航空技術學院學報　第十四卷　第一期　第 45－54 頁（民國一〇四年）
Journal of Air Force Institute of Technology, Vol. 14, No. 1, pp. 45-54, 2015

面對新型態網路戰爭發展國防通資安全防禦研究探討

National Defense Network Security Theories and Technologies on New-Era Information Warfare Developments

Chia-Long Wu

和春技術學院資訊工程學系專任教授兼系主任

Professor and Director of Computer Science and Information Engineering Department, Fortune University

摘要

據全球資安威脅資料統計，去年網際網路惡意活動以數量計算，我國佔百分之三，世界排名第九；若使用網路人口數改以密度計，則我國在全世界排名第二，是上網最不安全的國家之一。未來的戰略競逐中電腦網路本身就是一種武器與戰場，前線無所不在，奪取戰場控制權將不只是導彈、飛彈和士兵，還包括電腦網路與數位通訊機制。美國前國防部長黑格爾強調，網路領域的襲擊是美國目前面對關係到國家「經濟安全、政治安全、軍事安全、外交安全」等領域的最嚴重威脅。面對時有所聞的網路攻擊事件，政府亦相當重視資安工作的推動，尤其當前兩岸經貿交流頻繁，互通訊息難以避免，然而各種不斷變化的網路駭客，以及中共網軍的無孔不入，對我造成之無形威脅，其危險程度絕對不亞於沿岸部署的飛彈，對身負國家安全重任的國軍而言，更須具備高度警覺性，妥採因應措施。

關鍵字：資安威脅、資訊戰、駭客攻防、惡意程式、網路管理。

Abstract

According to the global information security threats to statistics, last year the quality of Internet malicious codes attack activity ranks 9 in the world of 3%. If we use the Internet population changed to "density" meter for analysis, then our country in the world ranked second, is one of the most insecure Internet environment. Former US Secretary of Defense Hegel emphasized areas of network attacks in the United States is facing the most serious threats related to national "economic security, political security, military security, diplomatic security" and other areas. Future strategies to compete in computer network itself is a weapon and battle front omnipresent, seize control of the battlefield will not only guides missiles, missiles and soldiers, but also including computer networks and digital communication mechanism. Heard in the face of network attacks, the government has also attached considerable importance to promote information security work, in particular the cross-strait economic and trade exchanges frequent exchange of information is difficult to avoid, but the ever-changing variety of pervasive network hackers, as well as the CPC network Army will rise the invisible threat, their degree of danger is definitely inferior to the deployment of missiles along the coast. The responsibility for national security relies on higher degree of alertness, proper measures taken in response..

Keywords: Information security threat、information war superiority、hacker attack、malicious code、network management.

1. 前言

邁克菲實驗室（McAfee Labs）2014年元旦發佈了《2014 年預測報告》，借助其獨有的邁克菲全球威脅智慧感知系統，對 2013 年安全趨勢進行分析並對新一年的威脅態勢作出預測，未來移動資訊化將進入建設高峰期，電腦管理者與使用者對移動安全全面深入瞭解中，在 2014 年，研究發展的移動平臺技術將主導成為惡意程式攻擊威脅之無形戰場。網路具有即時性及無國界的優點，也因此帶給現今繁忙的社會無比便利，現代科技運用網路進行資訊查詢、網路連線通訊或交易，但是面對惡意程式攻擊網路防護防不勝防，使網路攻擊有機可乘。也隨著資訊科技進步，網路戰爭已演變為一場無聲無形的戰爭。面對中共網軍攻擊，我國除應落實資訊安全管理制度等作為，降低危安因素外；更應根據科技進展，強化對未來資安威脅的防護，完善防衛能量。若在使用時疏於防範，則個人電腦中重要資訊將輕易落入有心人士手中，進而發生一連串的負面效應，其危害程度可危及國防安全，實在不容小覷。我們應保持高度警覺，熟悉相關資安管控規定，精進各項管理作為與方式，工作上確實依照標準作業程序，建構最縝密周延的資安防護，才能有效降低風險與危害，維護國軍資訊安全[1-5]。

