俄羅斯運用社群媒體進行資訊戰之分析
——以2014年克里米亞事件為例

作者簡介

曾柏元中校，陸官90年班、步校正規班339期、陸軍指參學院101年班、國立政大戰略與國際關係研究所；曾任排、連、營長，現任國防大學教官。

提　要

一、2014年俄羅斯以社群媒體製造假訊息，其多以境內俄裔遭受危險以及民眾(克里米亞)支持加入俄國為內容，最終僅以短短13日就已入侵東烏克蘭，可被堪稱為當代「資訊戰」的最佳範例。

二、俄羅斯資訊戰並非單純戰術(略)手段，其實它是可改變目標國的文化與社會的價值觀，若更為嚴重便可推翻國家政權，而俄羅斯則是首以資訊戰，達到政治目標的國家。

三、從克里米亞事件中，不難發現俄羅斯資訊戰具有多樣性，可跨越平時與戰時，其中影響最為嚴重的莫過於「心理認知面」，尤其在社交媒體運用上可說是相當活躍。

四、資訊戰是以非軍事手段，藉由社會心理控制，進而製造動盪與混亂；而近幾年各國都逐漸發覺社群媒體給予的影響，我國政府也不例外。據此，紛紛提出社群媒體的監管及對應之策。

關鍵詞：資訊戰、社群媒體、俄羅斯、克里米亞

前　言

自從普丁(Vladimir Putin)總統上台後，俄羅斯積極發展資訊戰(Information warfare)，從2014年對烏克蘭(Ukraine)衝突可見，廣泛運用資訊戰之元素「社群媒體」(Social Media)[1]實施國際宣傳、網路駭客與假新聞(Fake news)等活動，同時配合特種部隊(小綠人)在關鍵時刻奪取指揮與通訊設施，以最低限度之軍事力量，在短暫13日間奪取克里米亞(Crimea)，此事件被認為「資訊戰」最佳案例。

實際上，資訊戰也是「混合戰」(Hybrid War)中的一環，且是不可或缺的一環，因在資訊時代中，政治、經濟、軍事、文化、社會等等都相互關連，若任一領域遭受資訊危害，都可能會互相衝擊與影響，造成國家與社會動盪，因此常被稱之混淆戰爭與和平的界線。

因此，本文希藉從美國學者李比奇(Martin C. Libicki)所定義的「資訊戰」觀點，從國家角度切入，試以探究俄羅斯吞併克里米亞事件對於資訊戰的應用。再以研析俄羅斯如何對內(外)操縱媒體領域及干擾烏克蘭資訊系統。除此之外，也藉由整體事件的分析，引發國人思考，兩岸關係與俄烏關係頗相似，中共是否也以同樣方式對我國執行「統戰」。相對我國又須採取何種的態度與因應，也是值得持續關注與研究。

俄羅斯資訊戰的定義與準則

回歸歷史，在1900年發生的第一次波灣戰爭中，美國從人類社會進入資訊時代的「第一場資訊戰」。當時蘇聯尚未接觸西方大眾媒體，無法理解資訊戰的重要性。直至1991年蘇聯解體後，俄羅斯開始試圖學習與探索，如何以資訊戰手段謀取國家利益，重建世界強權的地位。

一、俄國資訊戰之定義

(一)資訊戰定義

首先，「資訊戰」[2]一詞是伴隨著1970年代末「資訊革命時代」

1　本研究為了符合一般的通稱，因此在內文中仍以「社群媒體」一詞來概括，主要定義以傳統的大眾傳播媒體如報紙、雜誌、廣播與電視等，也都是以一般社會大眾為主要目標對象的媒體，儘管沒有人以社群媒體來稱呼這些傳統的媒體，但其本質上均稱之為社群膜體，現在所通稱之社群媒體，真正名稱應該「數位社群媒體」。事實上，在數位媒體時代中，數位社群媒體已將以上內容與科技來區別大眾傳播媒體的類型加一模糊化，並且匯流在一起。參考胡光夏、陳竹梅，〈社群媒體與軍事公共關係〉《復興崗學報》，第 102 期，2012 年 12 月，頁 70。

2　「資訊戰」乃是危機和衝突時期針對敵方達成「資訊作戰」的特定目的，因而「資訊戰」是「資訊作戰」的一部分。呂爾浩、魏澤民，〈中國「資訊作戰」的類型分析〉《遠景基金會季刊》，第 7 卷第 3 期，2006 年 7 月，頁 190。

(Information Revolution Age)而誕生。[3]最早名詞是由1976年馬歇爾(Andy Marshall)團隊所領導軍事研究小組所提出，其要義在確保資訊優勢。[4]此資訊革命不僅影響社會變遷，也提升國家的競爭力，更帶動新戰爭思維，[5]本文先從美國學者李比奇對「資訊戰」的定義實施論述，概區分為「軍事」與「非軍事」兩個層次，意指「指管戰、情報偵蒐戰、電子戰」(軍事)與「心理戰、駭客戰、網路戰、經濟資訊戰」(非軍事)等7項。[6]從李比奇所定義的資訊戰可見，多屬於國家層次，其影響與衝擊層面相當廣泛。

事實上，可從表1針對美、臺、中、俄等國之資訊戰定義發現，多數國家在資訊戰的運用，多以侷限在作戰時期的應用，主要在於資訊環境下的攻防作戰，較屬於軍事層次，相對應用層次較為狹隘。以下就資訊戰提出比較分析(如表1)。

從上述各國定義比較得知，發現俄羅斯與中共的資訊戰(信息戰)更為主動，且採國家資助方式，成為戰爭主要戰略手段，易使傳統作戰方式逐漸成為輔助角色。

(二)俄羅斯資訊戰

俄羅斯資訊戰是源自於「spetspropaganda」(特殊宣傳)，為格拉西莫夫準則的一環，[7]它也是全球首先以資訊戰達到政治目標的國家。敘述俄羅斯對此戰法的廣用，可追朔至2009年喬治亞戰役後，因俄軍發覺在戰場上若改以負面方

3 同註2，頁189。

4 方鵬程，〈從福克蘭戰役到2003年波灣戰爭：公關化戰爭的發展歷程〉《復興崗學報》，第92期，民國97年12月，頁254。

5 「資訊」和「信息」均從英文的Information而來的，兩詞本義相同。

6 「資訊戰」定義：一為「指管戰」(Control Command and Warfare, C2W)，強調指揮中心利用先進電子通訊系統整合三軍作戰，而打擊目標亦為對方指揮中心，癱瘓指揮中心瓦解敵軍；二為「情報偵蒐戰」(Intelligence-based Warfare, IBW)，其中「攻擊的情報戰」為蒐集、偵測、分發與運用情報，在作戰中對敵方目標進行實體破壞；而「防衛的情報戰」在於加強或保持在戰場上的隱蔽性，以避免被敵方偵測發現；三為「電子戰」(Electronic War, EW)，以各種電子反制裝備干擾敵軍雷達和通訊；四為「心理戰」(Psychological Warfare, PSYW)，使用資訊對付敵方國家社會意志、部隊、指揮官，如運用電子媒體傳送有利於己方的資訊，以影響敵方意志；五為「駭客戰」和「網路戰」(Hacker War and Cyber-war)，網路入侵和資訊恐怖活動；六為「經濟資訊戰」」(Economic Information Warfare)，透過資訊誤導破壞敵國經濟。同註2，頁192。

7 2013年2月，俄羅斯總參謀長格拉西莫夫(Valery Gerasimov)撰寫〈科學價值在於前瞻〉一文，內容描述21世紀的戰場充滿各種新式戰力與戰爭運用方式，超越當代軍力的各種定義和用法。爾後西方世界針對格拉西莫夫論述，定名為「格拉西莫夫準則」(Gerasimov Doctrine)的探討，通常置重點於其理念究竟代表著戰爭的舊方法或新方法，以及格拉西莫夫是否想要提出俄羅斯在21世紀的特有戰爭形式。

表1　各國「資訊戰」定義比較分析

定義	美國	我國	中共	俄羅斯
作者	美國國防部 次長沛吉	國軍資訊戰 要綱	中共解放軍軍語辭典	俄羅斯 國防部
年別	1995	2004	1997	2000
內容	為獲得國家軍事戰略所需之資訊優勢，藉由各種手段以癱瘓對方的資訊系統與情報作業能力之外，更應妥善採取防禦與反制措施以鞏固其情報作業能力與資訊系統之安全。	廣義：運用各種手段影響敵方並防護我方決策程序與資訊系統之行動，以創造資訊優勢。 狹義：運用資訊科技影響敵方並防護我方指管程序與資訊系統之行動，以獲取戰場資訊優勢，本要綱所指資訊戰係以此定義為主。	敵對雙方在信息領域的對抗活動。主要是通過爭奪信息資源，掌握信息的生產、傳遞、處理等的主動權，破壞敵方信息傳輸，為遏制或打贏戰爭創造有利的條件。	兩個或多個國家之間的對抗以破壞信息為目的的信息空間信息系統流程和資源、關鍵和其他結構，破壞了政治、經濟和社會體系，對人口進行心理干預以破壞國家、社會穩定，以及強迫國家為利益做出決定對抗力量。
資助	軍事機構	軍事機構	國家組織	國家組織
運用時間	危機或衝突期間	危機或衝突期間	不分平時與戰時	不分平時與戰時
任務	輔助	輔助	輔助	主要
目標	在於以最小成本，來達致對敵人最大的破壞力。			

參考資料：1. 廖宏祥，〈資訊戰國家戰略〉《新世紀智庫論壇第 23 期》，2003 年 9 月 30 日，頁 105。
2.〈論恐怖主義可能實施的資訊戰及其反制措施〉《第二屆恐怖主義與國家安全學術研討暨實務座談會論文集》，頁 167。
3.Daniel E. Magsig 著，國防部史政編譯局譯，〈資訊時代的資訊戰〉《資訊作戰譯文彙集 I》(臺北：國防部史政編譯局，1997 年)，頁 250、251。
4. 呂爾浩、魏澤民，〈中國「資訊作戰」的類型分析〉《遠景基金會季刊》，第 7 卷第 3 期 2006 年 7 月，頁 207。
5. 2000/9/9."Ministry of Defence of the Russian Federation,"Russian Federation Armed Forces' Information Space Activities Concept.<https://eng.mil.ru/en/science/publications/more.htm?id=10845074@cmsArticle >.

