中共《網路安全法》簡介與潛藏威脅之研析

筆者/邱永彬

提要

一、 網際網路的快速發展及高普及率，使中共體認網路影響層面擴大，然因其「政黨政治」之影響，使其網路管控以網路長城及網軍等獨特模式發展，並對其他國家造成影響。

二、 中華人民共和國於 2017 年 6 月 1 日施行《網絡安全法》，是中共為加強境內網路安全管理而制訂之專法，內容以保護個資、防範網路詐騙及網路攻擊為主，但亦包含限制境外企業的相關條文。

三、 中共《網絡安全法》除明訂網路違法行為之定義、刑責與相關懲罰條文，藉此限制國際企業於中共境內提供之網路服務，更賦予政府在緊急情況下管控及壟斷網路之權力。

四、 我國網路軟硬體環境非中共《網絡安全法》管控之對象，然因民眾及企業使用中共境內之網路服務日益增加，亦受該法直接與間接影響。

關鍵詞：網際網路、網絡安全法、網路違法

壹、前言

因電子科技及網路資訊系統之快速發展，世界各國其金融商業活動、電力民生設施、大眾傳播電信及運輸交通管理等，均廣泛運用網際網路以獲取高效益之附加價值，並提供相關網路服務予一般民眾，藉此交流模式而獲取經濟成果；而網際網路的快速發展及高普及率亦帶來許多負面影響，如個人資料外洩、網路新形態犯罪模式及駭客惡意程式攻擊等，故各國政府亦制定相關法規以確保其境內網路使用之安全，隔絕來自境外他國之網路威脅。

相對於民主國家，中共自經濟制度改革開放後，龐大的人口使其成為世界主要經濟市場之一，其境內現代商業活動如金融交易、貨品物流及倉儲管理等，再加上交通運輸、民生醫療及衛星定位等，均大量使用資訊網路技術支援相關經濟活動，但其「政黨政治」的管理下，反以國家層級建置「網路防火長城[1]」，配合大量網軍人力管控其境內網路的使用及隔絕境外網路的服務，更於 2017 年 6 月 1 日施行其《網絡安全法》，做為法理之依據。

貳、中共《網絡安全法》

一、立法背景

中共於 2015 年 6 月第十二屆「全國人大」常委會第十五次會議中，初審通過「網絡安全法」之草案，同年 7 月公布草案全文，其官方發布之

1.中共國家防火牆，https://technews.tw/2015/12/24/what-is-china-censoring-on-the-web/

立法說明文件明確指出，該法案主要是為有效應對中共當前三大網路安全問題：一是「網路入侵及網絡攻擊等非法活動」；二是「宣揚恐怖主義、極端主義，煽動顛覆國家政權、推翻社會主義制度，以及淫穢色情等違法資訊」；三是「非法獲取、洩露及盜賣公民個人信息，侮辱誹謗他人、侵犯智慧財產權等違法活動」[2]。上述問題中，前兩項明顯影響中共之政權統治，而第三項則涉及中共對境內民眾的管控，就中共「對境外國家之網路攻防」及「對境內民眾之網路管控」分析其立法背景：

(一)境外國家之網路攻防：

近幾年許多國家的政府機關及企業均控訴遭受來自中共的網路攻擊，如《紐約時報》報導美國麥迪安網路安全公司的報告[3]中，直接點名 61398 部隊[4]屬中共總參謀部第三部(如圖 1)，負責偵聽、破解密碼及處理國外通訊傳播訊號參三部總部設在北京。

圖 1 中國人民解放軍 61398 部隊位置示意圖

資料來源：《紐約時報》，中國軍方是黑客襲擊者，BBC中文網 2013-02-19。

經由軍事學家的比對及分析攻擊來源後，認為來自中共駭客團體所進行的網路攻擊，其大規模、大面向以及其高度專業、細密組織的特性，應是中共的網軍部隊；然而面對各界相關的資訊及指證，中共當局一概不承認，僅以「…出於各種目的，就駭客攻擊進行無端猜測和指責，既不專業，也不負責，無助於解決該問題…」的官方說法回應，甚至指出中共也是駭客網路攻擊的受害者。

