DOI:10.6237/NPJ.201904_53(2).0009

資訊戰的矛與盾－蘇特系統與區塊鏈技術

海軍上尉　謝圓富

提　　要：

一、「電子戰」是使電磁設備受到削弱和破壞，且具即時性，一旦干擾停止，被干擾的對象就會恢復正常；而「網路戰」(也稱「資訊戰」)是使網路中各處理器產生錯誤操作，具一定持續性，且能擴大影響範圍，甚至有失控的可能，惟「網路戰」對實體隔離，及非通用的通信協議網路卻束手無策。為此，美軍將「電子戰」和「網路戰」相結合，並開發了網路電子一體戰武器「蘇特(Suter)」。

二、指管系統中，雖各站台間具資安防護設備，且採實體隔離的專網架構，但系統中的無線傳輸非實體線路，訊息有被截獲竄改等風險，且隨著現代科技發展，以往認為需長時間才能破解的密碼，現在只需一小段時間就能破解，網路安全愈顯重要。

三、「資訊戰」是未來戰爭的新趨勢，為滿足未來資訊攻擊等需求，建立符合「資訊戰」之指管/電子戰系統是我國當務之急。為能在未來的戰爭中獲得勝利，必須在資訊武器上超敵勝敵；而近年興起的「區塊鏈(Block-Chain)」技術，具有的安全性特點，可強化系統安全與確保資料正確，是值得投入開發的技術。

關鍵詞：蘇特(Suter)、指管系統、區塊鏈(Block-Chain)

壹、前言

以往在軍事上大多採用殺傷力大的武器，以快速獲得勝利；而在資訊化時代，則透過破壞敵方資訊系統，來摧毀敵方決策與指揮能力，從而取得戰爭勝利，過程中，甚至不會有己方人員傷亡，因此，「資訊戰」將會成為未來戰爭型態的主軸。誠如《孫子兵法》－謀攻篇提及：「不戰而屈人之兵，善之善者也。故上兵伐謀，其次伐交，其次伐兵，其下攻城[1]。」這一句說明戰爭的最高境界，就是不透過交戰而降服所有敵人，而使用武力乃是不得已而為之的方式。

「網路戰」也稱「資訊戰」是為干擾、

註1：星逝，〈《孫子兵法》第三篇 謀攻〉，隨筆，2009年8月20日，http://cutemike520.blogspot.com/2009/08/blog-post_9032.html，檢索日期：2019年1月8日。

破壞敵方網路訊息系統，並保證己方網路訊息系統的正常運行，而採取的一系列網路攻防行動。「資訊戰」正在成為高技術戰爭的一種日益重要的作戰模式，由破壞敵方的指揮控制、情報訊息和監偵等軍用網路系統，甚至可以悄無聲息地癱瘓、瓦解、控制敵方的商務、政務等民用網路系統，而不須實際攻城掠地。發展迄今，現在資訊安全已是全球性的問題，國家對資訊基礎建設的依賴越來越重，隨著網路興起也使得近年來網路上的資安事件不斷發生，即使防禦嚴密的系統也很容易被入侵與破壞，除了嚴重影響個人及企業，對國防資訊系統的安全也是一大隱憂；且在戰場上同樣適用，藉由網路破壞訊息傳遞，將使戰場武器、裝備、人員完全失靈，其破壞程度完全不亞於傳統的戰爭，卻沒有人員可能因此受傷死亡。

為使國軍瞭解新一代「資訊戰」武器系統-「蘇特(Suter)」及近年興起的安全性技術-「區塊鏈(Block-Chain)」，本文將以2007年以色列使用「蘇特」機載系統攻擊敘利亞為例，介紹「蘇特」與其攻擊手法，並以此延伸出本軍指管系統可能被入侵的方式與相對應的防制作為；另分析「區塊鏈」技術導入指管系統，以提高系統安全性、資料正確性與減少被入侵的機率，達到指管系統最大效能，提高指揮效率。畢竟唯有認識「資訊戰」的本質，才能在未來戰爭中降低損失，並確保能夠取得戰爭的勝利。

貳、「電子戰」與「資訊戰」的結合應用-「蘇特」系統

傳統的「電子戰」是使特定的電磁應用設備使用效能受到削弱和破壞，但這種破壞具有即時性，一旦干擾停止，被干擾的對象就會恢復正常工作效能。其中，只有電子摧毀才能造成永久性的毀傷能力；而電子偵察只能偵查出潛在的電磁威脅能力，偵察行為本身並不能對偵察對象構成實質的損害，因此需要反輻射飛彈(Anti-Radiation Missile，ARM)這樣的武器，對目標進行攻擊。而一般的「資訊戰」則是使網路中各個處理器產生錯誤操作，具有一定的持續性，並且還能衍生擴大效能影響範圍，甚至有失控的可能。這也是人們將「資訊戰」比喻成資訊時代的「核武器」之一。儘管如此，傳統的「資訊戰」對於物理隔離，以及非通用傳輸協定的網路卻束手無策。