式傳播，成效原比正向較佳，繼而改變作戰型態。

因此開始執行負面操作，主要以「訊息操縱」手段為主，試圖運用社群媒體對內(外)，散播具爭議性與情緒性議題，控制民眾輿論導向與行為態度，漸以產生社會極度對立氛圍。[8] 上述行為是在謀劃引發民眾爭戰，將百姓牽扯至衝突當中；因此，社會分歧越嚴重越亂的國家，所展現的效果將會越佳。此外，從拉脫維亞分析家賈尼斯・貝爾津斯(Janis Berzins)觀點認為，俄羅斯已逐漸轉變戰爭焦點，從

8　〈資訊戰中俄大不同：俄國快攻如暴風，中國布局如氣候變遷〉《臺灣事實查核中心》https://tfc-taiwan.org.tw/articles/2580，檢索日期：2020 年 5 月 16 日。

原先直接破壞轉化成直接影響，從武器和科技戰爭轉變為資訊戰，且更強調「人的思想」目標。[9]

不僅如此，從俄羅斯《軍事科學院公報》(Bulletin of the Academy of Military Sciences)報告中顯示：「受害國甚至不懷疑自己受到了資訊—心理影響。反過來導致了一個悖論：侵略者受影響國家人民的積極支持」。這顯示資訊戰可控制「人民的意志」。行動中更強調於「布局」，僅能透過長期性偽身至社群媒體之中，以獲取支持者的信任感，才是最完善的整備。因此，需要極大耐心等待引爆時機。

二、「社群媒體」與資訊戰之關聯性

現今社群媒體足以影響與介入民眾生活領域，例如像LinkedIn、Twitter、FB、IG、Snapchat以及新聞、廣播網站(包含傳統媒體)等，它提供民眾各議題的互動場域，同時也給予便利性及傳播性。因而，易引發政治渲染、民運動員與社會運動等情事。舉例來說，1.政治方面：2010年的阿拉伯之春(the Arab Spring)，2.經濟方面：2011年的西班牙「憤怒者運動」(Spanish Indignado)，3.災難方面：2019年的武漢肺炎(COVID-19)等等，以上均有媒體渲染蹤跡，引發各界關注漸漸成為討論議題。

資訊戰的運用可依循前文所敘述的特性實施，藉由龐大訊息、迅速傳播、網絡密切和難以辨識等特點，透過心理操控(psychological operations)，以實現國家戰略利益訴求。且根據美國外交政策研究所研究員華茲(Clint Watts)在美國參議院司法委員會(United States Senate Committee on the Judiciary)的發表指出，全方位的社群媒體須具備5項功能「偵查、集結、配置、宣傳與普及」。[10]而上述傳播方法使大眾可接受與自我立場相同政策，因而建立起對意見分歧者的對抗與偏見，進以產生的反饋機制，以期執行績效控制(如圖1)。[11]

如今，資訊戰最常運用方式則以假訊息與假新聞最多，因網路難以追尋與難辨真偽，且成本較為低廉，以致常遭部分國家與組織慣用，且有不斷增長趨勢。從

9 「寰宇韜略」俄羅斯以資訊戰回應現代戰爭改變(下)〈青年日報〉，https://www.ydn.com.tw/News/267292，檢索日期：2020年5月15日。

10 社群媒體需具備五項功能「偵查、集結、配置、宣傳與普及」：1. 偵查：先搜尋在社群媒體中那些人群是目標群眾。2. 集結：意指社群媒體平台。3. 配置：將一些議題藉假新聞刊登，使人信以為真。以現代運用上到主流網站中，持續擴大陰謀論和假訊息的論述。4. 宣傳：社群媒體將假議題迅速地傳播，再利用bots軟體帶動輿論風向。5. 普及：社群媒體的網路連結性，有利於滲透到多種形態的媒體中增添可信度。

11 「DQ小隊長學習日記」假訊息、資訊戰是什麼？可以吃嗎？〈DQ地球圖輯〉，https://dq.yam.com/post.php?id=11842，檢索日期：2020年5月17日。

數據調查顯示，使用國家從2017年28國、2018年48國，而至2019年已竄升到70國，由此可看出正成長趨勢；其中俄羅斯、中共、印度、伊朗、巴基斯坦、沙烏地阿拉伯、委內瑞拉等國家，不僅在國內政治宣傳和攻擊政敵，更將觸角「伸向國際」，影響其他民主國家的選舉。[12]

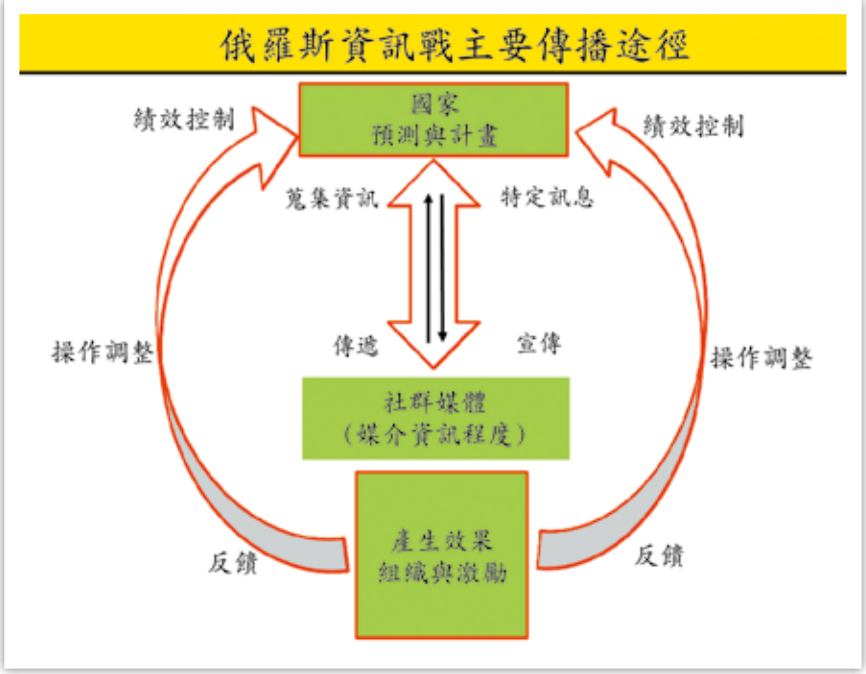

圖1　社群媒體與資訊戰之關聯性

資料來源：作者自製。

三、俄羅斯資訊戰發展趨勢

在冷戰時期原蘇聯就已具備資訊宣傳戰能力。可從1983年「感染行動」(Operation Infektion)中得知，當時蘇聯以捏造一篇虛構文章投書，指稱愛滋病(AIDS)是由美國所研發之生化武器，此事件嚴重創傷美國形象，產生後續輿論影響，證明蘇聯那時已具備資訊宣傳的能量。

但在蘇聯解體後，此警訊並未受重視，因是時的俄羅斯在經濟或軍事上，均無法與美國或北約抗衡，因而遭政府漠視。但自從1999年普丁(Vladimir Putin)執政後，開始轉變逐漸重視起媒體傳播，先對媒體立法、版圖分配、職能角色以及民眾意識形態等政策執行改革，賦予戰略目標與理念，重新塑立在蘇聯時期的「現實重塑戰術」(reality-reinventing tactics)，且此次改革更加先進及有效率。[13]

不僅如此，2005年俄羅斯政府便出資整併國營俄新社(RIA Novosti, RIA)與俄羅斯之聲(Voice of Russia,VOR)，2014年間轉型成為「今日俄羅斯」通訊社(Russia Segodnya)，[14]且任命親信基謝廖

12　「全球資訊戰」善用平台操弄民意、精準分眾影響外國選舉牛津大學專家：中、俄是製造假訊息「超級強國」！〉《風傳媒》，https://www.storm.mg/article/1933443，檢索日期：2020年5月19日。

13　〈聚焦—俄羅斯信息戰工具及手段〉《每日頭條》，https://kknews.cc/world/q48k2e8.html，檢索日期：2020年7月13日。

14　於下頁。

夫(Dmitry Kiselyov)為總編輯。[15] 此時期雇用大批網路「小白」，且設置數以千計的社群媒體「機器人」，意圖占領西方媒體評論版面、留言板與網路論壇為政府發聲。[16]

除了上述外，更於2014年4月在聖彼得堡設置「網際網路研究機構」(Internet Research Agency, IRA)又被稱之「巨魔農場」(Troll Farm)，[17] 後續更成立「翻譯者計畫」(Translor Streams)，[18] 此時的組織分工已相當明確，主以對美國群眾及社群媒體平台(諸如YouTube、Twitter、FB及Instagram等)執行假訊息行動，[19] 迄今仍持續在裂解北約與介入各國選舉。另外，2017年7月起，更不斷擴充武裝力量至190.3萬人，此次擴軍重點為強化資訊戰部隊，其目的就在於保護國防利益與參與現代化的網路資訊戰。[20]

況且，俄羅斯政府每年更花費13億美元經營社群媒體，對少數人實施「感染」任務，製造西方社會分化、介入各式選舉，甚至針對種族、暴力、同婚與

14 2012年，普丁再任總統，將所有中央媒體整合成國家媒體，命名為「RossiyaSegodnya」，(俄語中譯為今日俄羅斯)。與今日俄羅斯電視台「Russia Today」不同，「Russia Today」是外宣電視台。參考〈橙友圈—呂寧思：真實的俄羅斯媒體生態：自由，但受到有效管控〉《每日頭條》，https://kknews.cc/world/9oky84l.html，檢索日期：2020年5月213日。

15 Chris Collison, 2017/05. "Russia's Information War:Old Strategies, New Tools,"Working Drft, pp.18,<https://jsis.washington.edu/ellisoncenter/wp-content/uploads/sites/13/2017/05/collison_chris_Russia%E2%80%99s-Information-War-Old-Strategies-New-Tools-How-Russia-Built-an-Information-Warfare-Strategy.pdf>.

