅所必要的，但是基於「混合威脅」等新的威脅本質與行為者不同之演化與「灰色地帶」空間之運用，為了更有效因應發展所謂新的「情報典範」可能已是必然的，但問題是要如何結合「傳統典範」使之成為一個可以適應動變威脅的新典範？其中包括不再是想要解決不完整(Incomplete)的「拼圖」，而是想要如何可以產生更具有說服力的「調適性詮釋」(Adaptive Interpretations)，而此涉及了去除想要建構所有複雜的拼圖，因為既不要涉及秘密(Secret)也不要涉及神秘(Mysteries)之假設等等前述學理上之反思與實踐上之檢證。而走向情報事務革命必須思考的就是傳統與新的情報典範之間的差別，數位時代之資訊本質的改變，科技改變的速度及便利與廉價性，人工智慧之「武器化」運用，更多情報消費者的期盼，動變現實已經對於過時的情報定義、角色與任務之衝擊等。因此，美歐等國家之情報改革正在進行並持續發展，相對於我們面臨的嚴重威脅難道不也應該正視與改善嗎(汪毓瑋，2018b)。

二、情報與反情報分而合之

對於情報與反情報之認知，常存有「迷思」。但事實上，「反情報」與「情報」不同，也無主從或隸屬或大小之分，兩者有其各自功能且互補。而反情報就是秘密情報活動的最秘密部分，是洋蔥的最核心部分，也是各國最努力建構的部分。從 1990 年代開始，美歐國家就指出「反情報」針對的是關於外國情報單位與組織之活動而不論其「友善」與否，彼等使用人員與科技手段以蒐集關於國家

資訊而對本國之國家利益與目標產生不利影響。因此「反情報」不能夠僅是侷限於「抓間諜」領域，且「反情報」所應對之威脅亦再被定義為係人員與科技之混合威脅，因此必須發展出跨領域之反制措施才能夠擊潰此等威脅，並強調此等措施應是「整合性」設計下之產物，並需要有跨部門之堅強合作(Godson, 1989)。亦即在「國家安全」之整合下，各司其職的情報與反情報必須更佳的協作。

情報與反情報之定義不勝枚舉，若要以易懂易記的一句話去說明，情報就是「掌握對手機密並影響其決策」；而反情報就是「情報之情報工作」。而一般論及要反制外國情報威脅，就大概包含了間諜；欺騙/認知管理；及含秘密與敏感之外交、軍事、經濟、社會等之其它情報運作等三大類。因此，在戰術層次上，就有所謂的「攻擊性反情報」，包括了四大類：分別是偵測之攻擊性反情報，計有先期調查、調查等兩項；欺騙之攻擊性反情報，可以分類為認知、誘餌、偽裝、藉口與計謀等四項；抵銷之攻擊性反情報，其工作計有反間諜、圈套、代理人挑撥、間諜與反間諜、雙面間諜、出賣行為、瓦解等七項。而另一面就是「防衛性反情報」，也就是安全防護之相關工作，包括實體安全之機密保護；屏障控制；門之防護；窗之防護；安全圍堵；安全照明設備；閉路電視監視；入侵偵測系統；電腦安全；警衛服務；敏感資訊隔離設施；安全屋；預防犯罪之環境設計等十三項(Prunckun, 2012)。攻擊與防衛兩者必須兼具才是完整的反情報。

要警覺外國情報機構不只是鎖定個別之駐地官員或是情報機構外站或是軍事、外交、經貿等政府部門，而是鎖定我們「整個國家」。因此，要更好的維護國家安全就需要從戰略層次上去發展反情報，而不能夠再迷信於「案例導向」或是滿足於抓了多少間諜。亦即「戰略反情報」要能夠落實兩項視野：第一、必須透過凝聚過程之戰略導引，進行蒐集、調查、分析與運作，且當需要時必須整合，當分工時也要尊重隔離，才能有更大的安全圖像浮現且命令有效分配資源與創造性的努力；第二、必須戰略性的不斷檢視我們的安全與情報弱點，因為對手對我們嚴密守衛的國家安全秘密不斷的滲入，也對支撐我們財富、日常生活及最終影響我們安全的國家「重大關鍵基礎設施」與「關鍵資產」非常感興趣，而想要盡可能掌控(Van Cleave, 2004)。猶記得當年我們「太陽花學運」時之兩岸協議監督條例籲求之主要內容，就是在過程中之國安體系介入以避免被傷害。而所謂的「介入」就是要發揮反情報對情報之檢證，因為在先期階段情報早已進入。

三、對手與盟友均是鎖定對象

有興趣我們國家機密的外國或是非國家行為者或是兩者間之多變組合，將會持續的使用其含「情報機器」在內的一切國家能力或「非政府工具」，以達成下述的目的：第一、滲透、蒐集與危害我們國家安全秘密，包括資訊、計畫、技術、活動、運作等，以增進其利益與擊潰我們的目標；第二、操控與扭曲我們決策者所規劃與執行的國家安全戰略、技術發展與經濟福利之現實圖像，包括了破壞我們蒐集的情報及執行針對決策者之影響運作；第三、摧毀與反制我們秘密的國家安全運作，例如秘密行動、「特別運作」及其他敏感的軍事與外交、經濟等行動；第四、獲得我們的關鍵技術與其他敏感的專利資訊，以強化其軍事能力或是增進經濟好處，或是破壞及誤導我們在此等領域之發展(Van Cleave, 2007a)。

