論網路攻擊於國際法上之定位 - 以國家責任與塔林手冊為討論核心

楊尚博

摘要

近代戰爭中，攻擊的手法不再以傳統的物理使用武力為限，使用網路進行攻擊逐漸成為現代戰爭中的常見手法，而在近期的烏俄戰爭中即被廣泛運用。然而基於網路的特性，使網路攻擊在國際法上的定位相當模糊。對於此一爭議問題，本文擬將探討範圍限縮於被攻擊客體為具有國家或是政治實體性質者，此一限縮較能將討論重點聚焦在國家行為以及國家責任等相關國際法之議題，也較符合現今戰爭中國家間互相以網路攻擊之趨勢。而本文主要的探討順序擬先從武裝衝突法的角度出發，首先討論「網路攻擊是否屬於國際法上之武力使用」。對於此問題則主要取決於國際法上之「武力使用」應該如何解釋及定性。除此之外，也因目前規範上的缺乏造成網路攻擊在國際法上難以被追究責任。因此就定性完是否屬於「武力使用」之後，本文會接續探討前開網路攻擊行為，是否屬於國家之行為，以及是否有相關國家責任的成立，包含國家是否對於其境內 IP 有管理監督義務，而若有此義務，是否可以以作為以及不作為之形式達成，而有國家責任之產生。最後，本文將對上述討論的結果整理出目前規範的缺漏之處，並提出出未來可以採行之規範方向，同時提出現今未發生但未來可能會發生的爭議問題，例如：在使用 VPN 下的犯罪地認定以及網路攻擊的損害應如何認定等爭議問題進行分析，以作為日後相關議題的探討基礎。

目錄

壹、 研究動機

一、 研究動機及問題意識

近年來，隨著科技之進步，國家間之攻擊手段不再限於傳統物理上之攻擊，而是逐漸使用科技之手段，而網路攻擊則在近年成為顯學，而衍伸出之「資訊戰」以及「網路戰」之概念也是近年國際法上炙手可熱的議題，像是過去之 Stuxnet 事件或是近期之烏俄戰爭，都有網路攻擊的行為出現。然而在目前法制之建構上，仍未有完整之概念共識以及具有拘束力之規範提出，因此本文希望能藉由此研究對於此議題有更深入之探討。

而於深入研究前，本文欲先釐清研究範圍為何，就前段落所提及之案件中，可以發現共同之內涵為均發生於網路空間，本文將其簡稱為「網路行動」。而其範圍應如何解釋有探析之必要。而以行為性質區分網路行動，若其行為為中性行為而無侵害性，在國際法上並不會涉及太多法律問題，然若其行為帶有侵害性，在國際法上即有可能構成「網路攻擊」，而該行為在國際法上所適用之規範為何，則有探討之必要。

因爲從傳統武裝衝突法切入，現今網路攻擊之概念似無法完全被囊括其中，因此在現行法制下應如何定位即需要討論。而就網路行動及網路攻擊進行分析後，本文將從另一角度進行探討，從網路攻擊之程度出發分類，在傳統武裝衝突法中，若武裝衝突達到一定程度即有成為戰爭之可能，傳統之空間探討多集中在陸海空域，因此將發生之空間切換為網路，即為「網路戰」之概念，然而此概念在現今法制下是否有規範可以適用，涉及管轄權之相關爭議，有探討之餘地。最後本文將網路戰進行分類，其中近年最被廣泛討論的種類即為「資訊戰」，其中對於資訊之散播是否屬於作戰手法有定性之必要，因此本文擬先將這四概念定性以完備整體之討論架構後，並取其中之核心「網路攻擊」為重點向下探討。

就探討之順序，本文擬分為三個層次進行探討。首先，本文欲嘗試定義前段落所提及之「網路行動」、「網路攻擊」、「網路戰」以及「資訊戰」等 4 個概念之各自定義以及之間之關係。接著，本文亦會提出國際上曾發生之案例進行類型化之分析，以建立後續議題討論之背景，並將案例中之行為以前段落所提到之概念進行定性。