16 羅世宏，〈關於「假新聞」的批判思考：老問題、新挑戰與可能的多重解方〉《資訊社會研究》，第35期，(2018)，頁66。

17 「巨魔農場」，指利用網路散播仇恨的人或組織，進行宣傳和虛假信息，常見方式包括應用假新聞、假帳戶去做煽動性的言論，製造族群間的不信任和衝突。參考〈【川普當選是個假民主？】臉書證實俄羅斯花300萬廣告費散播假新聞，挑動對立讓川普上台〉《Tech Orange》，https://buzzorange.com/techorange/2017/09/07/russia-buy-facebook-ad/，檢索日期：2020年2月25日。

18 Chris Collison, 2017/05. "Russia's Information War:Old Strategies, New Tools," Working Drft, pp28,<https://jsis.washington.edu/ellisoncenter/wp-content/uploads/sites/13/2017/05/collison_chris_Russia%E2%80%99s-Information-War-Old-Strategies-New-Tools-How-Russia-Built-an-Information-Warfare-Strategy.pdf>.

19 〈當巨魔遇上小精靈：俄羅斯假訊息轟炸下的波羅的海〉《OCF Lab》，https://lab.ocf.tw/2019/06/24/%E7%95%B6%E5%B7%A8%E9%AD%94%E9%81%87%E4%B8%8A%E5%B0%8F%E7%B2%BE%E9%9D%88%EF%BC%9A%E4%BF%84%E7%BE%85%E6%96%AF%E5%81%87%E8%A8%8A%E6%81%AF%E8%BD%9F%E7%82%B8%E4%B8%8B%E7%9A%84%E6%B3%A2%E7%BE%85%E7%9A%84/，檢索日期：2020年6月15日。

20 〈俄羅斯新一代"網軍"公開亮相戰力幾何？〉《中國軍網》，https://hackmd.io/@billy3321/BkLG2lKY4/%2Fs%2FB1BeDC_tE?type=book，檢索日期：2020年6月18日。

移民等議題，目前已造成多國利益損失，且傷害並不亞於發動一場戰爭。因此，美軍也開始評估盟友與潛在敵手在資訊戰能力，發現俄羅斯在各項評選項次之中，已成為全球資訊戰的佼佼者(如表2)。

除上述之外，也須闡述俄羅斯資訊戰的傳播途徑與層面，大致可分為6大步驟：1.操控社群媒體假帳號(由國營附屬媒體，創建虛假或誤導性內容)→2.不斷擴大散播聳動不實消息(例如巨魔和機器人)→3.製造關鍵意見領袖、圈粉(帶風向)→4.吸引真正意見領袖加入→5.助推正、反兩面同溫層朝極端立場→6.製造對立，以達到政治效應。[21] 以上途徑與影響層面都將造成社會認知轉變，下述則依據各學者對於傳播作法及影響目的實施概述。

(一)俄國資訊戰的分析師尼莫(Ben Nimmo)指出，當代俄羅斯繼承蘇聯「假資訊」戰術，在輿論戰採取「4D」戰術，亦即駁斥(Dismiss)、曲解(Distort)、轉移注意(Distract)及震懾受眾(Dismay)。例如：以宣傳手法通過巨魔農場和殭屍(bots)進行挑撥離間、[22] 傳播恐懼、影響信仰或破壞社會規則，減少對目標國政府

表2　美軍評估盟友、潛在敵手在資訊戰能力

項次	比較項目	比較強者(國家)
1	媒體關係、媒體戰、公共關係、政府宣導	德國、俄羅斯、中共
2	資訊影響力	中共、俄羅斯
3	行動號召力	北韓、俄羅斯
4	欺騙、詭道、操弄	中共、俄羅斯
5	電磁頻譜戰、電子戰、干擾	以色列、德國、中共與俄羅斯
6	網路戰	以色列、中共、北韓、伊朗與俄羅斯
7	作戰安全、保密、阻斷、資訊安全	德國、中共和北韓
8	審查、資訊控制	中共、北韓與俄羅斯
9	以演習等實際作為傳達資訊	中共、俄羅斯
10	資訊相關能力的外包、代理人或民兵的使用、賦予特許權	中共、伊朗、俄羅斯
11	運用社群媒體、新媒體、今媒體	德國、中共、俄羅斯

參考資料：〈鄭智懷，【寰宇韜略】美取經資訊環境作戰—加強防禦力(上)〉《青年日報》，https://www.ydn.com.tw/News/330741，檢索日期：2020年6月11日。

21　〈瑞典專家：資訊戰是極權國家新武器〉《大紀元》，https://www.epochtimes.com.tw/n293399/%E7%91%9E%E5%85%B8%E5%B0%88%E5%AE%B6-%E8%B3%87%E8%A8%8A%E6%88%B0%E6%98%AF%E6%A5%B5%E6%AC%8A%E5%9C%8B%E5%AE%B6%E6%96%B0%E6%AD%A6%E5%99%A8-.html，檢索日期：2020年6月24日。

22　於下頁。

的信任，而掌握輿論主動權。

(二)分析家費登(Oliver Fitton)認為，網路空間和社群媒體的種種作為，難以明確歸究於俄羅斯所採取之手段。因此，使俄羅斯可以否認涉入政治宣傳行動。

(三)學者亞羅(Jes- sikkaAro)提到俄羅斯資訊作戰中，包含政府聘用的評論家，專責於社群媒體中散布宣傳假新聞與親俄的訊息，達到混淆閱聽或親俄資訊之目的。[23]

綜上述所言，社交媒體是俄羅斯施展資訊戰的重要領域，且外界解讀普丁上述行為，主要將所有媒體都受控於克林姆宮內，利於掌握資訊核心，執行戰略目的。再者，根據社群媒體(Facebook)在2019初至10月3日期間，發布18篇新聞稿指出，調查22個國家中，察覺俄羅斯政府是最常以國家機器來攻擊其他國家之一。[24]因此，筆者希藉由2014年俄羅斯攻擊克里米亞事件，闡述如何運用社交媒體實施作戰，進行敘述性剖析，證明資訊戰的重要性。

俄羅斯資訊戰在克里米亞的運用

在顏色革命(Color Revolution)的威脅下，推翻了烏克蘭的親俄政府，促使普丁逐步對2014年烏克蘭危機做出反應。最終，俄羅斯僅以短短13日就入侵東烏克蘭，使所有人都措手不及，可堪稱為當代資訊戰的最佳範例。

一、克里米亞

克里米亞位在烏克蘭南部(俄羅斯西南部)，陸地面積2.55萬平方公里(約臺灣的三分之二)，其地理位置瀕臨黑海和亞速海，領土深入黑海的半島，且位處黑海的航道上，致使成為環繞黑海諸國的必爭之地。再者，克里米亞陸地僅一邊(左半部)與烏克蘭相連，只要網路交換點(Internet Exchange Point, IXP)慘遭損壞或關閉，資訊就將遭受俄羅斯所控制。

二、戰前情勢

22 「bot」一詞是「robot」這個單詞的簡寫，意思就是機器人。bot 指的是特殊的電腦程式，也就是所謂的軟體機器人。軟體機器人甚至可能隱身於像是 Facebook、Twitter 之類的社群網路的假帳號 (fake account) 背後；人們則稱此為「社交機器人」(social bot)。這些機器人的帳號有時會附有個人的照片與虛構的自傳。參考資料〈戰爭的開始，常源於假新聞：有圖沒真相的年代，如何避免被操弄？〉《報導者》，https://www.twreporter.org/a/bookreview-nachgefragt-medienkompetenz-in-zeiten-von-fake-news，檢索日期：2020年6月25日。

23 Scott J. Harr、譯者黃文啟，〈定義新型態俄式資訊作戰〉《國防譯粹》，第45卷第2期，2018年4月，頁83。

24 019事實查核工作坊／高雄場報導四：網軍假新聞操弄民意三大社群媒體防禦作戰，〈臺灣事實查核中心〉，https://tfc-taiwan.org.tw/articles/1626，檢索日期：2020年6月29日。

2013年11月間，親歐派要求強化與歐盟正式合作關係，簽訂「歐盟協會協議」(EU Association Agreement)，而親俄派則堅持向俄羅斯靠攏，接受普丁總統150億美元的長期經援及天然氣與石油能源優惠援助。[25] 國內派系也因此政策問題，在首都基輔(Kiev)「獨立廣場」發生武力抗爭及衝突。當月下旬，俄羅斯的駭客組織已開始對批評亞努科維奇政府與親歐網站發動攻勢，此暴動持續至2014年1月還未能結束。[26]

2014年1月17日，烏克蘭議會通過「反示威法」，該法煽動歐盟以及美國進行更嚴厲抗議與國際譴責，此舉更引發反政府民眾的不滿，以致暴動持續發散。[27] 直至2月20日親俄派亞努科維奇(Yanukovych)總統下令暴力鎮壓，最終造成77人死亡，600多人受傷。此刻在國會占多數的親歐派於次日(21)就迅速通過總統彈劾案，總統因此流亡至俄羅斯。而烏克蘭東部、南部地區居民則開始抗議基輔的新政權，當基輔政情快速惡化時，莫斯科立即採取急速又具體的軍事部署及政治行動(如圖2)。

三、作戰經過

事實上，俄羅斯早在烏克蘭危機爆發衝突前，就做足資訊戰整備，以代號「反身控制」(Reflexive Control)，[28] 是為混合戰(hybrid warfare)的要項之一。其中包括大規模軍事演習、建立外語新聞媒體、運用社群網站與派遣特種部隊等「軍事」與「非軍事」行動，實施作戰攻勢；其整體經過概分為「初期、關鍵期、後期」等。

(一)作戰「初期」——奪取資訊與政治優勢

俄羅斯初期完成外交、政治與作戰整備，先以外交攻勢取得各國支持，企圖阻止俄羅斯鄰國(波羅的海國家，格魯吉亞和烏克蘭，以及以前的波蘭、捷克共和國和斯洛伐克)進入親西方之路。阻絕西歐國家和美國的武力介入，然後採取多重作為，以網路攻擊控制敵方境內各資訊與媒體設施，奪取輿論主導權，便以求得在烏克蘭的軍事行動成功。

1.外交媒體攻勢——戰略(外交)整備

25 2014/1/22. "Ukraine Protests: Two Protesters Killed in Kiev Clashes," BBC News, < http://www.bbc.com/ news / world-europe-25838962>.