國家內部的他國大使館和其他的外交建制(Diplomatic Establishments)均是外國情報活動的樞紐，而隨著科技發展與網路便捷，外國情報機構已越來越多地運用以前所未有的作為安全天堂之外交建制所獨立出來的「情報運作」，持續建構大量的正式和非正式的進入國家的管道，並利用民主國家內部易於旅行與相對友善的運作環境，執行量身定做的隱蔽蒐集活動。例如在國內數以千計的外國人擁有的商業建制，貿易、跨國經營和財務上的日常互動，以及成千上萬的學生和學者交流，均可能使外國情報延伸到我們國家安全的核心結構。此外，所擁有的廣泛、分工有序且任務明確與不同功能設計之運作有效的「情報機器」，亦會執行高度協調的針對國家資訊和電腦系統之蒐集與破壞活動。

因此，任何政府均把「外國」視為可能的假想情報蒐集國，而不論其是否是傳統或是持續的「友好」或是「敵對」國家。檢證已經發生過的國外間諜案例或是該等情報機構所提出的警告，均可以顯示出此等現實。所以看到美國抓到中共與俄羅斯間諜會覺得理所當然，但是看到美國也抓到日本、以色列或是英國間諜也不用訝異；同樣的，看到中共抓到日本或是美國的間諜認為很是正常，但看到北韓警告要注意中共對其之滲透與竊密，也不用懷疑彼等所謂兄弟之邦就不友好或是會被挑撥。因為情報與反情報工作的對象就是「外國」及被利用之本國人，而且任何國家均必須具備有效之「情報機器」，才能一方面抓到敵對國家間諜時之大快人心；另方面抓到友好國家間諜時之尷尬化解。因為任何國家都保有你想要但他絕對不給你的機密，而你又非取得不可。我們向來對盟國友善，只抓「共諜」卻似未顯出抓「外諜」之能量。但是機密外洩也常是來自於「他人」有心或無意之「間接途徑」，這也是「情報規律」。多年前我們的情報高層就曾警告

過，在臺灣最活躍的外國機構就包括了美國、日本、以色列等國家，且制式互動時我們常是「有問必答、不問也答」就必須改善。

肆、影響情報運用之危害

一、恐怖攻擊

近幾年來，世界各國推動情報之大幅改革，大概均是源於恐攻之「九・一一事件」，且改革之重點遍及於整個情報體制、法制及運作三個層面(汪毓瑋，2018b)。尤其是為了達成「先期預防」效果，涉及了情報與安全的法律改革最多，其中最具代表性的就是《愛國者法》(USA PATRIOT Act)、《情報改革與恐怖主義預防法》；並提出反情報戰略及不斷更新等，由於其過於強調先期行動，也因此引起破壞人權及政府濫權之質疑。但何以為了因應反恐，卻要改革情報呢？僅以「恐怖分子」與「間諜」為例，彼等平時有隱藏於人群中以伺機而動之共同特徵，且基於民主國家尊重人權之利便而易於籌謀、搜集可利用之「資源」；而兩者不同之處，就是恐怖分子的目的是要殺更多的人，且執行時要讓所有人知道以收其恐怖之效，然而間諜之目的是竊取機密與策反，且偷到以後更要隱藏也絕不能夠讓你知道，才能掌握決策與影響決策者以收到最大利用與破壞效果。

不論是惡意或是非惡意攻擊，型態上是自然的或是人為的災害，在初起之時總是不能那麼的「清楚歸類」，以致於會影響後續處理的難度。因此，美國發展「國土安全」(Homeland Security)概念，建立了包含情報單位在內之國土安全部，通過了《國土安全法》及其它互補之更多法律，並設計在此範疇下可更有效的統合資源與明確事權以處理「全危害」(All Hazard)可能造成之風險。此外，並分類了「恐怖主義資訊」、「國土安全資訊」、「執法資訊」以進入「資訊分享環境」(Information Share Environment)，盼達成中央與地方，公部門與私領域，執法、國防、外交、情報與國土安全各部門之間的必要資訊分享。且建立實體之「融合中心」(Fusion Center)，而能夠使情報、執法、消防、醫療等第一線回應人員之共同工作，以掌握「情勢警訊」(Situation Awareness)；同時亦可從下而上之鑑定、傳遞、評估「可行動情報」(Actionable Intelligence) (汪毓瑋，2021)。

二、自然災害

情報來源之分類各國不盡相同，但傳統上大概可以歸類五種情報來源：分別是人員情報(Human Intelligence)、電訊情報(Signals Intelligence)、影像情報

(Imagery Intelligence)、地理空間情報(Geospatial Intelligence)、測量和記號情報(Measurement and Signature Intelligence)、公開來源情報(Open Source Intelligence)。但英國的情報文件又多分類了聲學情報(Acoustic Intelligence)、材料和人員利用(Materiel and Personnel Exploitation)等二大類，而在這七大類之下又有「次」分類就不一一列舉(Ministry of Defense, UK, 2011)。另亦有所謂「科技情報」之說詞，但實際上它並不是情報學上正式分類，因為前述之每一分類，均包括「科技因素」在內。而一份完整情報產品，最佳狀態下，就是透過這些來源的蒐集與分析；再加上了「反情報」檢證，才可以說是達成了所需之「完成情報」(Finish Intelligence)。