因中共有目的性的網路攻擊涉及軍事層面，故部分國家陸續發布網路安全相關法令，如歐盟於 2013 年啟動審議立法的《網路資訊安全指令》、美國於 2014 年 11 月提出《網路安全增強法》、日本於 2014 年 11 月

2.羅世宏，大陸網路安全法簡析，行政院大陸委員會情勢簡報。
3.《紐約時報》，中國軍方是黑客襲擊者，BBC中文網 2013-02-19。
4.維基百科，中國人民解放軍61398部隊。

通過的《網路安全基本法》等，中共見國際情勢如此，亦開始其網路安全專法之立法過程。

(二)境內民眾之網路管控：

相對於我國網際網路的開放性，中共境內的網路管控不僅是以國家層級執行，更建置一套網路「防火長城」，以管控境內網路的使用及隔絕境外網路的服務；此網路防護機制跟大多國家相似，主要是監控境內之網路安全及隔絕境外之網路威脅，然在中共的政治干預下，其限制卻遠比其他國家來得多，如 Google、Facebook、Line 等知名網路服務企業，皆不能於其境內設置及提供相關功能，但中共卻不因此限制局限其境內網路發展，反而參考各國及企業的網路服務內容，發展境內專屬的網路服務，如搜索引擎的百度、通訊軟體的微信及行動支付的支付寶等，儘管部分民眾可透過 VPN 虛擬技術，「翻牆」使用境外網路服務，但就中共龐大的網路流量而言算是少數。

隨著中共資訊科技之進步，其境內網路管控的手段愈發明顯，不符官方要求的內容，都可由政府進行干擾、阻斷及遮蔽，包括嚴厲執行「網路實名制」、「清網行動」及加強管控微博、微信等一連串措施，顯有強化集權威信與結合網路進行社會維穩監控的意圖，如十九大前夕，中共境內大多數的 VPN 網站及軟體，均被攔截、封鎖及關閉，並針對相關政治議題，限制境內網路使用，可見其網路管控之執行，顯示中共當局將網路管控視為鞏固政權和維穩社會的首要工作。

二、《網絡安全法》條文內容

中華人民共和國《網絡安全法[5]》共有 7 章 79 條，分別為第一章-總則；第二章-網路安全支援與促進；第三章-網路運行安全；第四章-網路資訊安全；第五章-監測預警與應急處置；第六章-法律責任；及第七章-附則。各章節條文重點如表 1 所列：

表 1 《網絡安全法》條文內容重點

章節	標題	條文範圍	重點
第一章	總則	1-14	明定立法精神、適用對象、相關政府機關及部門之責任
第二章	網路安全支援與促進	15-20	政府機關及部門針對網路安全支援與促進的政策指導
第三章	網路運行安全	第一節 21-30	網路營運業者所負法律責任

5.中國人大網， www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm。

第三章	網路運行安全	第二節 31-39	政府機關及部門掌管關鍵資訊基礎設施之運行安全所具法律責任
第四章	網路資訊安全	40-50	定義「網路安全」之範圍及違法行為之處置作為
第五章	監測預警與應急處置	51-58	政府機關及部門執行維護網路安全之權力
第六章	法律責任	59-75	違反前述條文法律責任之罰則
第七章	附則	76-79	條文用語含義及補充

資料來源：www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm

各章節條文依內容相互對照形成5項重點[6]：一是明定網路營運業者的義務，並加重其營運責任；二是就網路犯罪及攻擊之懲罰條文；三是保護關鍵訊息基礎設施最為；四是強化境內網路使用者的實名監控；五是賦予政府網路監管部門之管控權力，分述如下：進而一舉達成國家安全、網路主權與網路信息安全和社會維穩控制的多重目的，其內容影響層面