而進入法律層次之討論，本文同樣分為三個層次探討，第一層次，本文將著重討論「網路攻擊是否為武力使用」之議題探討，於此層次，本文將先討論目前對於武力使用以及武力攻擊之定位為何，接著討論網路攻擊是否可以被上述概念囊括，最後整理出網路攻擊在國際法上可以適用之相關法源為何。第二層次，本文將從塔林手冊之觀點出發探討相關議題，本文首先會簡介塔林手冊之規範，接著就國際責任以及其他網路攻擊可能在現行國際法上所遇到之爭議進行分析，其他爭議包含「國家主權及相關義務之範圍」、「VPN 之相關爭議」

以及「自衛權」之主張。而於分析完前述爭議後，本文將以本文所抱持之觀點，重新觀察本文於最前面所提到之兩個案例，最後對於現行狀態以及法制狀況進行建議。

二、 相關規範適用順序

因對於網路攻擊，國際法上尚未有專門之公約以及條約進行處理，而多以不具正式國際法效力之手冊以及文件來對於網路攻擊進行專門規範。因此從宏觀之角度觀之，對於網路攻擊之規範，專門之規範像是《塔林手冊》或是《哈佛手冊》均為非政府機構所制定之規範，無強制拘束力，而若從法律之角度出發，則在網路攻擊符合武裝衝突之定義下才有適用武裝衝突法體系下之相關規範之可能，就規範之交叉適用順序，本文認為有先釐清之必要。

按《國際法院規約》第 38 條第 1 項[1]之規定，可大致分為兩部分，分別為主要法院以及輔助法源，而適用上主要法源是優先於輔助法源[2]。前者包含條約、國際習慣以及一般法律原則，而後者則包含判例以及學說。而將上述所提及之法源套入此架構中，可以發現《塔林手冊》以及《哈佛手冊》僅屬於輔助法源之各國權威最高之公法學家學說而武裝衝突法體系是屬於條約或是一般法律原則，因此在適用上武裝衝突法之體系優先於手冊。再進一步言之，論理之過程應先將網路攻擊進行定義，若其符合武裝衝突法中之定義，即可以適用武裝衝突法體系下之規範，而在武裝衝突法未進行詳細規範之部分，再藉由相關手冊來進行補充論述。反之，若僅有手冊有進行規定而現行武裝衝突法下無相關規定之情形，本文按規約第 38 條之規定，適用上可能要以反推之方式為之，即將學說中對於相關概念或規定之論述套回武裝衝突法之體系，判斷其概念是否可被囊括在武裝衝突法之概念中，如此一來，可以以解釋之方式合理擴大武裝衝突法之適用範圍，以彌補立法不及實務發展速度之情形。

貳、 網路行動、網路攻擊、網路戰以及資訊戰之定位

一、 網路行動、網路攻擊、網路戰以及資訊戰之定性

「網路行動」（Cyber Operations）、「網路攻擊」（Cyberattack）、「網路戰」(Cyber warfare)、「資訊戰」（Info Wars）在法律上之定性目前並未有統一之看法即定義，而本文認為在進入法律層次之探討前，應先明確定義四者之概念為何，之後再進入法律之探討過程中才可避免因定義之不明確造成討論重點失焦，因此於此段落，本文欲先嘗試定義何謂「網路行動」、「網路攻擊」、「網路戰」以及「資訊戰」，接著釐清四者之間之關係，以為後續之討論建立基礎。

首先，所謂「網路行動」，依據 2020 所出版的《奧斯陸特定武裝衝突法議

[1] 國際法院規約第 38 條第 1 項：「法院對於陳訴各項爭端，應依國際法裁判時應適用：（一）不論普通或特別國際協約，確立訴訟當事國明白承認之條規者。（二）國際習慣，作為通例之證明而經接受為法律者。（三）一般法律原則為文明各國所承認者。（四）在第五十九條規定之下，司法判例及各國權威最高之公法學家學說，作為確定法律原則之補助資料者。」