隨著全球暖化及自然氣候已不像以往可由氣象或地質等專家依於既有學理與經驗規律進行「預判」，且常會失準，但是這在些自然災害發生之前，若沒有更好的觀察與可供決斷的資訊，則造成的災難常會變成是「複合式的」，不僅會失掉多條人命，更會造成重大的經濟損傷與心理創傷。這些發生過的事件就包括了印尼的大海嘯，美國的凱崔娜颶風、四川的汶川大地震以及臺灣的九二一大地震等。因此，除了既有的氣象單位之外，美歐等國家也會要求情報圈以其強大的資訊蒐研能力必須提供更多貢獻。例如 1974 年，美國的「洛克希德委員會」(Rockefeller Commission)建議設立「民事應用委員會」(Civil Applications Committee)以強化在國內為了民事目的，例如火山活動、環境與地質改變、龍捲風與洪水等，而適當使用情報圈之太空影像與遠端感應能力之「地理空間情報」與「測量和記號情報」等。其後在此委員會的基礎下經由各方建議，2007 年 5 月，「全國應用辦公室」在國家情報首長麥克康奈爾(Michael McConnell)批准下成立，並由國土安全部情報長(chief intelligence officer)艾倫(Charles Allen)來負責此計劃之執行；並接續成立「全國應有執行委員會」，以提供跨部門之高層監督與指導。目的是如何透過其它重要蒐情部門所蒐集來的資訊可以在自然災害之減緩、準備、回應與復原過程中可以被有效與合法的使用(Civil Applications Committee, 2001)。

三、網路攻擊

網路空間是廣泛破壞行動的天堂，包括偵察、盜竊、破壞和間諜活動。且作為一個允許威脅硬體、軟體、金融資產、知識產權和個人身份之環境。動態的網路威脅是由三個部分組成，亦即網路空間環境、網路威脅、網路空間環境和威脅

影響的融合。而應對此等威脅必須付出兩個主要成本，就是對抗活動及提供和維持安全之費用。而必須關注之主題，包括：第一、應該系統性的定義和建立有效的網路情報途徑，持續的專業知識和所需的技能/培訓/教育和技術；第二、要能夠在企業、學術/非商業機構之間建立與網路相關的政策、途徑和試點努力，其中應該提供非機密的情勢警訊、指標、警告資料和分析，及提供全年無休之非機密及機密報告給政府部門、可信任的企業與全球夥伴；第三、建立公私夥伴關係之網路外聯論壇，以全面、務實和可執行的方式解決這些問題/疑慮；第四、在所有相關機構和私營部門間建立有意義的「虛擬夥伴關係」，確保威脅資訊的無縫分享，才能及時分析判斷和推理，衡量對明確威脅的反應。

由於網路挑戰了國家安全和利益，但網路安全又難以處理的兩個關鍵就是缺乏國際法律框架以及準確的「歸因活動」。因此，前述關注主題之處理，就需要充分利用「網路情報」(Cyber Intelligence)的資產和能力來解決這個無處不在、多樣化和不斷發展的不同以往之活動於網域(Cyber Domain)的虛擬對手類別。而對任何形式安全的強化，情報就是戰術和戰略決策的關鍵組成部分。有效的「網路情報」將會提高我們評估網路攻擊效果的能力，減輕與威脅相關的風險，並根據「被通知」而進行有效決策，且可以將網路安全簡化為一個高效且具有成本效益的流程。為了使網路情報有效運作及分享威脅資訊，也必須建立一個由軍文部門、電信和網際網路提供商、電腦緊急回應組(Computer Emergency Response team)和其他官方的資訊安全實體、專業公司和供應商所組成之獨特、特設的「網路情報圈」(Cyber Intelligence Community)，以進行可能是網路攻擊潛在受害者之無數鑑別與反制活動。而一旦此等情報領域建構與運作順暢，就可將各種軍事和政府網路指揮轉移到更好地履行其個體和集體之特定網路任務，並依於不同層次之戰略、戰役及戰術網路情報進行有效攻防。

四、新冠肺炎

美國情報官員仍在調查新冠肺炎(COVID-19)可能是從武漢病毒實驗室開始由蝙蝠到人的傳播的可能性，迄今情報人員尚無足以指控的具體證據(德國之聲中文網，2021)。但是從 2019 年底，聯邦調查局就警告中國公民企圖將潛在的危險病毒傳入美國；且 2020 年 4 月 1 日，根據「華盛頓審查員」(Washington Examiner)報告，該局至少偵查三起涉及生物與醫學危害之異常事件，指出外國科研人員以個人隨身攜帶和/或託運行李方式，將未申報和未記錄的生物材料運入美國，且幾

乎肯定會帶來美國的「生物保安」(Biosecurity)和「生物安全」(Biosafety)風險。但國際與美國內亦有把對中國大陸實驗室的懷疑與指控，視為是「陰謀論」的典型表現，目的是要爭取美國的最大利益及配合國內總統大選而運用的策略。

「伊斯蘭國」從 2020 年初開始追踪疫情，並在其《消息》(al-Naba)時事通訊中介紹與更新疫情狀況，要求在歐洲的任何生病的聖戰士都應該呆在那裡，以藉此加大對十字軍之傳染力度；其他未感染聖戰士不要進入傳染地。且在線宣傳海報之《庫拉夏媒體》(Quraysh Media)也製作並分發帶有危險物套裝和防毒面具者的海報，並指出：「承諾是我們不能忘記的債務」。此外，美國國土安全部「聯邦保護局」之《每週情報摘要》(Weekly Intelligence Brief)指出，「白人至上主義者」(White Supremacists)已在《電報》(Telegram)之貼文上，討論如何經由「唾液」、「噴霧瓶」或「飾帶物品」等各式不同方法將《冠狀病毒武器化》的計劃，並置目標於公共場所，且攻擊執法人員和「非白人」族群。因此，警告暴力極端主義者將繼續聚焦於「生物恐怖主義」之陰謀。