26 顏建發，〈烏克蘭危機與中國的戰略處境與選擇〉《臺灣國際研究季刊》，第 11 卷第 2 期，2015 年 (夏季號)，頁 53。

27 同註 26。

28 「反身控制」(Reflexive Control) 意指依賴以俄羅斯能力，先期掌控散布在敵境內的各種設施，再以選擇最有利的行動方案。

圖2　烏俄衝突地區

資料來源：作者自行繪製。
〈這一仗，普丁兵不血刃，所用新戰法讓西方國家意想不到〉，《每日頭條》，https://kknews.cc/world/vov8kkl.html，檢索日期：2020 年 6 月 9 日。

俄羅斯初期除在烏克蘭境內進行媒體傳播外，還利用國家資源對國際社會進行宣傳：如電視節目宣揚、大量親俄網路評論員。以建構出虛假與欺騙氛圍，分散國際對此議題的注意，阻止國際對烏克蘭危機作出反應。再者，俄羅斯長期對烏克蘭提供「人道主義」外交政策，其實是在增加烏克蘭公民對俄語的使用率，以及認同俄羅斯文化，舉例如下：1.提供俄語學校資金。2.支持親俄的文化中心與非政府組織(Non-Governmental Organization, NGOs)。便於後續對烏克蘭公民(尤其是東部居民)實施媒體宣傳。

除此，俄羅斯也採取有計畫、有組織地「主動」宣傳，獲取國內(外)支持，反制西方輿論戰，且不停誇大烏克蘭境內的俄裔將面臨危害，以及營造出俄、烏人民支持克里米亞加入俄羅斯的假象。接續善用高層會晤、雙邊及多邊磋商，尋求戰略上的主動。同時對西方國家進行對外軍事行動「正名」，以獲取國際支持。且普丁不斷在國際媒體上虛假陳述外交策略，否認對克里米亞的干預，[29] 進而使人民產生矛盾錯覺。

2.親俄政黨——政治整備

烏克蘭及各國親俄政客平時已與莫斯科有聯繫與互動，親俄政黨在烏克蘭局勢動盪中，發揮極大作用，因政治人物都受制於克里姆林控制，在聯合國或國內會議中均公開支持俄羅斯之行動；且在經由俄羅斯國營的社群媒體，採取重複性的渲

29　李俊毅、江雅綺，〈從俄羅斯對烏克蘭的混合戰－談臺灣國家安全問題的新考驗〉《思想坦克》，https://www.voicettank.org/single-post/2019/05/20/052002，檢索日期：2020 年 7 月 10 日。

染報導，讓各國對於俄羅斯的行動感到迷惑。[30]

3.俄羅斯和分裂主義的社群媒體——作戰整備

俄羅斯於作戰初期已對烏克蘭與西方國家的網絡與通信進行高強度網路攻擊(惡意軟體如Snake、Uroboros或Turla)，竊取克里米亞內部資訊，藉此研判及推測烏克蘭政府後續發展及整體局勢。另外，俄羅斯也趁機利用高科技通訊技術進行烏克蘭東部干擾，使東部人民僅能收視俄羅斯電視台。再以官媒《今日俄羅斯》(RossiyaToday, RT)成立親俄立場的新聞網站(Ukraine.ru)散播假訊息，並由巨魔農廠(聖彼得堡、彼得斯堡、愛沙尼亞和拉脫維亞等地)創設無數殭屍帳號，[31]更模仿烏克蘭新聞網站和YouTube的帳戶，例如虛假的《今日烏克蘭》帳號，重複撰擬虛假故事或克里姆林宮的重要談話。[32]由中央媒體(RT、PervyyKanal、Rossiya 1、Rossiya 2、NTV、LifeNews)擷取篩選出烏克蘭政府負面訊息，投放海量假新聞、民調與訊息，亦影響民眾的認知與行為，[33]為下一階段奠定基礎。以下為假新聞案例說明：

(1)俄羅斯雇用部落客(Blogger)建立多人帳戶，針對各網站發表利於俄羅斯或不利於烏克蘭之評論。根據數據顯示每12小時對新聞和社交媒體進行約126次評論。例如2014年2月，「歐亞青年聯盟」(Eurasian Youth Union)網站發布部落格文章，呼籲志願者在烏克蘭的頓巴斯捍衛俄國人：「我們可以幫助他們！準備幫助烏克蘭人的每個人，我們請您聯繫與我們的協調員一起採取進一步行動。」[34]

(2)親俄網絡在2014年2月間不斷散布描繪逃離烏克蘭前往俄羅斯的難民專欄的圖像。實際上，圖像只是烏克蘭和波蘭間

30 Igor Kopotin, KristiinaMuur, Vladimir Sazonov, 2017/8. "Methods And Tools Of Russian Information Operations Used Against Ukrainian Armed Forces:The Assessments Of Ukrainian Experts", KaitsevaeAkadeemia,Vol. 6, p.59.

31 Margarita Jaitner, Peter &Mattsson, 2015/5, "Russian Information Warfare of 2014", NATO CCD COE Publications, p.43.

32 Chris Collison, 2017/05 "Russia's Information War:Old Strategies, New Tools," Working Drft, pp.28,<https://jsis.washington.edu/ellisoncenter/wp-content/uploads/sites/13/2017/05/collison_chris_Russia%E2%80%99s-Information-War-Old-Strategies-New-Tools-How-Russia-Built-an-Information-Warfare-Strategy.pdf>.

33 「魯斯濱」解析俄軍資訊戰—給臺灣的啟示〉《報呱》，https://www.pourquoi.tw/2019/11/11/russian-sixth-generation-warfare/，檢索日期：2020年7月13日。

34 Chris Collison, 2017/05 "Russia's Information War:Old Strategies, New Tools," Working Drft, pp11.,<https://jsis.washington.edu/ellisoncenter/wp-content/uploads/sites/13/2017/05/collison_chris_Russia%E2%80%99s-Information-War-Old-Strategies-New-Tools-How-Russia-Built-an-Information-Warfare-Strategy.pdf>.

的交通擁擠路線。卻藉以誤導烏克蘭公民、新聞工作者和其他圍觀者誤以為難民潮。

(3)《Ukrainskaya Pravda 》網站是親俄的烏克蘭新聞網站。宣傳資料會傳達有關實際事件的虛假敘述，例如否認俄羅斯軍方存在於烏克蘭內部。外交部長拉夫羅夫(Sergei Lavrov)一再堅持，莫斯科將避免干預烏克蘭的國內危機，並敦促其他國家也這樣做，[35] 以及報導克里米亞歡迎俄羅斯軍人的場景。[36]

(4)《俄羅斯今日報》是俄羅斯政府資助的多語種新聞網站，針對全球視角傳播俄羅斯的虛假信息和宣傳而聞名。[37]

(5)Cyber Berkut駭客組織對烏克蘭和北約各網頁進行DDoS(分散式阻斷服務攻擊)攻擊和破壞，其中有35次遭受攔截，但也從中獲取烏克蘭軍事合作文件。[38]

由前述各項事實得知，俄羅斯主要以將西方與烏克蘭國內親歐勢力妖魔化，同時也在降低當地政府士氣，且動員相關支持者，使烏克蘭國內民眾陷於恐懼、徬徨與疑惑當中。而在柔性上主要藉訊息將訴求傳達給當地居民了解，強調文化、語言和意識形態上的相同性，可說是對烏的兩手策略。

此外，俄羅斯也會篡改圖像傳播至網路媒體，以建構烏克蘭政府恢復納粹主義的假象，將訊息和過去歷史作為連結，喚起烏克蘭和波羅的海，曾在衛國戰爭(ОтечественнаяВойна)所經歷的納粹暴政時期，以及紅軍入侵的回憶。上述之策略，可使部分歐洲國家為納粹歷史而起義，進而疏遠烏克蘭，具有強烈啟發性(如表3)。

(二)作戰「關鍵期」——確立軍事優勢

2014年2月20日，俄羅斯特種部隊(Spetsnaz)就已秘密滲透至克里米亞境內，潛入期間更利用普丁在烏克蘭東部大規模軍事演習驟然襲擊(如圖3)，[39] 採兵分兩路向雅爾達(Yalta)與辛菲洛普(Simferopol)取攻勢，並與當地支俄力量合作，促使破壞及占領克里米亞境內資訊與通信平台，再運用媒體戰與心理戰以策反烏克蘭官兵，加劇克里米亞緊張

35 Sergei L. Loiko& Carol J. Williams. 2014/2. "Crimean airspace closed after Russian transports reportedly land", <https://www.mcall.com/la-fg-wn-ukraine-russia-crimea-military-movements-20140228-story.html>.

36 Vitaly Shevchenko. 2014/11. "Little green men" or "Russian invaders"?", BBC News,<https://www.bbc.com/news/world-europe-26532154>.