(一)「網路營運業者」及「資訊相關基礎設施營運業者」之網路安全規範[7]：

主要針對「網路營運業者」和「資訊相關基礎設施營運業者」兩種類型的公司企業及個體，提出確保網路資料安全之規範要求。

「網路營運業者」之定義，為網路服務持有人、供應人及管理人，而「網路服務」定義，為電腦、伺服器和資訊終端設備等所組成之系統，用於收集、存儲、傳輸、交換和處理資訊，不僅涉及電信和網路服務供應商，亦可涵蓋在中共境內持有或從事資訊相關業務活動的任何組織個體;「資訊相關基礎設施營運業者」，則是網路營運業者的一部分，涵蓋範圍較廣，如電子通訊、能源、交通運輸、水資源、金融、公共服務等產業領域，及其他類型產業之資訊設施及活動等，若對國家安全、經濟或公共社會利益構成嚴重威脅，如遭受破壞、資訊外洩等情況，也可被視為基礎相關資訊設施業者。

(二)嚴懲網路詐騙和網路攻擊[8]：

關於網路詐騙防治，《網路安全法》明訂任何人、組織及企業不得利用網路發佈與實施詐騙，製作或者銷售違禁物品、管制物品以及其他違法犯罪活動的信息，並嚴懲網路攻擊的個人及組織，其中境外的個人或組織攻擊、侵入、干擾、破壞等危害中共的關鍵訊息基礎設施的活動，造成嚴重

6.羅世宏，大陸網路安全法簡析，行政院大陸委員會情勢簡報。
7.朱子亮，中國大陸網路安全法即將在2017年6月1日生效，科技產業資訊室。
8.郭芝榕，中國強力通過《網路安全法》背後沒說的那些事，數位時代報導。

後果者，中共公安部門和相關部門可採取凍結財產或者其他必要的制裁措施。

(三)保護關鍵訊息基礎設施

依據《網路安全法》規定，針對公共通信和信息服務、能源、交通、水利、金融、公共服務、電子政務等被列為「關鍵訊息基礎設施」的產業，中共特別實行重點保護，還要求網路營運商為了「國家安全」的目的，必須替中共政府部門及公安機關提供技術支持，甚至必須接受設備安全檢查，且「限制數據跨境傳輸」，意指來自中共境內的數據資料必須儲存在中共境內。

(四)網路實名制法令化

為了管制不當言論，《網路安全法》明訂網路運營商為用戶提供電話及網路等服務之前，必須要求用戶提供真實身份，才能夠提供相關服務，也就是要求網路服務落實實名制，而網路服務使用者必須實名制，讓中共控管所有網路運營商的「入口」。

(五)危及國家安全的重大突發事件可限制通訊

因維護國家安全和社會公共秩序，處置重大突發社會安全事件的需要，經國務院決定或者批准後，可以在特定區域對網路通信採取限制等臨時措施。

就《網路安全法》條文內容分析，中共訂定此法是為一舉達成國家安全、網路主權與網路信息安全和社會維穩控制之多重目的。

參、中共《網路安全法》之影響

一、《網路安全法》之權力

《網路安全法》制訂、公布及施行前，中共對於網路資訊安全之管理規範，散佈在若干獨立法條之中，如 2011 年互聯網資訊服務，或 2016 年中華人民共和國電信條例等，而中共境內第一部專門規範網路安全的《網路安全法》正式公布生效後，凡涉及維護網路環境、敏感資料安全性及保護公民隱私的範圍，皆有了詳細定義，且政府機關也具備執行公權力的法律依據。