流行病學之傳統醫學調查範圍與無意的「意外事故」和有惡意的「異常事件」發生後相似，必須協調情報、執法、公共衛生和私營部門社群的資源組合與協作，以實踐現地調查、發現、預防、回應和緩解潛在致命物質的目標。而從情報的角度言，「生物醫療情報」(Biological Medical Intelligence)旨在收集、分析和分發有關生物和醫學威脅的情報資料，也包括了已經影響國家安全和國土安全之「偵測」、「嚇阻」、「回應」和「緩解」包括化學、生物物質與病原體等造成之危害。而此種情報類型，共計有四種生物製劑或生物武器，情報圈必須關注蒐研與預防：亦即病毒(Viruses)、細菌(Bacteria)、瘟疫(Plagues)和未經修飾而發生的天然毒物(Natural Poisons)或毒素(Toxins)。且當「新冠肺炎」發生後，美歐之情報檢討仍沒有停止而持續進行評估，例如除了要有「醫療情報」外，也要有防範從網路盜取疫苗之「網路情報」、預防攻擊醫療關鍵基礎設施之「國土安全情報」等，均成為新興的情報類型及蒐研重點。此外，若僅針對生物與醫療情報檢討，它們是歸屬「情報來源」之「材料和人員利用」範疇，是一種系統性蒐集、資訊處理，和通過戰術質詢、詢問和從回收材料中提取資料所獲得之情報的「分發」。姑不論臺灣現行情報圈人員是否具有此等醫學專業，或是能將相關知識貫穿整個「情報循環」，而能及時向決策者提供預警？僅是由誰來定義？誰來負責？協作之法律授權？蒐研範圍？如何分發？等都必須儘快解決(汪毓瑋，

2020a、2020b)。

伍、改善軍事情報之思考

一、軍事情報的對象與任務應調適

混合威脅定義就如前述，可描述為行為者之「模糊性」、不受「地理」或「疆界」限制，「同時」存在於多樣化「空間」，混合採用結合「可調適」、「系統性」、「量身定製」的「不易歸類屬性」、又能夠悠遊於「灰色地帶」的隱而不顯作為。且不同於以往個別進行之恐怖攻擊、自然災害、網路攻擊及新冠肺炎等帶來之危害，因為均可能被融合成進行「混合戰爭」之一環。且「混合」之特徵，就絕非任何一個政府部門或賦予之權責可以獨自的承擔，特別是造成了新的「情報類型」之需求與蒐研，此不但衝擊到現有的情報體制、法律擬訂或修正與授權，也影響了以往「慣用」之思考與行動模式，而必須調整與變革。

「混合戰爭」也不同於以往「常規戰爭」(Conventional War)之鎖定對手國家之兵器與戰士，也要面對多樣化的「非戰爭軍事行動」(Military Operations Other Than War)(王寶付，2010；汪毓瑋，2021)。[2]又若從衝突樣式之角度進行檢視，則要反制「混合衝突」必須同時因應四項挑戰，亦即「非正規挑戰」(Irregular Challenges)，要能夠擊潰恐怖分子及網路空間破壞活動；「災難式挑戰」(Catastrophic Challenges)，要預防流氓國家或是非國家行為者取得大規模毀滅性武器，並要進行深度之「國土防衛」(Homeland Defense)(汪毓瑋，2021)；「傳統性挑戰」(Traditional Challenges)，要因應堪與匹敵對手可能之敵對作為；及「破壞性挑戰」(Disruptive Challenges)，必須協助型塑處於戰略十字路口之治理不良或脆弱國家，可以進行正確之發展選擇不被利用。此等相互重疊之四大挑戰，將會是持續變化過程的一部分，且均具有短期與長期之意涵(汪毓瑋，2016，2010)。因此，我們傳統上「打、裝、編、訓」之軍力整建的依據理念，可能均要重新思考。且必須強化一種「全政府能力」(A Whole-of-Government Capability)，擴大情報、分析與鎖定目標的能力，才能夠快速處理、利用與融合來自各式不同來源的

[2] 2005 年，美國在總結伊拉克戰爭的經驗教訓後，已開始以「穩定行動」取代「非戰爭軍事行動」概念。到了 2006 年 9 月 17 日，美軍參謀長聯席會議在公布新版的《聯合軍事行動綱要》中明確指出，不再使用「非戰爭軍事行動」的術語及其縮寫詞。用意是將軍事行動範圍之劃分，由原來的「戰爭行動」和「非戰爭軍事行動」兩大類，調整為「大規模作戰行動和戰役」、「危機反應與有限應急行動」及「軍事接觸、安全合作和威懾行動」，但仍將原來「非戰爭軍事行動」的相關內容保留。

資訊，且分發給戰術階層之行動者(Bolkcom, 2009; Department of Defense, USA, 2006)。

從作戰取勝的層面思考，情報就是戰術和戰略決策的關鍵組成部分，雖然混合威脅不易掌握，也不論它穿上了光譜系式之多變外衣而不易切割應有之應對「途徑」，但有一點卻是明確的，亦即它的鎖定目標就是國家之重要關鍵基礎設施與關鍵資產，因此以這些目標與領域(Sector)的安全防護作為情報工作之新起點已是趨勢，而這也是美國創立「國土安全」概念之用意。且檢視美國政府每年撥給國土安全運作的經費中，除了國土安全部以外的最高機構就是國防部。因此，軍方之作戰思考必須與時俱進的更新，軍事情報才能夠相應的聚焦。