為此，一直處在世界軍事技術領先地位的美軍，將「電子戰」和「資訊戰」相融合，並開發了一種神秘的網路電子一體戰武器「蘇特[2]」，美國空軍自2000年開始多次利用聯合遠征部隊演習，秘密試驗「蘇特」系統，之後開始採取漸進式推進方法，以兩年為週期，不斷改進其偵察能力、欺騙能力、運算法能力與評估能力等等，且蘇特是一種通過無線方式進入敵方資訊網路，並癱瘓其防空體系的武器，即使將實體隔離當作防禦盾，蘇特這支「長矛」也能刺穿這張盾牌。

註2：武備志，〈詳解：為何俄駐敘利亞S-400面對以色列F-35空襲成擺設〉，每日頭條，2017年10月23日，https://kknews.cc/military/65xzmal.html，檢索日期：2019年1月8日。

附表：「蘇特」系統各型號性能概略表

型　式	作　戰　目　標	特　點
蘇特1	俄製防空飛彈系統	即時監視敵方雷達圖像
蘇特2	機動戰術彈道飛彈系統、一體化防空系統、指揮控制網路、戰略飛彈指揮控制網路。	通過敵方傳感器天線等入口，植入惡意封包，使用系統管理員身分控制敵方防空網路並操作其傳感器。
蘇特3		可入侵敵方時敏目標鏈路。
蘇特4		可有效攻擊敵方時敏目標。
蘇特5	國家級戰略指揮控制系統、一體化戰略防空系統、反衛星系統、通信系統。	運用電子攻擊、網路作戰、情偵監(ISR)作戰等手段，透過指揮控制節點等系統共享信息。
蘇特6		
說明：「蘇特」系統最終目標：具滲透敵方信息通信網路，具備使其防空系統與指揮體系失效的能力，即戰場信息通信網路不可用或為美軍所用。		

資料來源：武備志，〈詳解：為何俄駐敘利亞S-400面對以色列F-35空襲成擺設〉，每日頭條，2017年10月23日，https://kknews.cc/military/65xzmal.html，檢索日期：2019年1月9日。

目前已經實驗了6代(「蘇特1」至「蘇特6」)，以下針對概略性能(如附表)逐一介紹：

一、各個型號的「蘇特」作戰目標如下

(一)「蘇特1」主要針對俄製防空飛彈系統。

(二)「蘇特2至4」進一步拓展到機動戰術彈道飛彈系統、一體化防空系統和指揮控制網路、戰略飛彈指揮控制網路。

(三)「蘇特5」與「蘇特6」擴展到國家級戰略指揮控制系統、一體化戰略防空系統及反衛星系統等，並可進一步擴展至通信系統等戰場信息系統。

二、各個型號的特點

(一)即時監視敵方雷達能力

「蘇特1」系統監視雷達的探測結果，能夠即時監視敵方雷達圖像。

(二)通過無線入口植入能力

「蘇特2」允許攻擊者通過敵方傳感器天線、通信天線以及微波中繼站天線等入口，植入惡意網路封包，以及使用系統管理員的身分控制敵方防空網路並操作其傳感器(主要為敵方雷達)，使其搜索不到美軍及盟國突襲的飛機，或利用假目標進行欺騙。

(三)入侵敵方即時敏感目標(Time Sensitive Target，TST，通譯為時敏目標)能力

「蘇特3」系統可入侵敵方時敏目標[3]鏈路；「蘇特4」系統則可有效攻擊敵方時敏目標等。

(四)運用綜合手段打擊能力

「蘇特5」與「蘇特6」綜合運用電子攻擊、網路作戰、情偵監(ISR)作戰等手段，透過在指揮控制節點、資訊戰操作員、情偵監平台、電子戰攻擊系統與「網路中心協同瞄準系統(Network-Centric Collaborative Targeting[4]，NCCT)」共享信息，實現了快速開發、執行及評估動能與定位方案。

而「蘇特」源於美國空軍為彌補當初對敵防空系統攻擊能力不足而提出，由英國航太系統公司(BAE)研製的機載資訊戰攻擊系

註3：指具有「發射後迅速逃逸」特徵的目標。如彈道飛彈核潛艇和移動式低空飛彈發射車等在移動與發起攻擊時比較容易被發現，但在隱蔽時無法被發現，就是典型的時敏目標。

註4：AIR FORCE TECHNOLOGY,” The Israeli ‘E-tack’ on Syria–Part I”,9 MARCH 2008. https://www.airforce-technology.com/features/feature1625，檢索日期：2019年2月1日。

統，其提出了一套以網路為中心的資訊戰作戰能力，是一種空中網路攻擊系統，或者可以做為一個軍事電腦方案，攻擊屬於敵人的電腦網路和通信系統，它專門干擾綜合防空系統的電腦，這些被干擾的電腦可以使雷達轉向錯誤的方向，或顯示假目標，完全破壞或控制與防空網路有關的軟、硬體。