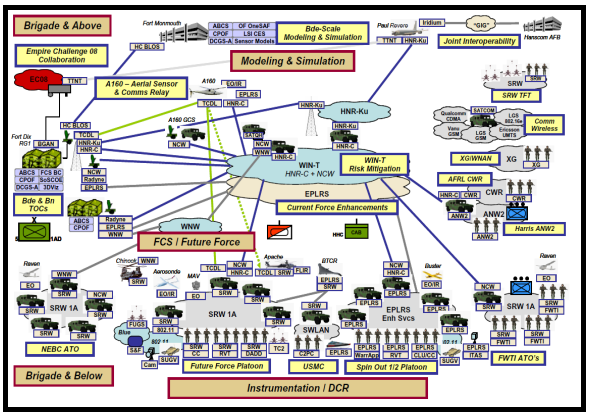
2. C^{4}ISR 理論技術發展研究與分析探討

資訊時代來臨影響所及，隨著資訊安全與網路威脅發展，當今我們所面對的真正威脅，已不再只是單一國家或其內部的軍隊系統，而是一種具有全球性滲透的特性，以及呈現倍數成長的網路攻擊事件。網路攻擊已成為一種新的戰爭形態，它可能對國家目標與國家安全利益造成更大更深遠的不利影響。分析當今戰爭形態，在空間上係以殲擊目標的局部作戰為主。全民國防包含國防軍事、全民防衛及與國防有關之政治、經濟、心理、科技等直接、間接有助於達成國防目的之事務。國防政策之考慮因素包括國際戰略環境、兩岸關係、經濟發展、社會發展、人口結構等影響。假設國家或政府的電腦系統遭到入侵，重要資料被截取或竄改，造成的危害就可能擴及國家整體安全。資訊戰就其層次可分為社會國家、戰略、戰術及戰場等層次，中共將資訊戰稱為信息戰[1-3]。

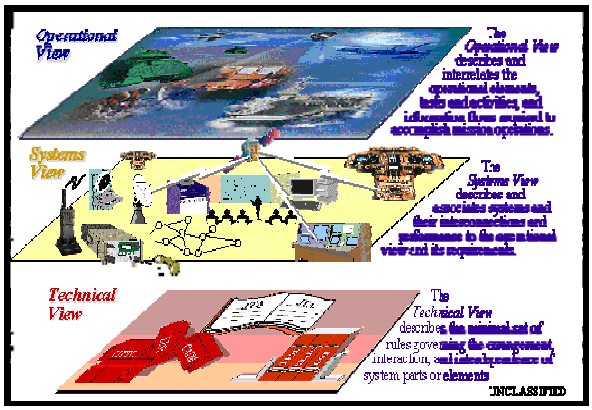
共軍積極整備，朝建立整體優勢電子戰能力的目標努力。網軍利用網路對我實施資料竊取與情蒐工作，侵入敵方指揮網路系統，進行瀏覽、竊取、刪改有關數據或輸入假命令、假情報、破壞敵方整體作戰自動化指揮系統。中國電子戰(稱之為電子對抗)相對各項武器系統中電子設備所占成本大為增加，電子設備技術為先進武器、裝備核心及神經中樞；未來戰爭並積極爭奪制電權成為戰場核心，亦為戰爭「第五種戰場」，武器與裝備能否發揮效力，作戰行動能否成功，均取決於掌握制電權優勢一方。中共主要攻擊模式發展趨勢是利用衛星、通資網路偵搜系統來竊取政治、經濟、軍事戰略，並透過電腦病毒、電磁脈衝炸彈攻勢作為，來干擾武器、戰情系統。未來戰爭發展是數位化與資訊化戰爭形態，掌握未來戰場關鍵是建立通資電優勢，通資電優勢所指的指管通資情監偵系統即為 C^{4}ISR (Command 指揮、Control 管制、Communication 通信、Computer 資訊、Intelligence 情報、Surveillance 監視與 Reconnaissance 偵查)系統是具備大規模與軟體密集特性的系統以提供軍事資訊化指揮管理系統藉以提高指揮效率[2-5]。

美國國防部2006年6月針對此系統整合成立研發工程指揮部(Research, Development and Engineering Command 簡稱 RDECOM)、美國陸軍與通訊電子研究發展工程中心

(Communications-Electronics Research, Development and Engineering Center CERDEC)共同開發網路科技與模擬系統於 2008 年 11 月出版 On-The-Move Event 08 文件，美國防部並將系統依照作業面、系統面與技術面三個層面定義出相關的連接性，圖一為美國陸軍 C^{4}ISR 模組架構示意圖[1]，圖二為美國國防部 C^{4}ISR 系統關聯圖[2]。其中作業面描述任務活動的資料交換以滿足相互獨立的系統，系統面將現存或規畫完成的技術之系統與相互連結與通訊關係加以定義，而技術層面則將系統元件與相互依賴關係所需標準規範及相互管理互動的規則加以訂定。