二、全國安全工作防護之軍事情報

因應混合威脅之軍事情報工作要檢討的議題與內容太多又敏感，只能夠謹慎的取捨及概述。若就體制言，依於《國家情報工作法》第三條第一項及第二項定義之情報機關與「準」情報機關所涉及的軍方機構就有六個之多，占據了十一個情報圈成員之一半，且其情報主管機關均是國家安全局；而情報工作運作的主要法律依據就是《國家情報工作法》，以及由國家安全局局長自行頒布的一些辦法、規定與函令，例如《國家情報工作法第七條第一項第三款所規定之其它重大治安事務之定義》等；亦即不論是對外情報或是人民日常生活可能涉及之安全及犯罪問題等均可以包括在內，也有先期行動權利。因此，不論是前任的馬總統或是現任的蔡總統均曾啟動訂定《保防工作法》，但可惜都未能完成。

若從國土安全之脈絡，及因應「自然」,「人為」與「資安」已有之混合威脅趨勢去思考，或許影響了 2019 年 12 月，法務部調查局終於將以往國內安全工作所依據的《保防工作作業要點》修正為《全國安全防護工作作業要點》，並公佈了《全國安全防護工作會報設置要點》，將涉及反情報之「軍中保防」亦更名為「軍中安全防護」。亦即國內安全工作應該不能夠再侷限於「保密」與「防諜」之窄化作為。但是何謂「安全維護」並未解釋，似想彈性而有更大主導解釋與活動空間。且規定「地區安全防護工作執行會報」要邀請轄區直轄市、縣(市)政府負責統合、督導安全防護工作之副首長或幕僚長列席，亦即既使非情報與準情報的地方行政實權者亦必須與會及協作。法務部廉政署也成為會報的新委員。而在 2020 年 5 月公布之《全國安全防護工作會報作業要點》中，地區會報之各地區與會成員，就包括了重要國家關鍵基礎設施之政風機構主管。這些新的規定與發

展，應可以緩解混合威脅之無法清楚的鎖定行為者及行為模式之情報工作難處，但也有待軍事情報部門思考如何進一步設計及精進新興之情資蒐研。

基於反制混合威脅之較可釐清的鎖定關鍵基礎設施與關鍵資產目標之侵入與破壞言，「重要國防軍事設施」早已被行政院列為關鍵基礎設施安全防護之範圍，因此有必要重新檢討在此等軍文互動之「安全維護」任務中，有關情報蒐研及資訊交流機制設計上可資發展方向，及參與關鍵基礎設施防護和有關公、私部門安全協作及相互支援方面之在組織架構、法律授權及實務運作上尚待補正充實之處。例如重新檢視安全責任區劃分之機密點、價值點、危害點衡量是否應配合「國土安全」要求而重新設計「國軍關鍵戰力基礎設施」之定義與範圍，特別是在我國防產業自主發展更趨主動的情勢下；以及就國軍核心機密事項，含 C4ISR 系統整合、武器研發測評、情報產品運用、兵火力部署、軍事合作交流、重大戰備演訓、敏感軍備採購、後備動員整備，以及涉及網路與電子等新興科技元素在內之「資訊管理」(Information Management)與「資訊作戰」(Information Operations)等也均涉及了私領域，包括了中科院、軍工複合體與科學園區廠商等，這些不同以往之工作「對象」，則究應如何建立信任關係以有效「進入」與「運用」也必須重新規劃，才可能完善情勢警訊與危害等評估。

隨著蔡總統之資安即國安的戰略宣誓及要求以「情報導向」之資安設計及建構「關鍵資訊基礎設施」的資安聯防及情資分享體系，以完善「數位國家」之發展方向；加諸行政院已執行之《資通安全管理法》、《資通安全情資分享辦法》，要求公部門與私領域之更及時與有效的資訊分享，並反映在要求「資安聯防監控中心」(SOC)、「資訊通報與應變中心」(CERT)及「資訊分享與分析中心」(ISAC)之運作完善；且接續依蔡總統指示成立的以完善網路戰之「資通電軍指揮部」之軍事情報介入，均彰顯維護實體與虛擬空間之「資訊優勢」的重要性。但問題是作為準情報單位之「資通電軍指揮部」是否真的有「網路情報」之概念？若無，則如何能夠架構出網路情報之「情報循環」？是否有明確的介入私領域之關鍵資訊基礎設施之法律授權？如何能夠與「資訊分享與分析中心」等有效互動？又國安局是否有網路情報之戰略規劃以作為分而統合之情報指導？且國安局內部不同之資訊與網路單位如何接軌軍文部門及私領域之授權，以優化情報導向之資安聯防體系？而作為「國土防衛」重要支撐之新成立的「國防部全民防衛動員署」在平時就應更好的整備全民防衛動員及軍事動員業務，目的就是希望在變時能夠充

分展現出「韌性」(Resilience)，則軍事情報可以扮演何種輔助角色？及應該建立合種合作模式？才能夠及於私領域之公私夥伴關係進而完善情報主導之「國土安全網」。凡此均是軍事情報工作必須整合思考的(汪毓瑋， 2021)。

若再從更一般及「混合防衛」(Hybrid Defence)之原則性設計角度言，軍事情報還必須思考努力改善方的方向包括：

(一) 必須超越只是提供「支持功能」的運作方向，亦即情報要有相互連接之多層面途徑，經由網絡互補以主動避免危害；其次、要有「系統性途徑」，從面去檢視點，從脈絡去發掘情報；第三、要建構「系統動態之系統途徑」(System of Systems Dynamics)，包括情報之反情報分析和應對新威脅之科技工具運用。