介紹「蘇特」時，也必須提到「網路中心協同瞄準系統(Network-Centric Collaborative Targeting，NCCT」，該系統由L-3通信(Communications)公司開發，是一種開放式的網路中心戰設施和軟體系統，這一系統綜合偵查和搜索系統，對其數據進行網路化的協同處理，降低定位誤差，並增強時效性，能夠快速對目標進行定位，對作戰人員提供準確的情報支持，網路中心協同瞄準系統設計的目標是能夠在數秒鐘之內，蒐集並融合多個平台所獲得的各類情報數據，同時對敵方的輻射源進行識別跟蹤與定位。

三、攻擊方式

「蘇特」最終的目標是使敵方防空系統失效，這要透過聯合使用「電子戰」和網路攻擊技術才能實現，其手段是攻擊並進入敵方的指揮通信網路(攻擊示意圖如圖一)，囿於美國絕對保密「蘇特」攻擊的具體技術，因此僅能通過對「蘇特」實驗的分析，與採用現代無線電技術、網路技術及「電子戰」等可以實現網路攻擊能力的作法，推斷「蘇特」系統可能的攻擊方式[5]，包含注入假目標、注入假指令與隱身等三種方式。

(一)注入假目標

圖一：「蘇特」系統攻擊示意圖

資料來源：作者整理繪製。

注入假目標主要是利用無人機載傳感器和電子偵察機的偵查結果，經過計算得出注入假目標的相關參數後，再由電子戰飛機向敵方多部雷達同時注入多個假目標。在「蘇特1」中實現的監視能力，是進行網路攻擊的基礎，因此有四項主要步驟：

1. 藉無人機載傳感器在敵區附近偵查敵方雷達信號，包括雷達探測信號和回波信號、無線通信天線輻射的信號和數據，由無人機載傳感器通過轉發網路進行簡單數據融合後，發給戰場機載通信節點，再由戰場機載通信節點轉發給電子偵察機，基於通信距離的考量，戰場機載通信節點是由中繼飛機擔任。

2. 電子偵察機自身偵查的數據和從戰場機載通信節點接收的數據，通過網路中心協同瞄準系統在網內共享，如此，電子戰飛機接收到敵方雷達的信號數據、地理位置等資訊，然後經過程序計算出要注入的假目標的航線數據(包括假目標的方位、仰角與對方

註5：趙敏，〈網路中心戰的網路攻擊-Suter計劃〉，《現代防禦技術》，第39卷，第6期，2011年12月，頁141-143。

雷達的距離，與電子戰飛機向對方雷達發射脈衝的時間及發射功率等），以達到成功注入假目標，混淆敵方指揮的目的。

3.電子戰飛機從敵方雷達的各個方位注入多個不同方向、不同距離和不同航線的假目標。

4.電子偵察機監視敵方無線通信信號，以確認數據流對敵方雷達是否產生預期的影響；如果沒有，則由無人機載傳感器在敵區附近持續偵查敵方雷達信號，並再依前述步驟實施攻擊。

(二)注入假指令

在「蘇特」計畫中不僅可以偵測到對方雷達的信號和數據，還可以偵收對方防禦系統的各種無線通信天線發出的報文，進行處理、破譯解密，獲取無線通信的協議和消息內容。對無法即時破譯和解密的報文，可發回己方的高級破譯和解密單位，並將破譯和解密結果及時反饋給控制中心，消息內容可能有：觀測到的目標及其數據、各種防空雷達及武器準備情況及工作狀態、目標指示和目標分配情況攔截結果等。對這些消息內容，可按己方意圖進行修改，變成假指令，由電子戰飛機傳送給對方無線接收系統，以改變對方的作戰行動或裝備操作。

例如在作戰過程中，要改變對方指揮中心所發出的打擊美軍戰機的指令，一般作法有四個步驟：

1.由無人機傳感器和電子偵察機共同完成截獲對方雷達向指揮所報告的目標訊息，電子偵察機經過破譯解密，修改目標信息的內容，通過網路中心協同瞄準系統發送給電子戰飛機，並由電子戰飛機發送給對方指揮所的通信天線。

2.偵測到對方雷達發現美軍戰機，並向指揮所的通信天線發送。

3.一旦敵方指揮所通過無線通信系統向武器系統發送作戰指令，就會被美軍截獲，這時電子偵察機更改作戰指令中的目標信息以及截獲時間等數據，透過網路中心協同瞄準系統發送給電子戰飛機。

4.電子戰飛機再將修改後的作戰指令發送給對方武器系統，指揮對方武器系統攻擊假目標或對方自身目標，這樣就改變了對方指揮所發送給武器系統的原作戰指令，對方武器系統實際執行的是經過美軍更改後的假指令。

(三)隱身

通過2007年以色列成功空襲敘利亞的實戰應用來看，使己方不具備隱身能力的作戰飛機避開對方防空雷達，從而具備隱身的能力是完全可以做到的。以下簡述3種可以達到隱身效果的技術。