37 鄧炘傑，〈資訊時代的資訊戰〉《陸軍學術月刊》，第 55 卷第 568 期，2019 年 12 月，頁 108、109。

38 Michael S. Rogers,2015. "A Challenge for the Military Cyber Workforce," Military Cyber Affairs, Vol. 1,pp. 5.

39 高英茂，〈俄國兼併克里米亞的國際政治及意涵〉《臺灣國際研究季刊》，第 11 卷第 2 期，2015 ／夏季號，頁 179。

表3　俄羅斯對烏克蘭(克里米亞)—作戰「初期」階段

階段	事件內容	資訊戰						
		指管戰	情報偵蒐戰	電子戰	心理戰	駭客戰	經濟資訊戰	網路戰
戰略整備(外交)	1.尋找烏克蘭政府的脆弱點，也就是「經濟和國防力量」。 2.建立親俄的非政府組織和媒體管道(RT和Sputnik)，以網路對應烏克蘭。 3.建立外交和媒體職位，以便影響國際觀眾。		√		√	√	√	√
政治整備	1.鼓動對烏克蘭中央政府不滿，藉由特殊行動和媒體工具等手段，以影響政治，外交行為。 2.加強當地分離主義運動，並加強種族、宗教和社會緊張局勢。 3.積極對烏克蘭國家與政府採取資訊措施。 4.賄賂國家之政客、行政官員和軍隊，將以策反。 5.與當地寡頭和商人建立聯繫，製造合同關係藉以攻擊烏克蘭。 6.與當地犯罪集團建立聯繫管道。		√		√		√	√
作戰整備	1.一致性發動政治壓力和虛假訊息與新聞等行動。 2.動員已策反的政府官員與當地犯罪集團。 3.藉由大規模軍事演習，動員俄羅斯武裝力量。	√	√	√	√	√		√

參考資料：TarasKuzio&Paul D. 2018/6/25,"Anieri,Annexation and Hybrid Warfare in Crimea and Eastern Ukraine",E-International Relations,pp.8-11,<https://www.e-ir.info/2018/06/25/annexation-and-hybrid-warfare-in-crimea-and-eastern-ukraine/>

資料說明：作戰「初期」可劃分為三個階段「戰略(外交)整備、政治整備、作戰整備」等，可從以上12點敘述發現在不同階段都運用資訊戰，且與美國學者李比奇所定義資訊戰中軍事及非軍事相互運用。

局勢。[40]

下述為特種部隊在2月下旬至3月初期間，對於克里米亞地區之軍事(基礎)設施及軍事行動之作為。

1.在2月26日煽動克里米亞群眾示威遊行，奪取辛菲羅波爾的行政大樓(議會、政府大樓)，28日迅速占領具有戰略意義的佩雷科普・伊斯姆斯(PerekopIstmus)，包含機場(辛菲羅波爾機場)、廣播電台及電視台。例如：突襲烏克蘭Ukrtelecom電信公司設施，使克里米亞無法與烏克蘭訊息交流。此外，烏克蘭安全服務官員的移動通信遭受IP電話攻擊，以及政府網站(World Wide Web)和新聞部遭受DDoS，造

40　Roger N. McDermott., 2015/4. "Brothers Disunited: Russia's Use of Military Power in Ukraine," The Foreign Military Studies Office, p.11,<https://community.apan.org/wg/tradoc-g2/fmso/m/fmso-monographs/197162>.

成72小時資訊中斷。[41]

2.在2月27日奪取克里米亞的指揮控制通信節點和防空部隊，以及3月3日封鎖克里米亞的各軍事基地(例如：巴爾貝克空軍基地)。

3.俄羅斯情報部門以運用親俄民眾與家人撥打電話給營區內官兵，採取親情對話攻勢，漸以策反烏克蘭官兵。例如：俄羅斯官方頻道撥放獲得俄羅斯國籍的Berkut軍官將在俄羅斯的某些地區提供職業機會。[42] 2014年3月2日烏克蘭海軍總司令貝雷佐夫斯基(烏克蘭語：ДенисВалентиновичБерезовський)少將叛變。

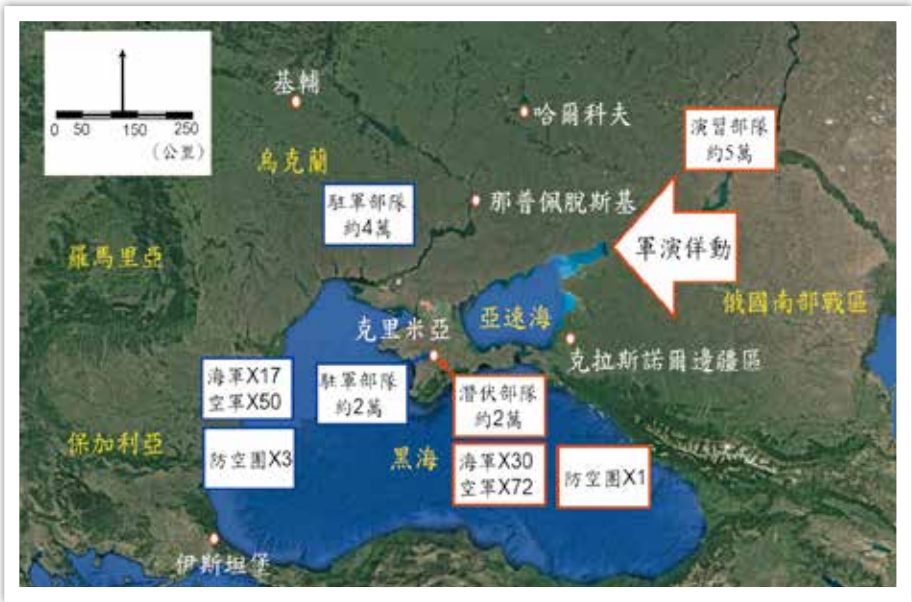

圖3　俄軍攻擊克里米亞作戰要圖

資料來源：作者自行繪製。〈這一仗，普丁兵不血刃，所用新戰法讓西方國家意想不到〉，《每日頭條》，https://kknews.cc/world/vov8kkl.html，檢索日期：2019年12月9日。

4.協同俄軍資訊作戰部門與媒體，傳播身著綠色服裝人士(小綠人)自發主動維持秩序的媒體訊息，在國際社會形成輿論優勢，並影響烏克蘭高層決策。

上述行動，使烏克蘭的俄語區與其他親俄地區都已遭社群媒體與小綠人影響，使克里米亞分歧更為兩極化，且對烏克蘭政府關係也更加惡化。2月27日俄羅斯武裝人員也幾乎解除烏克蘭軍隊武裝，完全控制克里米亞，並阻礙接連克里米亞至烏克蘭的交通要道，壟斷烏克蘭對內的資訊傳遞，此時響應愈加獲得人民力量的支持(如表4)。

(三)作戰「後期」——保持戰略優勢

2014年3月，俄羅斯議會批准總統普丁在烏克蘭使用武力，直至烏克蘭的社會政治情勢正常化為止，相繼烏克蘭海軍與空軍均遭受俄羅斯策反，同意支持克里米亞。後續俄羅斯總理梅德韋杰夫

41　Margarita Jaitner, 2015. "Russian Information Warfare: Lessons from Ukraine," CCDCOE, p. 91,<https://ccdcoe.org/uploads/2018/10/Ch10_CyberWarinPerspective_Jaitner.pdf>.

42　Soňa Rusnakova,2017/10/11. "Russian New Art of Hybrid Warfare in Ukraine," Slovak Journal of Political Sciences, Vol.17, No. 3, p.368.

表4　俄羅斯對烏克蘭(克里米亞)一作戰「關鍵期」階段

階段	事件內容	資訊戰						
		指管戰	情報偵蒐戰	電子戰	心理戰	駭客戰	經濟資訊戰	網路戰
加劇緊張局勢	1.製造烏克蘭國內大規模的反政府抗議活動和騷亂。 2.派遣第一批特種部隊滲透至克里米亞，偽裝成當地平民占領行政大樓目標區域（由本地官員和警察採取主動或被動方式支持），且與當地犯罪集團合作。 3.在克里米亞境內各地實施挑釁和破壞，轉移中央政府的注意力和資源。 4.攻擊烏克蘭的媒體，宣傳虛假訊息運動。 5.做好烏克蘭軍隊反擊之可行性，派遣俄羅斯正規軍實施邊境封鎖，施以常規性嚇阻。	√	√	√	√	√		√
從克里米亞獲取中央力量	1.占領行政大樓和當地區域的電信基礎設施。 2.阻止中央政府的媒體機制，建立溝通和訊息壟斷。 3.使非武裝國家的中央力量的當地武裝部隊失去能力方式，包括「封鎖營房、賄賂指揮官、破壞士氣等」（尤其是邊防人員）。 4.同時，襲擊的外交、媒體、經濟參與者和武裝部隊，使烏克蘭產生巨大壓力。俄羅斯媒體再試圖誤導和欺騙國際觀眾，並使烏克蘭蒙羞。	√	√		√	√		√

參考資料：TarasKuzio&Paul D. 2018/6/25."Anieri,Annexation and Hybrid Warfare in Crimea and Eastern Ukraine," E-International Relations,pp.8-11,<https://www.e-ir.info/2018/06/25/annexation-and-hybrid-warfare-in-crimea-and-eastern-ukraine/>.

資料說明：作戰「關鍵期」可劃分為兩個階段「加劇緊張局勢以及從克里米亞獲取中央力量」等，表上所列出之9點軍事及非軍事行動，都可看出美國學者李比奇對資訊戰定義中的運用。

(Dmitry Medvedev)宣布將給予克里米亞財政支援以及對烏克蘭的天然氣供應。11日議會通過獨立宣言，宣告為獨立主權國家。[43] 可見俄羅斯於後期保持戰略優勢，但未陷入戰爭泥沼之中。克里米亞自治議會和塞瓦斯托波爾市議會單方面宣布脫離烏克蘭，並就此議題進行了全民投票。16日，克里米亞約有150萬公民決定展開正式公投，[44] 根據克里米亞議會的決議，全民公投的問題只能在下列兩項選項擇一：

(1)是否贊成克里米亞再享有俄羅斯聯邦主體權利基礎上與俄羅斯重新合併？(Are you in favour of Crimea being reunited

43　洪泉湖、施正鋒、楊三億，〈當代歐洲民族運動：從蘇格蘭獨立公投到克里米亞危機〉(臺北：聯經出版公司)，2017年7月26日，頁114。

44　高英茂，〈俄國兼併克里米亞的國際政治及意涵〉《臺灣國際研究季刊》，第11卷第2期，2015年(夏季號)，頁178。

with Russia with the status of an entity of the Russian Federation?)