(二) 進行「三合一」之情報建構與協作，亦即統一國家情報工具的凝聚性應用；與其他行為者的全面性互動；以及在所有平台(Domains)和危機要素中的全面性行動。

(三) 要朝四項戰略方向努力，亦即創建一個聚焦於混合威脅的「情報中心」；加強和擴大應急規劃之情報蒐研，包括「低層次武力」(Low-Level Force)、網路攻擊和資訊戰(Information Warfare)等；完善法律工具以應對外國違反國內法的行為；及早發掘對手國家或其支持實體之任何政治融資。

(四) 改善檢測「混合威脅」的情勢警訊能力，亦即分享情報分析和評估工作，以減少不確定性；有條理的分發資訊以進行有效的「戰略溝通」。

(五) 建立融合之情報能力：加強十一個情報圈成員之間的有效協調；建立一種公私領域合作之「情報意識文化」，且輔以改進的培訓和實體安全，例如積極主動的報告機制，從而提高對「混合威脅」的認識；並以反情報支援與深化「投資查核」與「人員查核」。

(六) 加強可以作為預防和威懾行動之情報韌性，以鞏固社會錯誤資訊侵擾分化，避免內外的危機升級。亦即不可能完全避免危害之發生，但應能夠經由情報來減緩持續的時間及盡可能壓低損傷的程度，而使「核心功能」持續運作。

(七) 從嚴從難設計「混合威脅」情節，經由「系統動態之系統途徑」進行情報融合和分析(Intelligence Fusion and Analysis)之「完成情報」的桌上推演與

模擬與演習，而能達成檢證情報「效果」之「似真」、「逼真」與「超真」的三個演化層次。

三、六大作戰領域內之反情報發展

檢證任何標榜民主之國家情報體系大概都可以明確區分成「情報」與「反情報」兩大領域，且各有其法律依據，以避免濫權而危及民主與人權之基本價值(汪毓瑋，2018b)。我國則只有一套《國家情報工作法》，反情報已被窄化成情報之運用工具而已，此種現實不僅不利我國「整全」之安全維護，也不利對情報正確與否之第三方「檢證」，亦即對手之「謀略」與「欺騙」等作為無法有效辨識。或許也因為我國沒有反情報概念之現實與實踐作為；因此，2008 年 12 月出版的六大作戰領域中之「情報戰原理與運用」一書中，並未提及反情報之理論與實踐。

所以未來軍事情報作為可以再強化此部分之內容與理解以進行相關知識累積，本節因限於篇幅僅能重點概述一些推動「戰略反情報」應努力的方向；這些內容也可以作為目前被視為「準」情報機構之國防部政治作戰局、國防部憲兵指揮部、國防部參謀本部資通電軍指揮部等軍事情報工作改善之衡量指標：

(一)混合威脅是具有戰略性意涵的：

外國情報運作已更分散、更侵略性與技術上更複雜，且較以往更有成功的潛在可能性。這些主體包括了利用合作關係的外國夥伴，使用欺騙與否認技巧及執行可發揮影響與其他的秘密運作。利用民主社會與人民的開放性弱點發展接觸與沒有告警的運作；在國境之外，亦有許多潛在的有價值的被鎖定目標，包括了海外駐館人員、商業與工業的商人等，但是他們的中心目標仍是在我們國家之內。因此，反情報必須關注的不僅只是潛在必須鎖定的這些目標，更重要的是外國情報機構執行有關活動的範疇。

(二)改變威脅導引行動之傳統作法：

以往各個情報機構均有其各自一套情報作為及所賦予之個別權責，亦即在設計上是透過情報的「分開」責任，以務實的處理外國情報威脅。但這充其量只是服務於「個別」情報機構的任務目標。因此，反情報演變成只是由「威脅導引行動」，各情報機構均有其各自的威脅測量，而不是基於一個更大的「整體安全」思維。結果就造成了沒有認知可能被鎖定目標的「標準」鑑定途徑、跨部門的資訊分享不足、沒有支撐的關鍵基礎設施結構等無法克服的問題。

(三)戰略反情報應努力之七個重心：

反情報的任務就是行動，是對抗外國人行動及「操縱」外國人為我國家目標服務的行動，而其具體工作，就包括了鑑定、評估、抵銷與利用外國勢力。其中「抵銷」整個外國情報機構計劃尤為重要。因為如此的作為，需要有視野、領導、承諾、知識和耐心，且要從反情報建制的頂端去從事更多的作為，而不僅僅只是逮捕間諜或運作「雙面間諜」的行動。此等反情報工作雖然相對困難，但相關任務可以了解整個外國情報威脅，而不是它的片斷而已，並利用這些知識去破壞外國情報操作的優勢(Regan, 2005)。因此，必須深化與努力的七個重心如下：

1.瞭解外國情報威脅是戰略性的，此意味有目的的使用其情報資源以凌駕對手國的利益，並進而增進自己的利益。因此，必須適當的瞭解外國情報機構在我們國家的駐留和其情報活動，及其對於反制我們國家安全的更大努力。

2.戰略情報威脅無法通過現存的措施被獨自擊敗，這些威脅必須經由一個整全之戰略回應來反制。每一個案例均有其特色，但卻沒有將外國情報機構當成一個戰略性目標而視為是要進行更大反制的一個部分。戰略之目標不是等他們進入到國內才去逮人，而是在其「源起」時就要阻止他們進來。

3.戰略性威脅需要戰略性的凝聚性回應，不應該只是以「案例導向途徑」、聚焦於國內資源去應對外國情報的運作，而是應該到海外與外國情報機構直接交戰。應該掌握「戰略倡議」並開始鎖定在國外的目標，有目的之選擇降低外國情報機構及其對我們做工作的能力。而這就是戰略反情報的中心目標。