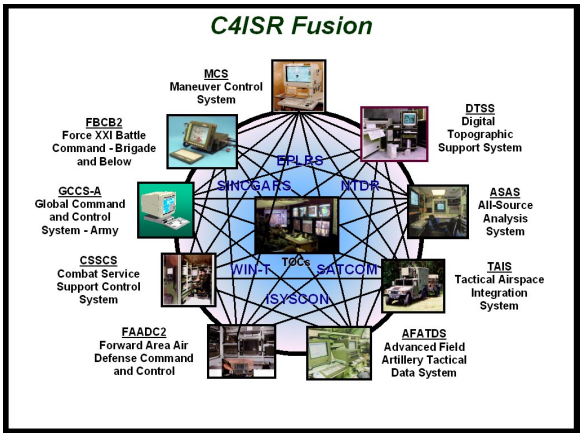
圖一：美國陸軍 C^{4}ISR 模組架構示意圖[1]



圖二：美國國防部 C^{4}ISR 系統關聯圖[2]

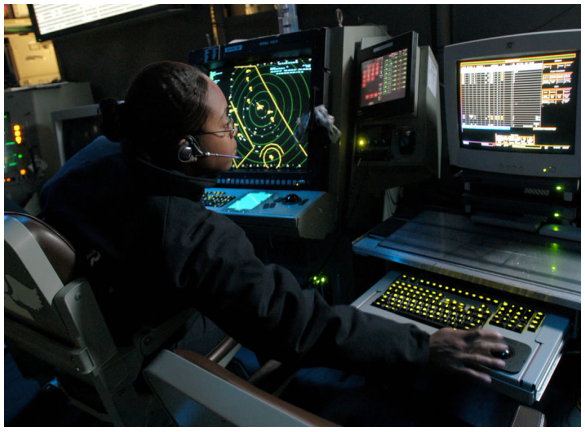
C^{4}ISR 系統是網路型式架構，為支援網路中心戰，電腦是構成自動化系統的技術基礎，是指揮系統中各種設備的核心，每一個 C^{4}ISR 系統平台可配置於載台上，而載台位置無需固定在某一地點，並具有機動性，有些大型的載台可以放置好幾台 C^{4}ISR 系統平台裝備，提供不同任務需求軍事人員指揮與管制操作[3-4]。

美國軍事作戰包括網路領域，聯合作戰與武器系統控制均於網路進行；美軍網路戰因應資訊時代需要，以通資電技術優勢獲取作戰優勢，在美國軍事轉型中佔有極其重要的地位，圖三為美軍國防部 C^{4}ISR 融合架構圖[3]，其融合的包括陸、海、空軍、太空、衛星通訊與戰術等系統；圖四為美國國防工業科技 C^{4}ISR 作戰圖[4]， 圖五為 BAE 公司針對美國海軍研發 C^{4}ISR 系統塔台航行指揮管制示意圖[5]。



圖三：美軍國防部 C^{4}ISR 融合架構圖[3]

圖四：美國國防工業科技 C^{4}ISR 作戰圖[4]



圖五：BAE C^4ISR 塔台航行管制指揮圖[5]

3. 資訊戰演變發展為無形戰爭型態

隨著資訊科技快速進步，電腦與網際網路的運用日益普遍，資訊戰不僅成為國際間廣泛討論的熱點，更被許多軍事戰略學者認為是未來戰爭的主流，甚至認定為「第五戰場」。觀察中國，中共在其管轄網際網路內部建立多套網路審查系統，公安部門、國安部門及新聞宣傳等部門聯合承擔相關行政權責，並輔以各式管制軟體如防火長城等技術手段，對網路活動進行嚴密監控，封鎖著可能影響其國家安全的資訊傳播，同時也對政治內容進行監視和過濾。反觀，美國除將網路攻擊列為全球首要安全威脅，並積極推動資訊安全分享機制、強化基礎網路設施維護，以及減少貿易與技術機密遭竊等相關政策應對；此外，今年度更投入數億美元預算，擴大既有規模安置所需資安組織與設備。另北約組織也於去年六月間，針對如何提高盟國應對現代網路戰爭的能力，以及北約集體網路安全，召開首次的二十八國國防部長會議，均說明「資訊戰」與「網路戰」已為當前各國重視的國防議題[6-9]。

面對中共嚴重威脅，戮力發展各項資訊作戰系統與戰術戰法，旨在爭取資訊優勢，確保國家的安定與發展。中國將資訊戰稱作信息化戰爭，共軍在信息作戰方面可能的犯台模式，已逐漸從全面封鎖、攻擊國軍有生力量，轉變為包括企圖採資訊戰攻擊或破壞我方的指管通情體系。為達成此目的，共軍成立「網軍」，平時蒐集我政府與企業情報，戰時則立即展開攻擊性行動，以有系統地對特定重要目標進行惡意攻擊癱瘓我方電腦網路運作或竊取重要情報與機密文件。觀察中國大陸對我國資訊安全威脅，除了駭客與犯罪性的資通攻擊之外，更面臨中國大陸對我採取組織性的網路攻擊，藉以竊取資料與滲透破壞，這一場無聲無息戰爭的挑釁，儼然形成國家安全的一大威脅[10-14]。