(2)是否贊成恢復克里米亞共和國1992年憲法，並贊成克里米亞或為烏克蘭一部分？(Are you in favour of the 1992 Constitution of the Republic of Crimea being restored, and of Crimea having the status of part of Ukraine?)[45]

其結果顯示約83%參加投票且絕大多數選民支持「脫烏入俄」(加入成為俄羅斯聯邦97.47%，留在烏克蘭2.53%，無效票0.71%)；[46] 17日普丁簽署命令承認克里米亞共和國成為主權國家。[47] 18日，普丁、克里米亞地方政府與塞瓦斯托波爾(Sevastopol)的領袖簽署條約，將克里米亞併入俄羅斯聯邦。21日，普丁簽署已獲俄羅斯國會上下兩院批准，使兩個地區正式加入俄羅斯聯邦。更在同年4月俄羅斯修憲，正式將克里米亞列為俄羅斯聯邦主體並寫入條文。雖然有其他國家質疑認公民投票的合法性，但克里米亞納入俄羅斯聯邦已是不爭的事實(如表5)。

由此觀之，俄羅斯充分運用資訊戰，考慮作戰地區民族關係、派系矛盾、社會熱點等問題，在敵、我、友與中間勢力中，尋找切入點與發力點，以爭取民眾支持，擴大烏克蘭內部爭議，使受侵略的受害者並不抗拒(例如克里米亞的情況)，且綜觀全程也被視為代理戰爭的衝突。

俄羅斯「資訊戰」之評析

從克里米亞事件中，可發掘俄羅斯資訊戰的多樣性，在衝突未發生之前，早已對烏克蘭展開資訊攻勢。「資訊戰」它是國家所主導的隱性角色，利用社群媒體的氾濫以及對此知識的缺乏和法律漏洞，營造出烏克蘭國內(外)的懷疑與不信任氛圍，以發揮對國內、區域甚至於全球的影響力，進而獲得戰略優勢。上述成功要素，主要還是須歸功於俄羅斯普丁現代化的宣傳工作，達成此任務必須依以下4個方向：

1.龐大的資訊宣傳預算支助。

2.克里姆林宮內所有社群媒體均採用現代化傳播機器。

3.克里姆林宮的資訊戰擁有專業技術，便於接觸更多的外國觀眾。

4.克里姆林宮利用西方媒體相對開放

45 施正鋒，〈烏克蘭的克里米亞課題〉《臺灣國際研究季刊》，第 11 卷第 2 期，2015 年 (夏季號)，頁 37。

46 〈2014 年克里米亞危機整理〉《公民行動》，https://www.civilmedia.tw/archives/27196，檢索日期：2020 年 6 月 21 日。

47 〈2014 年克里米亞歸屬公投〉《維基百科》，https://zh.wikipedia.org/wiki/2014%E5%B9%B4%E5%85%8B%E9%87%8C%E7%B1%B3%E4%BA%9E%E6%AD%B8%E5%B1%AC%E5%85%AC%E6%8A%95，檢索日期：2020 年 7 月 14 日。

表5　俄羅斯對烏克蘭(克里米亞)—作戰「後期」階段

階段	事件內容	資訊戰						
		指管戰	情報偵蒐戰	電子戰	心理戰	駭客戰	經濟資訊戰	網路戰
政治權力建立替代	1.占領行政當局宣布替代性的政治中心，指的是分裂主義的真實或虛構傳統。 2.以新的方式取代中央權力的行政機關建立政治機構，從而建立準合法性。 3.俄羅斯媒體加強新政治機構的合法性。 4.藉由訊息壟斷，疏遠克里米亞居民。 5.俄羅斯常規軍事持續不斷攻擊地區內之中央電源。	√	√		√			√
穩定結果政治	1.立即組織採取分裂國家/獨立國家的「公投」和決定，並獲得俄羅斯外交與媒體支持。 2.建立克里米亞向俄羅斯尋求幫助。				√			√
將克里米亞與烏克蘭隔開	1.俄羅斯吞併被占領領土（克里米亞）。 2.建立（公開或秘密）軍事存在，建立新政府並開始與烏克蘭中央政府對抗，繼續從政治、經濟和軍事上削弱東烏克蘭。 3.俄羅斯是以維持和平或危機管理為藉口的公開入侵。	√	√		√		√	√
限制烏克蘭戰略行動自由	1.領土的喪失（經濟、人口、基礎設施等）導致嚴重的經濟困境，國內政治動盪以及可能出現的嚴重人道主義局勢。 2.烏克蘭由於無法完全控制其領土，因此也無法要求領土完整的政治與軍事聯盟。				√		√	√

參考資料：TarasKuzio&Paul D. 2018/6/25."Anieri,Annexation and Hybrid Warfare in Crimea and Eastern Ukraine," E-International Relations,pp.8-11,<https://www.e-ir.info/2018/06/25/annexation-and-hybrid-warfare-in-crimea-and-eastern-ukraine/>.

資料說明：作戰「後期」可劃分為4個階段「建立替代政治權力、政治穩定結果、將克里米亞與烏克蘭隔開以及限制烏克蘭戰略行動自由」等，表上所列出之12點的行動中，在政局穩定後大概以「心理、經濟與政治」層面為主。

程度，執行俄羅斯宣傳攻勢。

除此之外，更從克里米亞吞併事件中，發現俄羅斯在軍事、外交及經濟等各體制上都充分運用社群媒體，不僅對國內(國際)的輿論影響、社會動員與情感傳播上都有「社群媒體」與「資訊戰」的影子。因此，筆者藉由美國學者李比奇所定義的「資訊戰」實施綜合性分析與論述。

(一)運用社群網路對國際影響

自從普丁執政後，藉由「愛國主義」和「管理式民主」之由，[48] 在短時間內投入大量國家資源，積極整合與升級原有舊媒體，包括傳播行為、過程、組織、

48　於下頁。

關係、功能與組件等改革，政府更挹注資金加以扶持。更在《大眾傳播媒體法》上逐步修法(1995年、1998年、2000年、2001年與2002年)，儘量利用司法綁住媒體進行控制，甚而對社群媒體執行嚴格的內容把關，奠定未來新聞傳播的法治基石。其中以第16條規定為最，即「可以停止媒體經營事業的權力」。從上述立法可見，俄羅斯正試圖從「自由化」逐漸轉向「國家化」，以掌控媒體傳播的主導權。[49]除此之外，更尋求最迅速的網路手段，反制國外媒體對俄羅斯的負面報導，且保證外交政策宣傳與克里姆林宮意圖一致，充分展現「社群媒體」在戰略的價值。

然而，在克里米亞事件中，發現衝突絕大部分都發生在社群媒體上，因為俄羅斯之任何軍事衝突，雙方都會耗盡相當大的軍事開支，因此在非傳統費用上特別給予花費。尤其是強烈利用社群媒體(電視，報紙和網路)作為操縱手段，主以宣傳、假信息、外交欺騙等，以影響各國、組織或者國際公眾。因此，在2013年11月至2013年12月31日「歐洲獨立廣場」抗議行動期間(EuroMaidan)，俄羅斯不斷藉由演講與新聞發布，適時扭曲敵對媒體的實際報導。且俄羅斯在外交政策上和價值觀均透過傳統報紙、廣播、有線電視、衛星電視以及新傳播媒體平台、網際網路、社群媒體等多元管道達到戰略溝通，而上述行為是具有高度的戰略價值。事實上，其結果也證實社群媒體發揮極致效能，因為隨著時間的流逝，各國決策者在觀念上都被影響，並未對俄羅斯採取積極性的行動方針，導致於後續發展。進言之，此種宣傳訊息的產製方式，就是採取不間斷方式渲染，藉由國內(外)媒體報導，進行引導國際輿論，占據國際話語權，以爭取國外支持，塑造俄羅斯在克里米亞的行動之「合法化」。

(二)善用特種部隊掌握媒體指管

俄羅斯高層在與烏克蘭衝突中，能確實掌握基輔政情惡化的時機點。在3月1日國會以「維安護僑」為名，授權普丁總統必要時可出兵至烏克蘭，保護在烏克蘭俄裔的安全及福祉；此時立即展開大規模軍事演習，代號為「快速校閱」，實際上，是以演習為掩護，以欺騙北約情報機構。並密遣特戰部隊(小綠人)潛進克里米亞地區，以蒙面偽裝成當地民

48 「管理式民主」(managwd democracy) 亦稱「可控民主」，是指運用強制性或半強制性手段來結束政治混亂，並且確立總統為核心，政令由上至下完全暢通的國政治體系。透過國家權力的加強來結束由激進變革所帶來的社會混亂，實現國家的強盛與發展。〈第三章普丁的強國策略與媒體關係〉，頁 47，https://nccur.lib.nccu.edu.tw/bitstream/140.119/33622/8/26300208.pdf，檢索日期：2020 年 10 月 21 日。

49 吳非、胡逢瑛，《轉型中的俄羅斯傳媒》，廣州：南方日報出版社，2005 年，頁 146。

兵、無其他識別標籤，充當為地方安全部隊，在於掩蓋其真實意圖，但主要在迅速占領與破壞地區內之通信設施，並且干擾電信訊號與切斷電源，造成民眾失去對外聯絡管道。相對地，也使烏克蘭政府無法了解該區之狀況，此情況確實讓地區與外界產生隔閡效果，以致造成以下3項結果：

其一、烏克蘭政府無法與克里米亞之進行訊息交流，未能獲取最準確的內部衝突。

其二、烏克蘭政府無法對克里米亞實施內部訊息控制以及傳達國家命令。

其三、烏克蘭政府無法與外國盟友交流，安撫親俄羅斯的烏克蘭人，或破壞莫斯科。

再者，小綠人也主動向克里米亞親俄勢力(或當地犯罪集團)提供武器、培訓與教戰守則，作為親俄勢力的先鋒部隊，使可迅速占領當地政府議會、辦公機構和機場、港口等要地。另外，也製造社會中對烏克蘭政府不滿的輿論和民意，而引發烏克蘭境內，尤其是東烏克蘭境內俄羅斯族人對烏克蘭政府的憤怒，上述條件則易於俄軍進入克里米亞，而且不費一槍一彈就將其占領。