4.反情報之戰略趨向就是要主動鑑定、評估與摧毀敵人的運作。例如透過網絡分析(Network analyses)以努力描繪出施展混合威脅的供應鏈、支援的關鍵基礎設施結構、金融交易、通訊管道、甄補與訓練活動，及與其他用於聚焦蒐集、鑑定弱點與告知戰略運作規畫，以攻擊、摧毀與消解敵對者的運作。

5.進行外國情報能力的戰略評估，可以協助決策者而告知政策可以如何的更佳細緻化與架構出最佳實踐的選項。而當整合其他的外交政策工具或軍事作為，透過戰略反情報行動的運作與洞見，就可以較佳之控制與區隔出想要與不想要的結果。

6.要執行戰略反情報的任務，則反情報分析人員首要決定外國情報機構是如

何建立與運作，這就是反情報之「戰鬥序列」準備：此等工作包括了要掌握外國情報機構鎖定我們的能力；如何部署；有那一些工作對象及方法；組織、結構與預算；如何進行甄補等。而經由這些分析工作，就可以轉而再重新定義蒐情需求、協助鑑定出外國情報機構的弱點、支援利用他們的戰略運作規畫，且可以激起有利我們達成目標之新可能性的一些方法。

7.必須有一個國家層面的反情報體系而能夠整合與協作不同的反情報計畫、資源與行動，才能夠達成共同的戰略目標。因此，戰略反情報任務需要有一個支援關鍵基礎設施的結構，以架構出反情報圈之資源，而能聚焦於外國情報機構的蒐情與分析，進行戰略運作規畫以處理蒐情之鴻溝、發展降低外國情報機構的選項，且能夠協作執行以達成「攻擊性」與「防衛性」的反情報目標(Van Cleave, 2007b)。

陸、結論

軍事情報工作之展望必須納入整個安全脈絡下去檢視，才能掌握其所處的定位，及進而整全的推動其應有之工作改善方向。想要回應或是反制不同以往之混合威脅的困難在於其無法清楚的切割「正常」與「異常」，因此就不易分辨是真的危害還是假的意外？也無法以傳統行政上之官僚體系區分權責去應對與解決。

隨著動變安全環境的變化，可發揮作為決策基礎之情報功能必然成為大家關注焦點及接續而來之檢討要求，而初起工作就是學理上之檢視並反映在實踐上之改革及不斷修正。我國情報體制延續對日抗戰與國共鬥爭，始終陷於保密與防諜兩項工作，既使防諜也只抓「共諜」而非「外諜」致有其相當侷限性。

雖然為了因應混合威脅已將保防改為國家安全防護工作，但「反情報」之實踐仍有相當大的改善空間。特別是在非戰爭期間，其實對手國之政治作戰就已進行。因此，基於混合威脅而來之混合戰爭似乎就是政治作戰之某個領域的外延而已。如此相較於他國之回應威脅，我國雖有政治作戰六種作戰方式之情報戰，但必須再強化反情報之內涵，如此軍事情報工作之變革與創新才有可能。

如果還無法判斷臺灣是否發生過混合威脅，而對於有關文字定義描述感到抽象，則基於混合防衛之「情報模擬演練」混合威脅的情節，應可以基於已發生過的外國案例或是軍事情報想定如下，並試想現有之軍事情工作是否能夠因應？

國家或是非國家行為者針對預定的連接軍事資產的國家重大關鍵基礎設施的

直接計劃性攻擊；或是更具機會主義，例如在極端的天氣事件，觸發電網故障，但因為非動態入侵不會觸發全面回應；軍事資產和專業知識可能會保持觀望，因為還沒有人受傷或死亡；警察和其他執法資源正在等待犯罪的證據；傳統的緊急情況和災難回應團隊和機制也可能不會受到警報或部署，甚至沒有進行人為惡意之預判。或至少直到惡意軟體導致連鎖效應的重大關鍵資訊基礎設施故障時，才會通知或部署。更糟的是，如果放置惡意軟體後進行跨界操作，國際合作與協調的複雜性將加劇上述所有待命攻擊的趨勢。也可以想像在夏季熱浪中，主要城市中心遭到大規模電網襲擊。攻擊者對「網格」硬體的實體攻擊包括跨縣市的變壓器和電站並與分佈廣泛的惡意軟體結合，且惡意軟體正在操縱和禁用控制電力分配，並連接到全球網際網路的「監督控制和數據採集系統」。由於電網硬體和設施上的襲擊者處於分散狀態，可疑犯罪嫌疑人未被發現，散佈該軟體的電腦遍布全球而不能歸因於任何特定位置，也無法歸因於任何行為者。在此等情節上，還可以再繼續混合多項威脅，例如新冠肺炎等以持續進行混合作戰，則軍事情報工作甚或整個國安局主導下之情治體系真的可以預警與處理嗎？

參考文獻

一、中文部分

王寶付(2010/2/5)。海地救災成練兵平臺，美軍詮釋非戰爭軍事行。*中青在線*。取自 http://military.china.com/zh_cn/news2/569/20100205/ 15806499_1.html(檢索日期：2021/7/14)

自由時報(2021/5/26)。白羅斯獨裁總統駁「劫機」 批歐美發動「混合戰」。*自由時報，國際*。取自 https://news.ltn.com.tw/news/world/breakingnews/3547411 (檢索日期：2021/7/14)