針對資訊戰發展，中共持續積極建構信息作戰能力，通過資訊技術手段實現對敵方資訊和資訊獲取、使用活動的抑制除已將相關理論應用於國家戰略、政治戰略與軍事戰略等階層，相關戰術戰法包括電腦對抗與心理戰等領域，並在戰略與戰術上均分別取得制電磁權優勢為對抗目的。美國國防部 2010 年 2 月發表《2010 四年期國防總檢報告》（QDR），國防部將基本國防戰略改為有能力對抗由恐怖主義到網絡攻擊的一系列威脅，以保護美國在全球的利益與美國國家安全。分析現代戰爭發展趨勢，資訊戰不僅是前哨戰，也是無聲無息的作戰，藉由網路通信技術先期掌握情資，癱瘓敵方軍事系統，進而獲取戰場優勢，成為作戰致勝的關鍵因素。美國表示網路作戰與防衛能力愈來愈重要，美軍必須持續投資開發，因為現今所有戰力都離不開網路，不論是戰場情偵、目標鎖定，或是聯合作戰，都需要運用網路。鑑於網路攻擊行為日益增多，為建構足恃的網路作戰能量，美國、英國、日本、德國等先進國家均已成立網路作戰部隊[15-18]。

日本在其公布 2005 年～2009 年四年期「中期防衛力量發展計畫」中，提出了網路「癱瘓戰」的作戰理論，並組建一支編制五

千人左右、由陸海空自衛隊電腦專家組成的網路戰部隊。近年網路安全及資料外洩等問題，一直困擾政府機關及民間企業，其中駭客（網軍）入侵、病毒感染、阻斷服務攻擊等等惡意程式肆虐等事件層出不窮，因而造成網路中斷、重要資料被竊等情事時有所聞。我國國軍深知資安防護重要性，依國家安全會議及行政院指導，負責國防網際防護任務，以資安防護為核心，負責規劃、推動國軍資安防護及應變等工作，除落實網路實體隔離作業，建置嚴密資安防護機制外，配合資安稽核並主動查察違規事件以強化資安整體安全防護強度[19-25]。

中國從波灣戰爭及 1996 年台海危機後，積極發展資訊戰攻防能量，中共本首戰即決戰的作戰原則，計劃以結合衛星、通資網路等偵蒐系統，全盤獲取對手政、經、均等戰略、戰術資訊；以資訊武器採取攻擊作為，一方面干擾對方武器與戰情系統，癱瘓指揮管制機制，迫敵軍於惡劣環境下接戰，另一方面則入侵破壞民生基礎設施，如電信、金融、水電與交通等資訊系統，影響民眾生計，造成社會秩序之不穩定。中國大陸自 1985 年起，就開始發展「網電一體戰」的能量。大陸國防部發言人耿雁生於 2011 年 5 月間證實，中共已經建立「網路藍軍」，並且強調「組建網路藍軍，就像組建陸軍、空軍一樣。因為我們生活在信息社會，就必須適應這種環境下的新時代戰爭」。針對敵情研析，中共軍隊近年來全力投資各項電子戰對策，以防衛電子攻擊，及建立電腦網路作戰單位，透過網軍攻擊，不斷在網路進行資訊竊取與惡意程式破壞，中共每天製造的木馬和後門病毒至少三百萬次，約佔全球同類病毒的三分之一，已成為網路世界的恐怖主義國家。美國與中國積極發展電腦網路作戰（Computer Network Operations）能力，是建立不對稱性戰略優勢的重要環節，而其中的內涵包括制信息權和制電磁權，並以電子對抗、通信對抗及網路對抗為主要作戰形式。美軍在 2003 年的伊拉克戰爭中，運用以共享通用相關作戰圖為基礎的“網絡中心戰”（Network-Centric Warfare 簡稱 NCW）作戰方式，使指揮控制、偵察監視、綜合通信、火力協調、防空指揮、電子對抗、後勤支援等分系統構成一個完整體系，確保通信裝備、戰位終端設備、導航定位設備及戰位信息綜合處理係統相輔相成連成一體，進而支援聯合作戰從而取得最佳的軍事加乘效果，以下表一為美軍資訊戰發展演變分析表[10-15]。