1.降低對方雷達接收機靈敏度：

一般雷達為了增大接收機的動態範圍，採用自動增益控制和瞬時自動增益控制等技術，保證接收機對大目標和小目標都能正常運作。當電子戰飛機向對方雷達注入假目標或假地形信號功率過強時，就會超過自動增益控制和瞬時自動增益控制的正常工作動態範圍，使接收機靈敏度大幅下降，導致對方雷達觀測不到中、小目標的回波信號，從而達到中、小目標隱身的目的。

因此可利用向對方雷達注入過強的假目

標或假地形雜波信號技術，以降低對方雷達接收機靈敏度(降低接收機增益)，使對方雷達不能發現目標，從而達到中、小目標隱身的目的，或將無隱身能力的中、小飛機變成隱形飛機。

2. 控制對方防空系統：

美軍人員以系統管理員身分控制對方防空網路，並操縱對方雷達的轉動方向，使其避開美軍戰鬥機的航向，在錯誤的方向上搜索，總之使對方雷達監測不到美軍突襲的飛機，同時，即使對方的操作員知道他們的系統被對手劫持，奪回系統的控制權亦非易事。

3. 使敵方做出錯誤指揮命令：

通過電子戰飛機向對方指揮所發送假目標，例如偏離美軍突襲飛機航向並且離對方設施更近更具威脅性的假目標，造成對方跟踪或攻擊這些假目標；發送誤導行動的作戰指令，例如錯誤的威脅告警或目標指示信息，使對方做出錯誤的作戰命令。

綜上有關「蘇特」之介紹，或許太過抽象，但「蘇特」系統是經過實戰驗證的，2007年9月以色列為防止敘利亞擁有核武科技，派空軍順著土敘邊境進入敘利亞領空，同時電子干擾機成功干擾了敘利亞位於土敘邊境塔爾阿貝德的雷達站，隨後攻擊機群將部署在此地的機動雷達和雷達站一併摧毀，而外界猜測可能使用「蘇特」系統干擾了敘利亞雷達[6]。而「蘇特」不僅可以對敵方雷達實施干擾，還可以破解敵方雷達系統，並控制雷達傳感器，使得敵方不知道雷達已被干擾進而無法做出預警。顯見「蘇特」可確定敵方電磁波發射台(如：雷達)的準確位置，以及誤導包括控制在內等許多活動，並於必要時結合傳統實體攻擊手段，使其最終失效或破壞。

參、海軍指管系統面對的威脅

因為「蘇特」具有滲透進敵方信息通信網路，使其防空系統與指揮體系失效的能力，且「蘇特」主要攻擊對象是無線網路，通過敵方無線網路等入口，植入惡意網路封包，以達成控制敵方系統或注入假目標等目的，而海軍指管系統網路區分為有線網路與無線網路(架構如圖二)，所以海軍指管系統確實有遭入侵的可能，可能入侵的方式，及可採取的解決方案，概述如后。

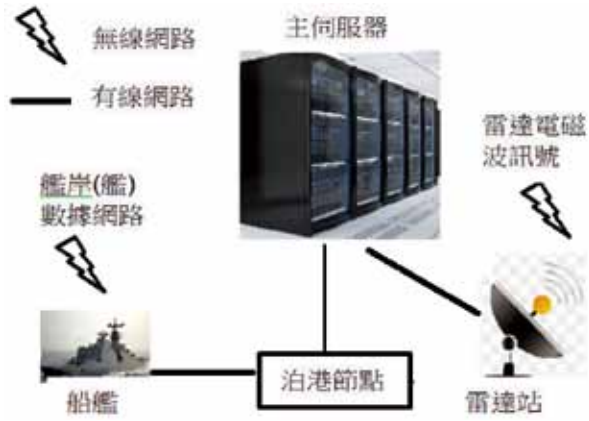
一、無線網路入侵方式

海軍指管系統的無線網路是使用相同頻率、工作模式(如跳頻、展頻等)與金鑰互相傳遞資訊，而如果敵方使用「蘇特」系統通過無線網路入口(如：雷達站)成功入侵系統，並植入惡意封包以癱瘓網路或注入假目標致做出錯誤命令，甚至敵方進而控制系統管理權限(無線網路入侵，如圖三)，我方便有可能遭遇跟敘利亞相同處境，連系統遭入侵都不自知。

二、防禦手法

在資訊化時代來臨之際，網際網路已成為大家高度倚賴的傳播媒介。「資訊戰」的防禦是以維護國軍資訊系統的安全為主，因此以下提出六點針對無線網路攻擊的防禦手法，以避免系統遭敵進一步入侵，而如在平

註6：Saturn V，〈以色列總愛幹這事：裝逼成功卻不承認，揭秘炫酷的「黑色行動」〉，壹讀，2016年5月4日，https://read01.com/zh-tw/gkmL6z.html#.W4uFpOgzZQI，檢索日期：2019年1月9日。