余瀟楓、王江麗(2006)。非傳統安全維護的邊界、語境與範式。*世界經濟與政治，11*，41-42。

汪毓瑋(2010/9/28)。*從美、中等國陸軍非戰爭軍事行動發展趨勢探討我國陸軍應有作為*。桃園市：中華民國 99 年陸軍年會專家學者論文集，1-27。

汪毓瑋(2016)。*恐怖主義威脅及反恐政策與作為-上、下冊*。臺北：元照出版社。

汪毓瑋(2018a)。「混合戰爭」脈絡下之「假消息」工具運用。*清流雙月刊，18*，26-31。

汪毓瑋(2018b)。*情報、反情報與變革-上、下冊*。臺北：元照出版社。

汪毓瑋(2020a)。灰色地帶與混合威脅之虛與實。*清流雙月刊，25*，34-39。

汪毓瑋(2020b)。從新冠病毒思考因應生物恐怖攻擊之模擬演練。*清流雙月刊，27*，10-15。

汪毓瑋(2020c)。新冠肺炎引發之情報工作思考。*清流雙月刊，29*，50-55。

汪毓瑋(2021)。*國土安全-上、下冊*。臺北：元照出版社。

德國之聲中文網(2021/6/28)。拜登政府：情報機構新冠溯源調查或無法得出結論」。*德國之聲，時政風雲*。取自 https://www.dw.com/zh/拜登政府情报机构新冠溯源调查或无法得出结论/a-58076261(檢索日期：2021/7/16)

二、英文部分

Aaronson, M., Diessen, S., De Kermabon, Y., Long, M. B., & Miklaucic, M. (2011). NATO countering the hybrid threat. *Prism, 2*(4), 111-124.

Bolkcom, C. (2009) Statement before the Senate Armed Services Committee. Retrieved from http://armed-services.senate.gov/statemnt/2009/April/Bolkcom%2004-30-09.pdf (檢索日期：2021/7/16)

Buzan, B., & Herring, E. (1998). *The arms dynamic in world politics*. Lynne Rienner Publishers.

Buzan, B., Wæver, O., Wæver, O., & De Wilde, J. (1998). *Security: A new framework for analysis*. Lynne Rienner Publishers.

Civil Applications Committee, USA (2001/7). *Fact Sheet*. Retrieved from http://www.fas.org/irp/eprint/cac-fs.pdf(檢索日期：2021/7/14)

Collins, A. (Ed.). (2016). *Contemporary security studies*. Oxford University Press.

Department of Defense, USA (2006). *Quadrennial Defense Review Report*. Retrieved from http://www.globalsecurity.org/military/library/policy/dod/qdr-2006-report.pdf(檢索日期：2021/7/15)

Department of Defense, USA (2007). I*rregular Warfare (IW) Joint Operating Concept (JOC)*. Retrieved from https://fas.org/irp/doddir/dod/iw-joc.pdf(檢索日期：2021/7/16)

Department of Defense, USA (2009). *Capstone Concept for Joint Operations Version 3.0*. Retrieved from https://www.globalsecurity.org/military/library/policy/dod/ccjo_v3_2009.pdf(檢索日期：2021/7/16)

Department of Defense, USA (2010). *Quadrennial Defense Review Repor*t. Retrieved from https://www.defense.gov/Portals/1/features/defenseReviews/QDR/QDR_as_of_29JAN10_1600.pdf (檢索日期：2021/7/16)

Department of the Army, USA (2008). *America’s Army: The Strength of the Nation*. Retrieved from https://www.army.mil/e2/downloads/rv7/aps/aps_2010.pdf(檢索日期：2021/7/14)

Godson, R. (1989). Intelligence Requirements for the 1990s. *Washington Quarterly, 12*(1), 47-65.

Hoffman, F. (2014). *On Not-So-New Warfare: Political Warfare vs Hybrid Threats*. War on the Rocks, July 28. Retrieved from http://warontherocks.com/2014/07/on-not-so-new-warfare-political-warfare-vs-hybrid-threats/.(檢索日期：2021/7/16)

Joint Forces Command, USA (2010). *2010 Joint Operating Environment*, Retrieved from https://fas.org/man/eprint/joe2010.pdf (檢索日期：2021/7/16)

Kennan, G. (1948). *The inauguration of organized political warfare*. State Department Policy Planning Staff, National Archives and Records Administration, RG, 273.

Ministry of Defense, UK (2011). *Joint Doctrine Publication 2-00 Understanding and Intelligence Support to Joint Operations*.

Prunckun, H. (2012). *Counterintelligence Theory and Practice*. *Lanham*, Maryland: Rowman & Littlefield.

Regan, M. L. (2005). *Introduction to U.S. Counterintelligence*. Retrieved from http://www.hsdl.org/?view&did=460369(檢索日期：2021/7/16)

Supreme Allied Commander Europe & Supreme Allied Commander Transformation (2010). *Hybrid threats description and context*, IMSM-0292-2010. Retrieved from http://www.act.nato.int/images/stories/events/2010/20100826_bi-sc_cht.pdf(檢索日期：2021/7/16)

Terriff, T., Croft, S., James, L., & Morgan, P. (2000). *Security studies today*. London: Polity Press.

Treverton, G. F. (2003). *Reshaping national intelligence for an age of information*. Cambridge University Press.

Van Cleave, M. (2004). National Counterintelligence Executive Remarks for Department of Defense Conference on Counterintelligence San Diego, California.

Van Cleave, M. (2007a). *Counterintelligence and National Strategy*. School for National Security Executive Education. Retrieved from https://apps.dtic.mil/sti/pdfs/ADA471485.pdf(檢索日期：2021/7/16)

Van Cleave, M. (2007b). Strategic Counterintelligence: What Is It, and What Should We Do About It? *Studies in Intelligence, 51*(2), 1-13.