表一、美軍軍種資訊戰發展演變分析表

軍種	美軍各軍種資訊戰發展演變內容
陸軍	資訊部隊負責蒐集敵人武器系統，培訓指揮員確定這些系統如何使用，擬定資訊戰新指南收錄在《FM100－6 資訊戰》手冊中。資訊處理器使指揮員能夠將整個戰場傳來的各種資訊綜合起來並運用這些資訊有效判斷敵人動向
海軍	艦隊資訊戰中心負責研究海軍及各軍種聯合資訊技術、過程和訓練，作為新軟體試驗場所，有一個整個艦隊電腦安全設置全天候服務危機反應中心，可以為大型海上演習訓練提供資訊戰假想敵來支援反恐作戰或監視區域危機
空軍	美國成立空軍資訊戰中心，其任務是制定一套戰略和戰術，保護美軍的指揮、控制和通信（3C）資源，有效遏制敵方利用空軍指管通資情監偵資訊系統

4. 現代資安威脅與網路管理技術研究

美國國會從 2000 年起要求國防部針對大陸軍事發展發表年度報告；路透華盛頓 2013 年 5 月 7 日報導指出美國國防部今天首度在年度報告直指北京當局試圖入侵美國國防電腦網絡，利用間諜活動獲取加速軍事現代化計畫的技術，網路戰爭早已在世界各地夜以繼日地進行，雖沒有砲聲隆隆、烽火硝煙、血肉模糊的畫面，但是隱藏在電腦的網路戰爭讓人防不勝防，更是危機重重。從資訊保密角度看，小從網路遊戲帳號密碼被盜，大到企業、國家機密外洩，無不造成個人與團體的傷害。在高度電腦化的今日，資訊與通訊安全攸關國家安全，由於電腦網路資料使用極為便利，資訊上傳下載也非常容易，資通安全管理在網路科技環境中益顯重要[16-20]。

網路是駭客入侵的途徑，所以網路的安全是資訊戰的第一道防線，對資訊系統的攻擊是來自多方面的，中共第十八屆三中全會提出「加快完善互聯網管理領導體制」，據此，北京媒體透露中共將會把現有相關的「國家資訊化領導小組」及「中央互聯網資訊工作領導小組」合併為一，成立「資訊化和互聯網資訊安全領導小組」，由中共總書記習近平親任組長、國務院總理李克強及掌管意識形態的中央政治局常委劉雲山出任副組長，以加強管理中國大陸境內的網路資訊與其安全政策，足見中共對於網路資訊戰的重視。中共當局不僅全面掌握了「網絡主權」，更可使共軍藉由網際網路管控來直接提高網路作戰和情蒐能力，對各國造成威脅已是不爭事實。如中共駭客近年入侵攻擊美國政府機關及企業、隸屬共軍總參謀部網軍「六一三九八部隊」攻擊重點不僅止於企業、政府機關的資訊竊取，還包括控制電力網與空中交通控管系統等重要基礎設施、「十八大」召開期間美國谷歌被大面積阻礙連線等，嚴重程度促使去年的歐習會將「駭客網攻」列為首要議題[19-22]。

2011 年 3 月，日本首次舉行網路安全戰略兵推，自衛隊組建網路防護隊徵求民間專家，充實網路安全防護，並與美國合作，提高防禦能力。針對敵情分析，2013 年 3 月 20 日國家安全局長蔡得勝曾提出警告，中共對臺灣的網路攻擊相當嚴重，可能危害臺灣交通運輸及金融秩序，竊取的資料也從軍情，轉向蒐集高科技及商業機密，已遠比恐怖活動更加威脅全球安全，「政府與民眾應該共同重視這樣的問題」。若相關資料及個資遭竊，讓對岸取得納入資料庫，藉由交叉比對，中共即能完全掌握臺灣相關人員的素質和資訊；若國人危機意識不夠的話，讓政府防禦系統難以面面俱到。由於社會逐漸數位化及資訊化，加上中共「網軍」四處蒐集機密資訊，導致世界強權的美國也預測透過「網路 911」的攻擊模式，就能夠延遲、甚至癱瘓整個美國社會的正常運作，因此美國總統歐巴馬決心成立網路戰司令部，以整合當前美軍的網路作戰資源。美國國防部於 2011 年 7 月中旬發佈「網路作戰戰略」，除明確要求五角大廈將網路視同作戰領域，並對來自其他國家的網路駭客攻擊，認定為已構成戰爭行為，將比照陸、海、空三軍，從被動防禦轉為主動攻擊，以因應日益升高的網路安全威脅，同時計劃與民間企業，以及其他美國盟邦共同發展網路作戰能量。美國在 2011 年 9 月間，由當時國防部長潘內達與澳洲國防部長，在舊金山發表聯合聲明，美澳兩國決定將網路領域納入共同防禦條約的主要內容，無論是美國或澳洲單方面受到網路攻擊，兩國將同步採取防禦行動，這也是網路戰第一次被規範在美國與其他國家的雙邊防禦條約中。美國總統歐巴馬在 2012 年 1 月發佈《21