在國家安全、網路主權與網路信息安全的名義下，該法賦予中共網路監管部門監管權力，如有權對網路關鍵設備和網路安全專用產品實施安全認證檢測；有權因國家安全和偵查犯罪需要，要求網路運營者提供必要的支援與協助；有權對關鍵資訊基礎設施的安全風險進行抽查檢測；賦予監管部門要求停止傳輸或刪除違法信息，及採取防火牆等措施阻斷違法資訊傳播的權力；甚至有權「在部分地區對網絡通信採取限制等臨時措施」。

前述權力使中共對網路營運業者、網路使用者或是網路管理部門工作

人員，對其違法情事具有包括警告、沒收獲利、監禁之罰則和罰款外，還可責令網路運營業者暫停相關業務、停業整頓、關閉網站、撤銷相關業務許可或者吊銷營業執照等處分。

二、《網路安全法》對企業之影響

《網路安全法》要求「網路營運業者」、「資訊相關基礎設施營運業者」履行以下網路安全規定：

(一)訂立企業內部安全管理制度和實施規則，包括採取技術措施，防止病毒和其他網路入侵行為；保存至少六個月的網路連線紀錄；採取資料分類系統、備份系統和加密等安全措施。但這些資料的安全措施，必須按照中共網路安全保障體系實施。

(二)擬訂網路安全事故之因應方案，在事故發生時能夠及時實施補救措施，並向監管部門報告。

(三)向政府機構提供技術資源和其他支援，以協助維護中共國家安全和犯罪調查。

(四)採取額外安全保障措施，例如對重要職務負責人員進行安全背景調查、網路安全教育和技術培訓、事故資料恢復備份等。

(五)採購可能影響中共國家安全的網路相關產品或服務時，應接受中共權責機關、部門實施安全審查。

(六)每年進行網路安全檢查。

上述規定加重營運業者的責任和義務：如政府機關可要求業者依關鍵信息基礎設施重要資料境內留存制度，若確需在境外儲存或向境外提供者，應按照規定進行「安全評估」；要求業者遵照網路安全等級保護制度，採取相應管理和技術防範措施；要求業者承擔處置違法信息的義務，以及發送電子信息、提供應用軟體合法發布或傳輸信息之義務。

三、《網路安全法》對使用者之影響

《網路安全法》亦對中共公民使用業者提供之網路服務，要求履行以下網路安全規定：

(一)個資儲存於中共境內：

中共公民個人資料及重要資料，必須存放在中共境內，其中「個人資料」一詞在《網路安全法》第 76 條廣泛定義為「以電子方式存儲、可單獨或在結合其他資訊下識別特定自然人身份，包括其個人姓名、出生日期、身分證號碼、地址、電話號碼、個人生物特徵資訊等」。

(二)個資處理及轉移規定：

前述「個人資料」，基於合法商業原因，必須轉移至中國境外，資訊基礎設施營運商，必須接受中國國務院和國家互聯網信息辦公室所制訂的安全審查。

(三)網路用戶真實身分驗證和未成年人隱私保護：

提供網路服務之前，必須驗證使用者的真實身分，藉此來強制執行網路或即時訊息服務用戶使用真實身分識別之要求；另保護未成年人隱私，以避免個人資料不當利用情形。

(四)配合官方監督、調查及執法行動：

中共監管機關可明確及廣泛執行監督、調查和執法權力，並要求網路及資訊設施營運商，必須與監管機關保持合作。不合作情形將招致處罰。

法案強化對個別網路使用者的實名監控權力，要求網路服務提供商、基礎電信運營商在為用戶提供網路服務、使用電信基礎服務時，要嚴格推行「實名制」，禁止網民以匿名的方式使用網路服務；亦禁止網路使用者發送「含有法律、行政法規禁止發布或者傳輸的資訊」。