(三)應用社群媒體執行心理控制

自2015年1月以來，歐盟數據庫中顯示在8,223件虛假訊息案例中，烏克蘭則占3,329起(占40%)，居歐盟各國之冠。[50] 可見烏克蘭的資訊環境是多麼窮困。其實，早在未發生衝突前，俄羅斯就已知悉克里米亞使用俄語人數眾多(有77%使用俄語，11.4%使用克里米亞韃靼語，而只有10%的居民使用烏克蘭語)，且均集中在俄羅斯接壤的邊界。

前述因語言屬性相同，過於俄羅斯化，而易於對克里米亞人民傳播「假新聞」，因為錯誤的訊息將造成社會分裂和混亂，使真相越來越難辨認。雖初始烏克蘭政府希能全面封鎖來自俄羅斯的新聞，但此種「言論審查」的行為，並未受民眾支持，僅能作罷。使親俄思想的訊息，有如「病毒式傳播」，進而傳達至全球、區域和本地受眾。更使國內、外「社會大眾」與「軍隊」無法分辨真實與虛構訊息。

1.社會心理認知：俄羅斯政府在衝突期間花費超過1,900萬美元資助社交媒體，藉以「產製」(Manufacture)各種議題與影響層面的新聞作為爆點，通過社交媒體散布毫無根據的陰謀論或網路惡作劇的巨

50 Taras Kuzio,2020/4/23."Russia's Information Warfare Has Deeper Roots Than the Soviet Union,"<https://reframingrussia.com/2020/04/23/russias-information-warfare-has-deeper-roots-than-the-soviet-union-guest-blog/>.

魔工廠，相信他們是真實的。在題材選定上也精緻挑選，主在烏克蘭東部人民最敏感和沉痛的部分，例如：俄語地位衰落、不平等、經濟持續沒落等議題上，從而影響民眾認知與行為，不停造成社會秩序混亂與製造抗議，讓人民產生兩極化的預期結果。

2.國防心理認知：在烏克蘭東部戰爭爆發時，烏克蘭士兵遭受社交媒體上的大量垃圾郵件訊息，例如：「你的營長退縮了，照顧好自己」、「你不會重新找回頓巴斯」、「進一步流血是沒有意義的」或「烏克蘭士兵，活著退縮比留在這裡死好」等字句，以錯誤訊息及媒體宣傳為攻擊武器，試圖影響烏克蘭士兵的判斷能力，進而遭受策反，導致俄羅斯併吞克里米亞。

以上都透過國營媒體進行宣傳以及收買或施壓當地媒體，協助宣揚俄羅斯理念或抹黑反對人士等。且從俄羅斯資訊戰中不難分析到作戰時序是經過縝密計畫，且是有階段劃分，以達到「癱瘓→隔離→取代」等目標(如表6)。

綜合前述分析，可知資訊戰之重要性，且得知資訊戰場是無處不在 。 反 觀中、俄間對資訊戰的操作手法是否有所差異性？其實最主要是因俄羅斯需花費大量資源與時間與美國建立「信任機制」。反之，對兩岸間每日中共均在推動統戰，已不需重新建立信任機制，可直接藉由社群軟體來進行統戰議題操作(政治與軍事)。[51] 例如像「斷邦交」、「經濟制裁」、「經濟誘因」、「散布謠言」、「破壞金融市場機制」等，都是企圖形成國內心理鬥爭，弱化政府輿論信度，使社會與國際偏差的認知與誤解，而最終目的還是在於「社會控制」。

影響及對我的啟示

從國安局108年《外交及國防委員會議》報告中，針對「中國假新聞心理戰之因應對策」議題提及中共正複製俄羅斯併吞克里米亞模式，利用我國民主自由與資訊傳播環境以及法律漏洞等，散播爭議性議題對我進行「認知作戰」。[52]

對中共而言，弱化我國的主權與矮化政府是一貫之目標，若能在國際宣傳上，形塑「一中」議題，將為其重大的政治勝利。另外，影響我國社會內部對立、衝突也是中共選項之一，例如2018年九合一選舉事件，中共早已利用資訊戰帶動國內政治選舉風向，作為操作項目，此議題瞬

51 吳俊德，〈中國與俄羅斯資訊戰手法初探〉《國防情勢月報》，第 144 期，民國 108 年 6 月，頁 32、33。

52 國家安全局，〈中國假新聞心理戰之因應對策〉《立法院第 9 屆第 7 會期外交及國防委員會會議》，https://lis.ly.gov.tw/lydbmeetr/uploadn/108/1080502/01.pdf?fbclid=IwAR0ApykPJIB6pBcxpuIIepNTCN3JXWMH6vektu7PIHvTo8SvVjk2dLFbJfM，檢索日期：2020 年 9 月 21 日。

表6　俄羅斯對克里米亞之用兵分析

<table>
<tr><td colspan="8">俄羅斯對克里米亞作戰時序</td></tr>
<tr><td rowspan="2">用兵步驟</td><td>1→</td><td>2→</td><td>3→</td><td>4→</td><td>5→</td><td>6→</td><td>7</td></tr>
<tr><td>引導國際話語權。</td><td>發動軍事演習牽制。</td><td>癱瘓行政指揮機構。</td><td>占領關鍵聯外管道與設施，隔離、孤立對外聯繫。</td><td>包圍、控制政府、軍事設施與重要節點設施。</td><td>網路、資訊與傳媒接管，擴大既定適時之宣傳。</td><td>正規部隊開進接管。</td></tr>
<tr><td>使用方式</td><td>社群媒體</td><td>軍事力量社群媒體。</td><td colspan="3">小綠人社群媒體</td><td>社群媒體</td><td>軍事力量</td></tr>
<tr><td rowspan="2">達到效果</td><td>增取對克里米亞用兵之合法性。</td><td>運用媒體宣傳達到欺敵效果，吸引西方國家與烏克蘭注意。</td><td colspan="3">破壞克里米亞對外通聯與訊息管道，使島上政府機構、軍隊與人民孤立，利於俄羅斯執行資訊戰。</td><td colspan="2">持續對克里米亞實施資訊宣傳已達到政治目的。</td></tr>
<tr><td colspan="2">癱瘓</td><td colspan="2">隔離</td><td colspan="2">取代</td></tr>
<tr><td>發揮效用</td><td colspan="7">一、使烏克蘭政府內部產生「戰爭迷霧」無法知道俄羅斯的戰略策略。
二、俄羅斯有效破壞烏克蘭與西方國家的行動能力。</td></tr>
</table>

資料來源：筆者自行自作；參考黃柏欽，〈俄烏情勢與兩岸關係：地緣戰略與比較的觀點〉《國防雜誌》，第 29 卷第 5 期，2014 年 9 月，頁 60。

間成淪為各政治節目的口水戰，同時也使人民意識形態有所偏見。

除此之外，若能直接分化主權更是政績之一，如金、馬地區因距離中共過近，亦屬邊陲地帶，中共假使要瓦解我國的自主權，可從邊緣開始分化，如同克里米亞事件一樣，引導展開公投；從上述案例可見影響國安範疇之大。因此，筆者想結合克里米亞歷史事件與我國受中共資訊戰處境相互鏈結，所得之影響層面及啟示思維，作為我國未來之因應。

一、在影響方面

(一)假新聞影響社會民心

從克里米亞事件中，發現俄羅斯善以社群媒體對外從事假新聞(訊息)製作與宣傳，藉以使烏克蘭部分領土喪失。試想中共在語言、字形與文化上都與我國相似。其實早已運用「大外宣」(Grand External Propaganda)的海外宣傳計劃，[53] 大肆收購或入資國際媒體，收買代理人媒體，藉以刊登文宣廣告，或者隱匿遮掩地經由紅色媒體、網路水軍、演算法輔助的社群媒體發布傳播假消訊息，且傳播管道不斷精進，讓偵測和回報機制更加困難。實際上，假新聞已滲透至我國的社會當中，已淪為「重災區」。

53 「大外宣」是「中國對外宣傳大佈局」的簡稱，指中國政府從 2009 年開始，投入 450 億人民幣展開的全球宣傳計畫，第一步是以擴大中央媒體的海外業務為主，包括建立新媒體、增設辦事處、吸納外語人才等，藉此與西方媒體「爭奪話語權」。資料來源顏建發，〈從 COVID-19(武漢肺炎) 疫情看中國大陸的「大外宣」走向崩壞之途〉《展望與探索》，第 18 卷第 5 期，民國 109 年 5 月，頁 10。

另外，新加坡拉惹勒南國際研究學院(S. Rajaratnam School of International Studies, RSiS)所發布的研究報告中提及「五毛黨」(50-cent army)，它是中共網路大軍，曾大量翻牆至蔡英文總統臉書留下各種負面言論(僅12小時內就灌進4萬多則)，藉此企圖干擾或影響國內社會動態。[54]以上事件若政府未能採取監督管理，將會受中共境外勢力干預與影響。據此，應重視假新聞議題，同時也應謹慎處理，避免跨越侵害言論自由之紅線。

(二)大外宣影響辨別能力

俄羅斯在作戰「初期」與「關鍵期」兩階段，不斷從社交媒體上，以各類訊息對克里米亞民眾實施欺騙與誘惑，導致認知偏差，以造成社會大眾均支持俄羅斯政府。反思中共是否也運用同樣手法，透過滲透、收買與操弄輿論等方式以威脅我國民主國家的概念。持續對臺提出「入島、入戶、入腦、入心」與「三中一青」的統戰策略。更於2017年提出「一代一線」策略，將統戰工作投入臺灣「年輕一代、基層一線」，可見積極程度。[55]