世紀美國國防戰略綱領》將網路空間能力列為最優先發展、重點保障的六大軍力之一。此外，美國白宮於 2013 年祭出 13636 號行政命令，要求改進美國關鍵基礎設施網路安全，針對各國對於資訊安全威脅因應作為分析如表二[20-30]。

表二、各國對資訊安全威脅因應分析表

國家	對資訊安全威脅因應作為分析
美國	將網路攻擊列為全球首要安全威脅，推動訊息安全分享機制、強化基礎網路設施維護，以及減少貿易機密遭竊等相關政策應對；立法限制政府採購中國網通產品；並將網路攻擊部隊人力由五百名提升到四千五百名，預算由二〇一二年三十九億美元，增加到二〇一三年四十七億美元，以強化網路攻防能量。
日本	防衛省年內編列一百億日元成立「網路空間防衛隊」，警察廳四月起於十三個道府縣警局，成立「網路特搜隊」防止網路駭客攻擊。
英國	近將成立「反網路威脅中心」，延攬通訊總部（GCHQ）及軍情五處（MI5）網路專家專責保護網路安全，計劃在 2010 年至 2014 年間，投資六億五千萬英鎊，執行國家安全防護專案。
德國	憲保局為因應社群時代通聯模式與攻擊目標變化，將加強網路早期預警能量；聯情局亦於今年四月組建「網路戰爭處」，招募相關網安人才，應對愈趨嚴峻之國際網路威脅。
中國	執行網電一體戰任務，主要機構包括：解放軍總參四部負責電腦網路運作及電子反制能量的組建；解放軍總參三部負責國防信息化保障任務，並執行戰場網路情報蒐集；在大陸七大軍區設置戰區聯合作戰指揮部，並成立信息對抗中心，負責電子對抗及網路信息體系的防護；大陸軍事科學院及國防大學則是負責研發各種「網電一體戰」的作戰指導與準則，並積極培育訓練各項執行任務的軍官和士兵。
北大西洋公約組織（NATO）	2013 年 4 月北約秘書長拉斯穆森（Anders Fogh Rasmussen）於部長級會議上同意，加強組織的網路防禦能力，以應對不斷增加的網路攻擊，這是北約部長級會議首次提出網路安全議題。共有 28 個會員國的北約國防部長們同意，網路防禦能力在 10 月可以全面運作，延伸網路保護至所有會員國擁有或操作的電腦系統。

5.結語與未來因應作為

現代戰爭中，資訊戰不僅是一場無煙硝的戰爭，亦是武力戰的前哨戰，擁有決定勝敗的重要關鍵；且透過網路和通信技術，將可掌握情資，癱瘓敵人軍事系統，進而獲得戰場上決定性優勢。因此，任何一個國家，一旦相關重要資訊缺乏完善的防護機制，便可能遭受敵人擷取，嚴重威脅國家安全。面對一個新形態的戰爭，才能有效掌握網際網路相互通聯與相互依存特性，進而採取可行的因應對策；而且在實務上必須針對敵人可能採取的惡意程式攻擊行動予以立即性、可控性及預防性之反制作為，以掌握資訊戰場優勢。美國在國家安全策略制定區分為：國

家安全策略、國家軍事策略、國防政策指引及軍種執行指令等各種不同層級的文件。自國家高階的發展性策略，到中階規劃性指引，最後到低階的執行性指令發展完備，並成為確保資安策略一致性貫徹執行的基礎。我國應參考其作法，訂定具體的政策及戰略指導、規劃指引及執行指令，以落實強化資訊安全因應措施的執行。國防部為強化資訊安全管理，訂定資訊安全政策，於建立安全資訊環境時，確保國軍資料、系統、設備及網路整體安全。其主要目標為保資訊機密性、完整性、正確性與可用性；保護國防部資訊資產免遭不當使用、洩漏、竄改、破壞等情事；確保資訊蒐集、處理、傳送、儲存及流通安全，確保國軍資訊受到妥善保護[18-20]。