肆、中共《網路安全法》潛藏威脅

中共《網路安全法》雖是中華人民共和國所制定之法律條文，然中共在兩岸關係上仍秉持「一個中國」之原則，故此法案對我國而言實有其潛藏威脅存在。

一、三戰

2003 年間，中共中央委員會與中央軍事委員會批准「三戰」解放軍作戰概念，即輿論(媒體)戰、心理戰及法律戰，其戰略目標分述如下：輿論(媒體)戰影響中共國內和國際輿論，以支持中共軍事行動，並削弱敵國獲取中共利益的合理性；心理戰透過軍事與政治作為，降低敵國軍事人員和人民士氣；法律戰利用法理精神影響國際公約，為其軍事行動辯解及宣稱自身利益。

《網路安全法》雖非三戰之產物，但究其條文內容卻有異曲同工之效，筆者個人見解如下：

(一)輿論(媒體)戰：

隨著中共整體經濟的進步，投資大量物力、財力於傳播媒體上，如中央電視台就以中國官方頻道為名，向全球以中文或當地語言播放相關節目，在軍事節目中描述解放軍部隊訓練及演習動態，展現其軍事武力；在專家評論節目中討論其處理「一個中國」的正當性；或是不同主題的專題節目，如批評台獨、美國干涉兩岸事務、國際地位等，運用所有形式的傳播媒體影響中共國內及國際輿論，不僅宣傳中共的立場，同時反駁批評中共政策及軍事行動的言論，使其軍事行動獲得支持，而在資訊爆炸的網路時代，網際網路早已成為群眾獲取新聞的主要管道。

《網路安全法》讓中共政府可控管網路業者，以網路的社群功為例，

中共可運用非官方組織影響輿論，如中共網路評論員[9]，最初是一群人受雇於特定人士，以一般民眾身分於網路上發表有利中共地方、中央政府或是反駁批判政府之言論，以達到製造或影響輿論之目的，如每發一篇網路評論加薪五毛的「五毛黨」一詞，便是中共境內民眾諷刺這些受雇的網路評論員產生的代名詞。而隨著中共經濟起步帶動網路之影響下，網際網路的社群功能開啟另一種商業模式，一般民眾可依個人喜好或需求在網路上留下相關訊息、影片，企業網站則開放客戶留言及評論，透過網際網路散佈以達到「廣告」效益，獲取龐大利益，但若在網路留言的民眾，其內容係針對特定網站及目標，或是具有特定政治目的，則會形成另類的網路攻擊。

我國屬亞洲地區中網際網路自由度高的國家，政府機關、組織及企業網站，除因特殊安全考量外，大多採開放式供民眾瀏覽使用，然此一民主開放的美意，卻成為中共另類的網路攻擊方式，如臉書部份的反台灣帳號，用其高度政治化的言論在各網站留言、洗版，或是用網路留言舉發所謂的台獨份子，影響輿論及我國民眾在中共境內的人身安全。相關事件都曾因媒體報導而引起關注，如牛津大學執行「運算宣傳研究計畫[10]」的報告中，我國就因中共的單向跨國網路攻擊，成為研究對象之一。在此報告中，明確指出「五毛黨(50-cent Party)」的存在，其組成份子非一般網路使用者，而是政府機關有計畫雇用，專職使用網路功能影響輿論的團體，其主要作為包含短時間大量發佈特議題之言論及就不利政府言論提出反駁等。報告內容更以我國總統臉書帳號遭受惡意言論攻訐、我國藝人戴立忍被指責傷害中共人民感情等案例進行分析，並在總結說明就網路宣傳戰爭而言，中華民國之數位民主，面臨中共自發性的獨裁威脅。

(二)心理戰：

軍事心理戰之主旨是打擊敵方士氣、削弱戰鬥意志，進而製造摩擦及不信任，使敵方產生異議、疏離和不滿。但中共其政治背景，更可針對敵方的國家認同感、社會價值觀、國防意識及外交政策，採用進一步的手法，如政治及軍事恐嚇手段；網際網路正是提供此戰略目標的最佳傳遞管道，可依作戰目標選擇最適合的網路管道，如攻擊瀏覽率高的人氣網站，置換或張貼不實訊息，讓民眾一時之間無法查明真偽，以達到影響層面的事實。