然而，現今一代的國人對共產黨缺乏認識與理解，易遭滲透、分化、顛覆、破壞、竊密、統戰影響，其中「滲透」作為是當中最模糊難辨、最難以因應的攻勢。因此對中共的資訊作為需首要防範，除應加強識讀教育對共產黨的理解，其次前述「紅色滲透」在臺灣媒體影響層面之深，甚多媒體如同《環球時報》臺灣版，僅在繁體字與簡體字之差別而已，上述均屬「大外宣」之一部。[56]因此國人須強化對真、假訊息的判斷力以及公民素養水準，了解中共資訊戰的手段與影響，降低奇襲之效應。

(三)假媒體影響政治議題

克里米亞事件的媒體亂象已造成烏克蘭重大危害，被多國認為是一場「國安危機」。因此，各國吸取經驗教訓，紛紛對不實訊息加以防範；事實上，2019年牛津大學網路研究所(Oxford Internet Institute)主任霍華德(Philip Howard)以「運算政治宣傳」(computational propaganda)概念，分析各國政治精英將利用社群媒體演算法操縱公共輿論，進行政治宣傳及其可能的負面效果，企圖影響政治環境。[57]因此，我國行政院也應重視，因為這將使假媒體大肆介入政爭，黨同伐異，錯假新聞，誤導大眾也損及政治的公

54 〈中國的銳實力大平台：統戰、「大外宣」與假新聞〉，https://whogovernstw.org/2019/04/15/linpu4/，檢索日期：2020年11月19日。

55 李哲全，〈中國對臺滲透作為與因應思辨〉《新社會政策》，第62期，2019年4月，頁61～65。

56 全球圍剿中共大外宣專家：臺灣處理紅媒了？《大紀元》，https://www.epochtimes.com/b5/20/5/1/n12075961.htm，檢索日期：2020年11月19日。

57 於下頁。

正性。例如像2018年關西機場假新聞事件、九合一選舉等等，都在社群媒體間不斷流傳。

事實上，我國在2018年也陸續成立專案小組對散布「假訊息」實施修法，至今在不同領域上均課以罰則，防堵假訊息流竄。例如：《反滲透法》、《災害防救法》、《糧食管理法》、《傳染病防治法》及《廣播電視法》等。實際上，雖然已完成修法但此趨勢卻無遏止，如我國已通過《反滲透法》，但至目前為止還未有人因違反《反滲透法》被逮捕或判刑，因此政府在國安法津方面還須再檢討。

二、在啟示方面

(一)落實監督管理機制

國內正遭部分親中媒體大量假資訊轟炸，政府、民間及社群網站、媒體應共同參與假新聞防範，而政府部門更應擔負起責任，擬定必要危機處理機制，以設置「公開、快速和結構化」3原則的查證窗口，以即時澄清不實謠言，提供正確訊息，以下有3點提出建議：

1.具備健全查證機制：政府雖有與民間、社群網站及媒體共同參與假新聞查證機制，但仍處於協調角色，希能在機關建立專責查證辦公室，使機制更為健全完整。例如各機關單位可結合科技與群眾力量，建立即時「闢謠專區」回報平台等。

2.落實政府資訊窗口：各政府機關可在各業管網站增加「假新聞」資訊平台，一旦有發現假新聞事件，一律在官方網站以公開、迅速和結構化實施說明與澄清，例如像「Q&A專區」實施統一回覆，避免造成滾雪球效應，引發社會恐慌。

3.強化新聞判斷能力：各政府機關可思考設置「事實查核專責人員」，藉由該員之專業能力與經驗，對於可疑而待查證的訊息執行把關，並且判斷所損害之公共利益與影響程度(個安、社安、國安)。

再者，除上述外，政府並可廣邀相關部會以及專家學者共同研討如何強化國家資安防護、犯罪偵防及國家安全等面向的配套處理機制。

(二)強化媒體識讀教育

我國面對中共資訊戰影響是無所不在的，社會大眾不宜愚昧介入網路爭議，易產生同溫層效應，引發社會議題，如國家安全、資安等等。除政府應處機制外，各地方政府還可從「教育訓練」與「知識素養」兩方面著手。

1.教育訓練：國人最主要的武器就是「教育」，而如今社會最刻不容緩的就是「媒體識讀」(Media Literacy)能力，務必將媒體資訊素養課程納入學校(尤其在國

57 「全球資訊戰」善用平台操弄民意、精準分眾影響外國選舉牛津大學專家：中、俄是製造假訊息「超級強國」！》〈風傳媒〉，https://www.storm.mg/article/1933443?page=1，檢索日期：2020 年 11 月 19 日。

中、高中階段)與社會教育的課程內。教育課程可涵括：一、了解與辨識廣告對心理的影響。二、區辨媒體訊息中的事實與虛構。三、辨別與理解媒體訊息中的不同觀點。四、理解媒體類型與內涵。五、區分媒體節目製作的元素。其重點在教導如何辨識假訊息和批判性的思考模式。

2.知識素養：政府亦應強化大眾的媒體素養，應該不斷提升民眾對於社群媒體所傳出之訊息，需有「識假、破假、抑假」的思辨能力，更重要在於解讀媒體的能力。長期來說，還是必須植基於教育，將媒體素養、公民資訊素養普及化、深耕化，才有可能發揮更大效果。

其實，英國在1989年就開始將「媒體教育」納入國定課程(The National Curriculum)實施。而近期歐盟也深受假新聞影響，也已開始規劃「媒體識讀週」(Media Literacy Week)，進行有效的媒體識讀能力提升。所以，國人要有所認知，唯獨接收各方資料分析，培養獨立思考的能力，才能跳脫「同溫層」效應。最後，政府在人才培育上也須加強，可以廣納具媒體素養師資或者師資培訓課程，利用各種場合，辦理「媒體識讀」研討會或研習營，增加主動宣導的效能。

(三)精進資訊法治漏洞

事實上，因應假訊息事件，各國均是嚴陣以待。所以不僅是我國受攻擊，而是各民主國家均面臨的危害，成為破壞社會秩序、國家安全及民主政治的威脅。因此，我國應仿效與參考新加坡、德國與法國等國家，同步修正更新社群媒體議題條文。以下為上述國家修法內容：

1.德國聯邦議院於2017年6月30日通過《社交網路強制法》(Netzwerkdurchsetzungsgesetz, NetzDG)，要求一定規模以上的大型社群網站，必須撤除明顯違反德國刑法的仇恨言論。且社群媒體公司則有7天期限，決定是否要移除該貼文；而多次失責公司將面臨5千萬歐元罰款。[58]

2.法國於2018年7月以選舉為中心立法管制，一、在全國性選舉的前3個月期間，政黨或候選人得向法院申請禁制令，禁止錯誤資訊傳播；二、要求社群媒體平台與傳統媒體應公開廣告之贊助公司；三、法國高等視聽委員會得將意圖介入法國選舉的外國廣電業者下架。[59]

3.新加坡於2019年10月生效的「防止線上虛假與操縱法」(Protection from

58 「全球我最有Guts」德國立法約束假新聞，要用17億懲罰散布者與網路平台，〈報橘〉，https://buzzorange.com/2018/07/26/we-need-to-talk-about-how-we-define-responsibility-online-and-how-we-enforce-it/，檢索日期：2020年7月9日。

59 於下頁。

Online Falsehoods and Manipulation Act 2019)，該法賦予當局有權認定什麼是假新聞，並得對散布假新聞的媒體和網路平臺，最高處100萬星幣，折合新臺幣超過2,300萬元的罰款，個人部分將面臨10年有期徒刑。[60]

其實，各國對於假新聞、社群媒體與網路都有所重責，且都要求業者自律，若明顯違法內容則與下架及刑責。除上述之外，也可加諸「自律」條文要求，凡具有一定規模以上的社群媒體，應建立自律機制，自我先行檢視、過濾與排除違法等行為，例如像「達成自律協議」和「提供自律建議」，並以法規或公權力要求該自律機制的落實。

總之，檢視中共對我國的資訊戰已跨足平、戰時，顯見資訊戰已悄悄地替代了傳統戰爭。在此資訊化社會環境與政府機制現況下，確實凸顯出許多脆弱性，因為沒有血腥的殺戮，沒有驚悚的報導，也造成了人們對危險的麻痺。因此國人更宜慎思因應，強化中共資訊戰威脅之防範力道，以維護國家安全。

結　語

《詩經》記載：「民之訛言，亦孔之將」，可用於對現今社群媒體的負面評價，尤其是對國家控制媒體的極權國家，更是如此。從俄羅斯吞併克里米亞之事件過程可見，資訊戰是場無砲火的戰爭，不須經由宣戰，就可達到全天候作戰，異於傳統軍事戰爭，是對於民主國家的警示，因此，我國更加以防範與注意，尤其在「假新聞」的心理認知部分。

然而，透過本文對資訊戰的探討，發現目前兩岸關係現況，雖不像昔日緊張對峙，但至今仍未放棄「統戰」。因此，平時更應瞭解與重視「中共網軍」可能運用資訊戰對我國步步進逼，長期監控國內社會議題，企圖以「假訊息」擾亂民眾的「認知空間」，使國人與政府對此毫無警覺心，就如同溫水煮青蛙一般，久而久之將可能會使民主、自由與法治喪失。

因此，我國政府機關應重新檢視對於資訊戰的備戰方向與作為，絕非僅靠單一機關能夠克服，須整合國內資安力量，建構一套「社群媒體安全防護機制」，如此才能防範對於社會的危害，也必能阻絕中共採用各種滲透手段，製造社會紛擾，危害我國民主體制的正常運作。

(109年8月6日收件，109年11月18日接受)

59　〈國際應對爭議訊息法制及政策簡介〉《臺灣新社會智庫》，http://www.taiwansig.tw/index.php// 政策報告 / 憲政法制 /8482—國際應對爭議訊息法制及政策簡介，檢索日期：2020 年 7 月 12 日。

60　楊惟任，〈假新聞的危害與因應〉《展望與探索》，第 17 卷第 12 期，民國 108 年 12 月，頁 110。