美國因應資訊站威脅啟動規劃與研究各種先進武器與概念的國防部「先進研究計劃署」(DARPA)，發展網路安全 X 計劃（Plan X）以保障敏感電腦網路不受攻擊，並加強研究網路攻擊能力，以處理特定軍事需求，未來一旦美國與其他國家發生軍事衝突時，第一波攻擊者將不再由戰斧巡弋飛彈或隱形轟炸機擔綱，而是由坐在美國本土的網軍，以各種程式、網路病毒或蠕蟲發動攻擊，癱瘓對手的公開網路，甚至以駭客方式，攻入對手的保密網路，破壞對手指管通情監偵系統，或者從內部摧毀發電廠和通訊等重要基礎設施。面對中共持續強化資訊作戰能力，透過網軍與網路駭客對我造成不可預測之極大威脅，政府可以國軍為領頭羊來積極結合產官學研各界力量，自行研發更精良的全國資安預警及網路防禦系統，以強化整體安全防護機制。為了肆應各種可能的網路駭客手法，政府也已將防護層級升高、廣度延伸至全國，各機關應確實積極配合現階段所推動的資安重點工作，全面加強資安防護能量，以擴大整體防護網絡，共同防範駭客攻擊。其次，提升網路作戰投資，強化網路作戰能力。網路戰爭已成為一場無形戰爭，中共認為資訊戰在未來扮演關鍵角色，網路戰則為資訊戰主要形式，並視電腦網路戰為新形態作戰及不對稱殺手武器。甚至共軍可能利用電磁脈衝等武器，以點穴戰方式，在第一擊時瞬間破壞國軍戰情中心，大量癱瘓國軍網路作戰系統。因此，國軍除了藉資訊作戰部隊建置，累積相關能量外，必須如同嚴明部長指示善用通資電科技，逐步進行不對稱戰力的建構，期能滿足聯戰實需。因應共軍攻擊手法、技術不斷更新，密切掌握中共的網軍部隊動態、發展資訊戰能力，並備妥包括衛星和無線等各種備用傳輸管道，已是當務之急。第三，深化網路心戰，爭取大陸民心向背。第四、健全資訊基礎建設與落實資訊緊急應變機制 [15-22]。

現今資訊作戰形態已無平戰時區分與時空間限制，透過網路駭客攻擊，輕者能夠竊取個人資料與商業科技機密，嚴重以讓關鍵國家軍事機密資料外洩。我國須審慎整體規劃，除打造安全資訊作業環境以深度、廣度及速度三維度，強化資安防禦縱深、建立資安聯防，擴大整體防護網路共同防範駭客攻擊並強化基礎網路設施維護有效發揮統合功能，以達克敵制勝之國家安全目標。因此，有效整合通資網路：為因應未來作戰任務需求，新一代軍事通資裝備系統的構建將持續推動，期整體規劃通資系統作業環境與平台，以整合軍種與聯戰網路為目標，建立作業相容、程序一致聯合作戰通信系統。國防資訊基礎建設：配合國家資訊基礎建設各項推動方案，全力推動國防資訊基礎，以提供軍事戰情、指管、人事、後勤、財務等系統資訊傳遞與交換，並運用各網路與各地區構連交換資訊。國防部長嚴明在 102 年通資電

工作檢討會中期勉國軍運用通資電科技，逐步進行不對稱戰力的建構以滿足聯戰實需，有效掌握資電優勢，支援防衛作戰任務遂行。國防部依據十年建軍構想及五年兵力整建計畫落實各項整備工作，以聯合作戰為目標。在國軍資訊安全規劃構想上以資安組織、資安管控、技術研發、風險管理、資安稽核、資安管理為發展策略，訂定通報應變、防禦偵測、聯防機制、監偵分析、作業規範、資安教育等行動方案，輔以復原備援、交流互通、早期預警、安全部署、合格簽證、攻防演練等配套規劃，落實資訊確保與資安防護之目標，並提昇通報應變成效、推廣資安認知教育、強化資安防護能力及建立國際聯防機制等績效指標，期達降低國軍資安風險，擴大資安防護縱深之效益[21-25]。為因應資訊科技快速發展所衍生之新形態資安威脅，現階段資安政策係以確保國防資訊不受任何有形及無形之破壞為前提，以維護國軍網路之機密性、完整性與可用性：首先強化單位資安環境強化軍網網路架構，落實網路惡意行為管控等措施，完善單位資安防護能量及網路異常告警機制，妥善建置資訊存取、交換運用環境，以滿足資訊作業需求；其次是資安教育訓練配合各級實施高階資安長、資安官資安講習，以強化資安知能；第三是落實儲存媒體管制，重點在集中管制、專碟專用、用畢清除及每日清查檢整等作業，以確維資訊安全。第四是精進資訊資產管理禁止採購大陸製電腦及媒體設備等相關規定並結合資訊資產管理系統，強化網路管理效能。最後是強化軍民網資安環境，落實實體隔離並依規定使用軍民網，確保網路作業環境符合規範要求，以降低網路作業之風險[23-30]。