我國開放的網路環境，提供國民可依個人需求、意願瀏覽世界各國開放的網站，包含中共，在《網路安全法》的規範下，中共運用心理戰之方式，除軍事作為外，更可深入至目標的政府機關、國家人民，從境內政府決策到國際外交政策，或是國家認同及戰爭價值等，甚至於「邦交國」，都是其心理戰的目標。

9.維基百科，網路評論員。
10.Computational Propaganda Research Project，分析美俄德中等9高國家，近3年社群媒體的宣傳戰。

(三)法律戰：

二次世界大戰剛結束時，主要軍事強權國家把持著國際間的調度與平衡，適時中國共產黨尚未取得政權，但卻也是因部分國家間的條約，使其有發展的空間，自此中共體認軍事衝突前法理依據的重要，有充分的法律準備工作能減少境外對其軍事行動的干涉，故中共單方面發布各式的法令及條文，以確保其國際權益。於是透過法條明文訂定相關內容，營造中共在軍事行動或政策之法理依據，進而作為法律先例，加上中共為聯合國理事會主要成員，配合國際社會認同的公約，其目的為朔造有利於中共的國際法，或增加其合理性，以壓縮戰略目標的國際空間，無法尋求外交協助。

「影響和制約國際公約，為其軍事作為做準備」是中共法律戰的主要目的，《網路安全法》就可視為是中共信息戰與法律戰的結合，其立法精神以保護個資、防範網路詐騙及網路攻擊為主，並訂定相關罰則，展現中共想降低網路威脅之決心，用法律明確定義網路營運商的種種責任，但卻也透過法條限制國外企業在其境內提供的網路服務，甚至要求企業配合法條提供涉及「個人隱私」的資訊。

二、壟斷網路服務市場

前述《網路安全法》管控範圍包含「網路營運業者」及「資訊相關基礎設施營運業者」，意味著中共當局，可藉由法令條文，對所有類型之產業及業務活動，進行全面性的網路安全管制，此舉使非中共境內的企業營運成本變高，甚至可能根本進不了中共市場；反之，已在中共營運的網路業者可視為已符合該法令之要求。換句話說，要走進中共龐大的經濟市場，就得按規矩來，不符合中共法規的要求，嚴重者甚至違及中共的國家安全，就禁賣產品、禁用服務，甚至退出市場，如華碩公司因應新的《網路安全法》，就選擇退出中國市場11：「華碩公告表示，為配合中國政府監督管理部門的互聯網存儲治理專項活動，Web Storage 將在 3 月 1 日起關閉上傳服務，用戶將無法再上傳任何數據，而 3 月 1 日至 4 月 30 日僅提供下載服務。上海機房將於 5 月 1 日正式停止，如果想繼續使用的民眾，可以登錄專用網站並選擇重新開通帳戶至其他國家或地區」。

此外依照條文要求網路營運業者擔負清除或阻斷「有害信息」傳播，否則採取各種懲罰措施，如暫停相關業務、停業整頓、關閉網站、撤銷相關業務許可或者吊銷營業執照等，此舉無限制地擴充中共網路監管部門權力，加重網路營運業者負擔網路信息內容審查、清除和阻斷的責任，並嚴格限制一般網路使用者發送「含有法律、行政法規禁止發布或者傳輸的資訊」，藉以達成防止網路成為引發社會騷亂或威脅政權穩定的源頭。

11.黃敬哲，華碩雲端退出中國市場關閉資料中心，科技新報，2018年2月12日，版C7。

三、侵犯個人隱私

現今多數網路服務大多要求需先申請帳號，方可使用其相關功能，舉智慧型手機為例，啟用 Android 系統手機須有 Google 帳號、蘋果 IOS 系統手機須有 Apple ID，而這些帳號申請時均需輸入個人基本資料，如姓名、聯絡電話、出生日期等，若有交易、消費行為還需信用卡卡號及授權碼等，而這些資料在《網路安全法》中被廣泛定義為個人資料，也就是若網路服務是由中共境內企業所提供，當中共政府當局認定有需求，就可要求網路業者提供資料，且不用當事人同意。