圖二：海軍指管系統架構示意圖

資料來源：作者研究整理繪製。

圖三：無線網路入侵示意圖

資料來源：作者研究整理繪製。

時以危機處理方式，針對敵方可能遂行之攻擊方式，演練各項因應作為，強化應變能力；在戰時，則經由指管系統掌控全軍資料傳輸，確保指管機制與神經中樞運轉之安全無虞。

(一)我方操作人員必須有警覺不定時更換頻率與工作模式(如跳頻、展頻等)，使敵方無法確切掌握。

(二)雷達發射天線和接收天線的位置分開，因發射天線位置容易被定位，而採取隱蔽措施的接收天線則難以定位，從而增加注入假目標信號的難度。

(三)我們常用的電腦常遇到系統更新的情況，由於存在許多未知的漏洞，可能成為系統安全性的死角，系統廠商會不斷釋出更新修補漏洞。同樣的，無線網路設備也面臨各種安全漏洞，這也是資安疑慮與風險所在，所以雷達或相關設備必須時常更新軟體，無法更新軟體之老舊雷達必須汰換，以防止敵方利用該漏洞實施無線網路攻擊。

(四)提高無線通信系統的抗干擾能力，並針對資料傳輸通道及資訊封包加密，除了選擇較安全的加密方式之外，同時也需要設定一組金鑰來保護無線網路的存取，最好也能定期更換金鑰，以免成為攻擊目標。

(五)我方無線網路站台(如：雷達站)可自行發射假訊息或假目標之網路封包，混淆敵方判斷與干擾敵方定位。

(六)用防空武器或反彈道導彈武器摧毀敵方的網路攻擊，包括敵方的偵察手段、「電子戰」和「資訊戰」手段和作戰飛行器等。

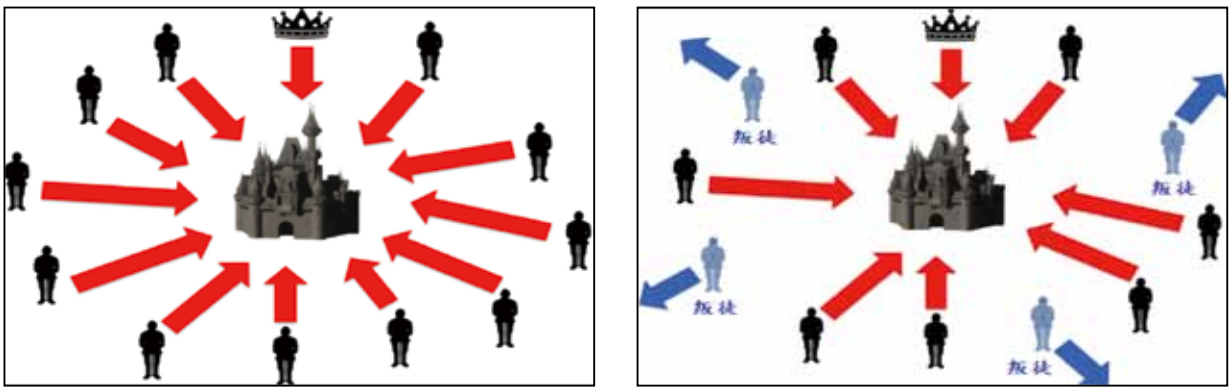
肆、提高系統安全的新技術－區塊鏈

近年區塊鏈[7]觀念興起，它去中心化[8]與不可竄改性[9]等特性，使它逐漸被應用於各

註7：Lydia，〈「區塊鏈」到底是什麼？專業懶人包在這裡〉，CloudMile，https://www.mile.cloud/zh-hant/what-is-blockchain/，檢索日期：2019年1月9日。

註8：區塊鏈是一個去中心化的系統，意即如果你想要改變什麼，那就得經過多數人同意，而這些多數人通常分布在各個國家，並且難以追蹤，因此去中心化的區塊鏈很難受到政府或者財團的限制。

註9：區塊鏈中的每一筆資料一旦寫入就不可以再改動，只要資料被驗證完就永久的寫入該區塊中，透過一對一的函數來確保資料不會輕易被竄改，這種函數很容易被驗證，但卻難以破解，無法輕易回推出原本的數值，資料也就不能被竄改。



一致的攻擊導致勝利　　不一致的攻擊導致失敗

圖四：拜占庭問題示意圖

資料來源：Lydia，〈「區塊鏈」到底是什麼？專業懶人包在這裡〉，CloudMile，https://www.mile.cloud/zh-hant/what-is-blockchain/，檢索日期：2019年1月10日。

領域中，因為這些特性，如將區塊鏈與指管系統相整合，則可提高系統的安全性及降低被入侵的機率，以達成指管系統最大效能，並提高指揮效率。

一、緣起

區塊鏈的源起有兩種說法，首先是今日土耳其的伊斯坦布爾，是當年東羅馬帝國的首都拜占庭，當時東羅馬帝國國土遼闊，在國防配置上，每個軍隊的駐點都相隔遙遠，將軍之間只能依靠信差來傳遞重要消息，因此對外作戰的時候，內部所有的將軍和大官員需要達成一致的共識，才能夠決定是否出兵，但若軍隊中存有叛徒或是間諜更可能影響將軍的判斷，結果往往不能夠得到大多數人的意見，在已知有成員謀反的情況下，如何連結相隔遙遠的軍營來取得一致協議，就成了有名的「拜占庭問題(The Byzantine Generals Problem)」(如圖四)。