參考文獻

[1] U.S. Army Research, Development and Engineering Command，C^4ISR OTM E08 Executive Summary，https://publicintelligence.net/c4isr-otm-e08-executive-summary/，2014年12月6日存取。

[2] Steve Carey and Michael Jacobs，Enterprise Architecture in the Defense World - DoDAF / C^4ISR，Extended Enterprise Architecture Framework，2014年12月6日存取。

[3] U.S. Department of Defense，DoD News Briefing，17 May 2001，http://www.defense.gov/news/briefingslide.aspx?briefingslideid=214，2014年12月6日存取。

[4] National Defense Industrial Association，Military Electronics, Networks, as known as C^4ISR seems as Industry Lifeline，14 October 2011，http://www.nationaldefensemagazine.org，2014年12月6日存取。

[5] Defense Industry Daily，BAE Wins US Navy C^4ISR Integration Contract，Feb 18, 2008，http://www.defenseindustrydaily.com/，2014年12月6日存取。

[6] 艾揚科技，C^4ISR系統的作業傳輸方式，艾揚即時訊息技術電子週報第26期，2003年6月24。

[7] 聯合新聞網，鬼網竊103國機密文件、台灣也受駭，2009年3月30日。

[8] Hampton Stephens，陳克人譯，第三領域戰爭，國防譯粹地34卷第七期，10─12頁，2007年4月。

[9] 萬濟人，資訊時代的作戰趨勢─網狀化作戰，國防雜誌第21卷第三期，130─135頁，2006年3月23日。

[10] 錢逢水，解讀信息戰、網絡戰、網絡中心戰，2004年07月22日。
[11] 雅虎新聞，美改國防戰略準備打網絡戰不點名針對中國稱須防範通訊衛星攻擊，香港明報專訊，2010年2月2日。
[12] 美國國防部，《2010四年期國防總檢報告》（Quadrennial Defense Review Report， QDR），2010年2月1日。
[13] Hampton Stephens，陳克人譯，第三領域戰爭，國防譯粹地34卷第七期，13-15頁，2007年4月。
[14] 張玲玲，中共管控網際網路 對內維穩對外情蒐，青年日報軍事版，2014年3月9日。
[15] 中國評論新聞，美國組建駭客部隊，搶佔網路制高點戰勝對手，2007年3月13日。
[16] 吳冠輝，嚴密資安管控、確保演訓安全，青年日報社，2010年4月25日。
[17] 鄭大誠，中共網軍的發展與評估，空軍學術雙月刊，603卷，1-4頁，2008年4月。
[18] 謝宗憲，強化資安防護打贏網路戰爭，青年日報軍事版，2013年12月5日。
[19] 廖宏祥，資訊戰國家戰略，新世紀智庫論壇第23期，2003年09月30日。
[20] 吳明杰，國軍資訊戰力大幅超越共軍，自由電子網，2002年04月26日。
[21] 吳聖超、柴惠珍、林勤經，無線隨意網路的安全，國防通資半年刊第8期，2005年6月30。
[22] 鄒永龍、揚安康，世界新軍事變革─數位化戰場的基礎建設，國防雜誌第22卷第2期，56-62頁，2007年12月。
[23] 國防部通資次長室，認識駭客攻擊趨勢落實資安防護，國防部青年日報社，2014年5月12日。
[24] 李自虎，中共「超限戰」對台運用之可能模式及對我之影響，.國防雜誌第18卷第12期，48-50頁，2003年06月。
[25] 蔡宗恆，掌握資電優勢建構不對稱戰力，青年日報，2013年11月27日。
[26] 社論：資安防護與時俱進　杜絕網攻捍衛國安，青年日報，2014年4月9日。
[27] 國防部通信電子資訊參謀次長室，認識駭客攻擊趨勢 落實資安防護，青年日報，2014年5月12日。
[28] 曾章瑞、陳志誠、張榮鋒，認識資訊戰資訊作戰及政府應有軍政作為，T1：資通安全政策，2006年12月。
[29] 社論：資訊作戰能力攸關勝負-資安防護人人有責，青年日報社，2013年10月15日。
[30] The Epoch US，北約首度談網路安全 將成立防禦小組，大紀元2013年06月05日，http://www.epochtimes.com，2014年12月7日存取。