除了網路服務外，中共近年在智慧型手機產業上，市占率亦大幅提申，我國部分民眾使用小米、華為等中共境內廠牌手機已是常態，軟硬體規格皆符合中共法令規範，其潛藏的資安威脅更是令人擔憂。

伍、結論

我中華民國可說是名列世界「資訊大國」之一，網路普及度名列前茅，中共資訊網路的基礎上雖不比我國，但中共境內網際網路的發展相當迅速，加上網際網路是個全方位開放的「虛擬世界」，中共近年來透過法令、國安部、公安部及保密局的介入，管控資訊網路是以國家層級推動，在現階段無論是科技、預算、人力投入、政策指導與執行等方面，總體而言已超越我國。

中共《網路安全法》雖屬其國內法，但對在中共經商之台灣及國外公司企業，已構成資安保護及資料跨國轉移方面之重大影響，例如屬於中國公民之個人資料等，將必須在當地設置網路系統來進行儲存。鑒於大多數在中共從事商業活動之公司企業，皆使用網路資訊系統，境內存放要求，將構成顯著限制，並提高資料處理成本；同時在資料跨境轉移方面，也將面臨顯著限制及監督。對此，我國軍同仁應該初步瞭解該法內容及個人隱私潛藏威脅，以確保使用網路服務時，成為敵人收集資料的對象。

透過加強資安應變及處理復原能力，配合政府推動機關資安管理制度，提升資安防護技術與軟體安全管理，培訓資安專業人才及國際交流合作等措施，預期可提升我國軍整體應變及處理能力等目標，加上資訊戰涵蓋層面寬廣，且資訊科技發展日新月異，更何況我國資訊產業體質健全，在研發與生產方面仍具有相當潛力，在基本因應能力上仍可占有優勢。是故，如何以實際行動落實推動資安防護，以強化我網路安全，是我國軍在面對中共信息戰之首要工作。

參考文獻

一、中共國家防火牆，https://technews.tw/2015/12/24/what-is-china-censoring-on-the-web/，檢索日期：2016 年 12 月 11 日。

二、羅世宏，大陸網路安全法簡析，行政院大陸委員會情勢簡報，https://www.mac.gov.tw>News，檢索日期：2018 年 1 月 13 日。

三、《紐約時報》，中國軍方是黑客襲擊者， 2013 年 2 月 19 日，版 4。

四、紐約時報中文網，中國人民解放軍 61398 部隊，https://cn.nytimes.com>china>zh-hant/，檢索日期：2016 年 10 月 22 日。

五、中國人大網， www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm，檢索日期：2017 年 10 月 22 日。

六、朱子亮，中國大陸網路安全法即將在 2017 年 6 月 1 日生效，科技產業資訊室。

七、郭芝榕，中國強力通過《網路安全法》背後沒說的那些事，數位時代報導。

八、博聞社，網路評論員，https://tw.appledaily.com>new>realtime/，檢索日期：2017 年 4 月 31 日。

九、Computational Propaganda Research Project，分析美俄德中等 9 高國家，近 3 年社群媒體的宣傳戰。

十、黃敬哲，華碩雲端退出中國市場關閉資料中心，科技新報 2018 年 02 月 12 日。

筆者簡介

姓名：邱永彬
級職：少校教官
學歷:國防大學管理學院資訊管理學系碩士班 100 年班、通資安全正規班 15 期。
經歷：排長、副連長、資訊官、通信官、現任裝訓部通信組教官。
電子信箱：軍網：s925539@webmail.mil.tw；民網：s925539@yahoo.com.tw