拜占庭問題在網路世界的解讀，是在容許入侵體系的一種模型化，後來發現區塊和區塊鏈可以解決這個問題，1982年美國計算機科學家萊斯利・蘭波特(Leslie Lamport)把軍中各地軍隊彼此取得共識、決定是否出兵的過程，延伸至運算領域，設法建立具容錯性的分散式系統，即使部分節點失效，仍可確保系統正常運行，並可讓多個基於零信任基礎的節點達成共識，並確保資訊傳遞的一致性，而2008年出現的比特幣區塊鏈便應用了此觀念。

第二個也就是大家所熟知的區塊鏈起源就是「比特幣」，為了比特幣而產生了區塊鏈，比特幣就是區塊鏈的第一個應用。比特幣的發明人中本聰(Satoshi Nakamoto)在2008年發表了一篇名為「比特幣：一種對等式電子現金系統(Bitcoin：A Peer-to-Peer Electronic Cash System)[10]」的論文，提出

註10：區建仲，〈比特幣的核心技術，區塊鏈的原理與應用（上）：比黃金還貴的比特幣〉，財經新報，2017年5月11日，https://finance.technews.tw/2017/05/11/block-chain-principle-and-application-bitcoin-pt1，檢索日期：2019年1月10日。

圖五：區塊鏈概念示意圖

資料來源：王宣智，〈區塊鏈是什麼？為什麼連美國國防部都搶著投入？〉，泛科技，https://blablablock.asia/archives/69，檢索日期：2019年1月12日。

了稱為「比特幣」的電子貨幣及其演算法，後來有人將比特幣的部分技術抽離出來，尋找新的應用，並且取了新名字「區塊鏈」，這就是區塊鏈這個名稱的由來。

二、區塊鏈概念

區塊鏈是一種分散式的資料庫[11]，最初被應用在比特幣上，為去中心化交易平臺的概念性驗證，採用密碼學來控制貨幣的生產和轉移，屬於加密電子貨幣，所有成員都能夠參與貨幣的驗證交易和記錄電子貨幣，在交易過程中不需再通過任何金融機構或第三方機構進行擔保與驗證(如圖五)。區塊鏈維護著一份連續不斷的交易紀錄檔，每筆資料被稱為一個區塊(Block)，單一區塊內可以包含一筆以上的交易資料，任一個區塊均會與另一個區塊連結，區塊上會有一個獨特的雜湊值(Hash Values)[12]，通過區塊間的彼此驗證，將每一個區塊彼此連結形成了鏈(Chain)，換言之，區塊鏈就是由多個區塊組合而成的一個資料鏈。區塊鏈中的每筆區塊一旦產生即無法更改，每一筆資料都能夠透過連結找出所有可靠的歷史資料，資料會分散於每一個節點，而資料庫的完整性則由所有節點共同維護。

三、運作流程

在比特幣區塊鏈中，當一筆交易經由某個節點或錢包產生時，這筆交易需要被傳送給其他節點來作驗證，作法是將交易資料經由數位簽章加密並經由雜湊函式得出一串代表此交易的唯一雜湊值後，再將這個值廣播給比特幣區塊鏈網絡中的其它參與節點進行驗證。以下是以未來導入區塊鏈技術的金融轉帳為例：假如A要匯款給B，則將這筆交易的資訊先收集至區塊內，並將此區塊廣播傳送給所有銀行主機實施驗證，通過驗證後，將此筆交易區塊接上區塊鏈，A即可成功轉帳至B帳戶(如圖六)。

(一)產生一筆新交易：一筆新交易產生時，會先被廣播到區塊鏈網路中的其他節點。

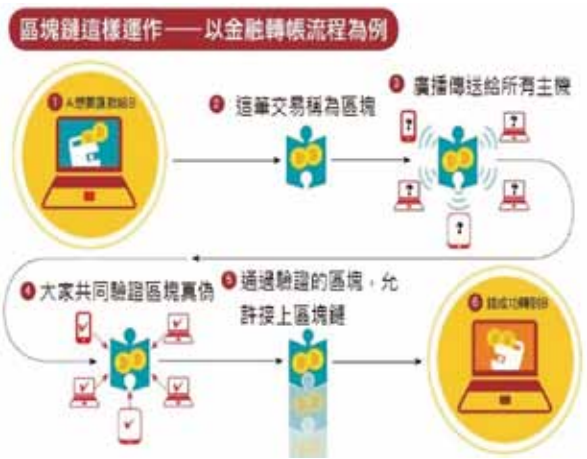
(二)各節點將數筆新交易放進區塊：每個節點會將數筆未驗證的交易雜湊值收集到區塊中，每個區塊可包含數百筆或上千筆交易。

(三)決定由誰來驗證這些交易：各節點進行工作量證明(POW[13])的計算來決定誰可以驗證交易，由最快算出結果的節點來驗證交

註11：王宣智，〈區塊鏈是什麼？為什麼連美國國防部都搶著投入？〉，泛科技，2017年3月1日，https://panx.asia/archives/56913，檢索日期：2019年1月10日。

註12：雜湊函式把訊息或資料壓縮成摘要，使得資料量變小，將資料的格式固定下來。該函式將資料打亂混合，重新建立一個雜湊值(hash values)。

註13：陳柔蓁，（區塊鏈技術 PoW與PoS），自由時報，2017年12月28日，http://ec.ltn.com.tw/article/paper/1163926，檢索日期：2019年1月12日。



圖六：區塊鏈運作流程圖(以未來導入區塊鏈技術的金融轉帳爲例)

資料來源：張小玫、杜君妮，〈區塊鏈弱點可能對用戶造成隱憂〉，科技產業資訊室，http://www.bigdatarchitect.com/blog/ba74cd1c82e，檢索日期：2019年1月12日。

易。

(四)取得驗證權的節點將區塊廣播給所有節點：最快完成工作量證明的節點，會將自己的區塊廣播給其他節點。

(五)各節點驗證並接上新區塊：其他節點確認這區塊所包含的交易是否有效，確認沒被重複花費且具有效數位簽章後，接受該區塊，此時區塊才正式接上區塊鏈，無法再竄改資料。

(六)交易驗證完成：所有節點一旦接受該區塊後，先前沒算完工作量證明的區塊會失效，各節點會重新建立一個區塊，繼續下一回工作量證明計算工作。

若能將以上的區塊鏈運作流程，應用至指管系統新增海空情目標，其運作流程如下：

(一)新增一筆目標：A站台發現目標隨即新增一筆海空情目標，以利其他站台也能識別。

(二)將新增目標放進區塊：將未驗證的新增目標雜湊值蒐集到區塊中，並將此區塊廣播傳送給其他站台來執行驗證計算。

(三)決定由哪個站台來驗證新目標：各站台進行計算來決定誰可以驗證目標，由最快算出結果的站台來實施驗證，並將自己的區塊廣播給其他站台；另因區塊鏈的去中心化特性，使各站台的地位均相等，所以沒有以往主伺服器與用戶端設備的區別，因此，每個站台也等同是一部主伺服器，就算遭敵軍摧毀一站台，餘站台仍可發揮指管系統功能，不影響區塊驗證與資訊傳遞。

(四)各站台驗證：其他站台確認這區塊所包含的資訊，且確認沒被重複驗證及具有效數位簽章後，接受該區塊，也代表此訊息的正確性，並可以順利傳遞。

(五)接上新區塊：此時通過認證的區塊正式接上區塊鏈，表示此區塊的資訊已在系統間流通，意即此階段即使指管系統遭敵軍入侵，欲更改相關參數，擾亂我軍訊息傳遞，亦無法再竄改資料。

(六)新增目標完成：通過認證的區塊接上區塊鏈後，即完成新增此筆目標。

四、特性

區塊鏈有幾個最重要的特性，首先就是它的核心宗旨－去中心化，為了強調區塊鏈的共享性，讓使用者可不依靠額外的管理機構和硬體設施、讓它不需要中心機制，因此每一個區塊鏈上的資料都分別儲存在不同的雲端上，計算和儲存都是分散的[14]，每個節

註14：楊少康，〈區塊鏈的優缺點都有哪些？〉，未來財經，2017年10月24日，https://kknews.cc/zh-tw/tech/b49pmj6.html，檢索日期：2019年1月12日。

點都需要自我驗證、傳遞和管理，這個去中心化是區塊鏈最突出也是最核心的本質特色，同時也就衍生出了區塊鏈的安全性及開放性等特性，就以導入區塊鏈技術的指管系統來說，已經沒有主伺服器及用戶端的區別，任何一個雷達站損毀，其餘各站台仍可繼續傳遞與分享海空情目標的資訊，且新增上傳一筆目標時，均須由所有站台執行驗證，大幅減少了資料可能被竄改的風險，進而提升指管系統資料的正確性與安全性，而針對區塊鏈的特性，摘述如后：

(一)去中心化

所有站台的權利和義務都相等，無以往主伺服器及用戶端的分別，即每台都是伺服器與用戶端，因此任一站台停止工作都不影響系統整體的運作，就算遭敵軍摧毀任一雷達站，仍不影響指管系統整體的運行。

(二)集體維護/開放性

因區塊鏈具有集體維護的特性，所以整個指管系統是由其中所有站台共同維護的[15]，且因開放的網路架構，任何站台都可以通過查詢介面去尋找所需要的數據。

(三)安全性

區塊鏈的數據是分散式的演算，因此沒有人可以隨意修改網路上的數據，去除掉了人為操控的可能，也就讓區塊鏈本身相對安全[16]，且站台新增的敵情目標，也須經由所有站台實施驗證通過後，才可順利上傳至指管系統，所以就算其中一個站台的資料已遭竄改，便可在驗證過程中，得知誰已被入侵，以確保系統資料的正確性與安全性。

(四)不可竄改性

區塊鏈中的每一筆資料一旦寫入就不可更動，只要資料被驗證完就永久的寫入該區塊中，即便系統已遭敵軍滲透，仍無法更改相關參數，擾亂我軍的指揮判斷。

五、運用分析

區塊鏈是一個去中心化與集體維護的網路，且每隨著新增一筆資訊時，均需由網路上的各個節點去實施驗證，因此它的安全性就相對比較高，而現在使用的指管系統是主從式架構，主伺服器一旦被入侵或毀損，則整個系統將無法發揮原有功能，若指管系統能導入區塊鏈技術，將不再有主伺服器與站台之分，而是每個節點均有相同的功能，且如欲成功新增或修改海、空情目標，須由系統上的每個節點共同驗證通過後，才可執行，因此就算敵方截取我軍無線網路傳輸的資訊封包，也大幅增加破譯的難度與時間，此更可保證系統的安全性與資料的正確性。

資訊傳輸的安全，將影響著國家安全或軍事活動的成敗。現今國軍網路雖是透過實體隔離的網路架構，藉以提升安全性，然而在軍事的應用上，資訊傳輸的使用者並非均位於封閉式網路內[17]。在開放式環境的資訊傳輸中，過去通常採用集中式的系統，通過

註15：端小二，〈以去中心化為特徵的區塊鏈技術，會為我們帶來一個更好世界嗎？〉，科技黑鏡，2018年4月13日，https://theinitium.com/roundtable/20180413-roundtable-tech-blockchain/，檢索日期：2019年1月13日。

註16：周維忠，〈區塊鏈技術的衝擊與課題〉，資策會，2016年10月9日，https://www.iii.org.tw/Focus/FocusDtl.aspx?f_type=1&f_sqno=I%2FO8yiy831hzYkZviFdfPw__&fm_sqno=12，檢索日期：2019年1月13日。

註17：王宣智，〈區塊鏈是什麼？為什麼連美國國防部都搶著投入？〉，國研院科政中心，2017年3月1日，https://panx.asia/archives/56913，檢索日期：2019年1月13日。

複雜的驗證機制後，情資人員或使用者方能取得部分的資訊。然而集中式系統，其資訊傳輸路徑易被掌握，進而可能導致資訊在訊號轉接的過程中被竊聽，而如果透過區塊鏈分散式的系統架構，將可大大減少資料外洩的問題，且網路攻擊愈來愈頻繁，針對軍事設備及關鍵基礎設施的國家安全逐步面臨日益嚴重的威脅，為了抵制這種威脅，運用區塊鏈技術可以防禦駭客與恐怖分子攻擊網路，並可利用區塊鏈去中心化的特性，打造成網路安全的防禦盾，可安全即時發送和接收訊息，亦能降低被駭客攻擊的可能性。

雖然目前系統實體設備與無線網路頻寬的限制，無法將區塊鏈導入指管系統，但相信未來如果突破此無線網路頻寬的限制，並將區塊鏈納入指管系統網路架構後，依前段所述的各項區塊鏈特性，必能提高系統整體安全性，及降低資料被竄改的機率，以達成指管系統資訊即時與正確、安全的最大效能。

伍、結語

「資訊戰」是廿一世紀戰爭發展的新趨勢，也是戰爭的另一種型態，為滿足未來資訊攻擊、資訊防護與資訊運用之需求，發展資訊武器，建立符合「資訊戰」之指管/電子戰系統是我國當務之急，在未來可能面臨的戰爭中獲得勝利，必須在資訊武器上超敵勝敵。從以往認知的「資訊戰」來分析，「資訊戰」具有十分顯著的效果，且網路已經成為提升軍隊作戰能力的利器，如同「制海權」、「制空權」一樣，爭奪「制網權」已逐漸演變成為各國維持軍事優勢的重要部分；再者美軍已開發資訊戰武器－「蘇特」，並應用於戰場上，均有顯著的效果，但如果敵方掌握「蘇特」技術，並入侵我軍指管等系統，我方便有可能喪失制網權等優勢，所以近年興起的安全性技術－「區塊鏈」，無論是它的去中心化或是不可竄改性等特性，皆獲得金融界及醫療界重視，並逐步納此技術至相關系統中，因此，如果我方各系統若能導入區塊鏈技術進入架構中，則可大大提升系統網路安全。

當前，金融、交通、軍事等面向隨著網路逐漸深入社會的各個領域，國家的整個民用和軍用基礎設施也越來越依賴網路，一旦出現漏洞，許多重要系統都將陷入癱瘓的狀態，國家安全也岌岌可危。因此我們須加強對「資訊戰」或網路偵查與攻擊的危害性認識，重視資訊戰法的研究，並重視其對衛星系統等網路設備的綜合性保護，如此，才能在未來不見硝煙的「資訊戰」戰場中，將損失降到最低，並取得戰爭的勝利。 ⚓

作者簡介：

謝圓富上尉，國防大學管理學院資訊管理系102年班，曾任海軍教準部程設官、資參官、左支部程設官，現服務於國防大學。