[2] 丘宏達、陳純一，現代國際法，四版，三民書局，2021 年，頁 58。

題手冊》（Oslo Manual on Select Topics of the Law of Armed Conflict）（以下簡稱奧斯陸手冊）中的第 20 條第 a 款，將網路行動定義為「在網絡空間或通過網絡空間實現目標的行動[3]」，而學者 Gary Solis 則將網路行動定義為「針對特定電腦、電腦系統或是用戶的秘密行動，而採用不具攻擊性的小規模入侵，而其個別破壞將具有重大價值[4]」。綜觀上述兩種觀點，前者主要對於所為行為之空間進行描述，而後者則著重於行為所針對之客體以及行為樣態進行描述。本文認為「網路行動」屬於一個較為廣泛之概念，其定義應為「包含所有於網路空間所進行之行為」，其重點應著重於空間之描述，即行為進行之場域為何，而非著重於詳細之行為態樣，因此本文認為在網路空間中所為之任何行為應該解可以認為是網路行動，至於其行為所針對之客體以及態樣為何則為下位層次之問題。

接著，對於「網路攻擊」，在《關於網路行動的國際法塔林手冊第二版》(Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations)（以下簡稱塔林手冊 2.0）中，第 92 條認為網路攻擊為「一種網絡行動，不論性質是進攻性的還是防禦性的，合理預期會造成人員傷亡或物體的損害或破壞[5]。」而在《適用於空戰以及導彈戰之國際法手冊》（Manual on International Law Applicable to Air and Missile Warfare）（以下簡稱哈佛手冊）[6]之第 1 條第(m)款則把「電腦網路攻擊」(Computer Network Attack)定義為「操控、破壞、拒絕、降低或是破壞電腦以及電腦網路或是點網路中之資訊或是增加對於電腦或電腦網路之控制[7]」。而除上述定義外，國際紅十字會以及許多學者皆有對此提出其定義，囿於篇幅，本文將其於註解列出[8]。綜觀目前大多數之定義，本文認為可以整理出「網路攻擊」應主要包含以下要件：「對於他方之電腦以及其所衍生之網路所為」、「不論行為之態樣，只要該行為會造成電腦或是網路功能之破壞或是減損」、「前述之減損不應只限於物理上之減損，也應包含功能之破壞」。主要之重點在於損害態樣之認定，因在傳統之武裝衝突法上，損害大多只限於物理上之損害，然而在網路空間中，許多損害皆非物理上損害，而像是系統癱瘓或是網

---

[3] 本句原文為:“cyber operations” are operations that employ capabilities aimed at achieving objectives in or through cyberspace.”，可參：

[4] 本句原文為：”Cyber operations may be described as covert actions employing small-scale intrusions against a specific computer, computer system, or user, whose individual compromise would have significant value”。可參：Gary D. Solis, The Law of Armed Conflict: International Humanitarian Law in War [537] (2022).

[5] 本條英文原文為：” A cyber-attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects.” ，期條文排列順序有所更動，在第 1 版本中，原本對於網路攻擊之解釋置於第 30 條，兩個版本中的條文並無差異。

[6] 因本手冊為哈佛大學之 Program on Humanitarian Policy and Conflict Research 所提出，因此簡稱為哈佛手冊。

[7] 本段原文為：” Computer network attack” means operations to manipulate, disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computer network itself, or to gain control over the computer or computer network.”

[8] 紅十字會將網路攻擊定位為目的為干擾、拒絕瀏覽、損害或是破壞電腦以及電腦網路中訊息或是電腦以及網路本身的行動。學者 Oona A Hathaway 將網路攻擊定義為破壞電腦網路功能的行為，主觀上需要有破壞之意圖。

路斷線等情形，因此為貼合此情形，本文認為應將損害之態樣擴大，而詳細之論述，本文將於後文論述之。

而「網路戰」(Cyber warfare)，學者 Steven Hildreth[9]將其定義為「在網絡空間發動的戰爭」，其內涵為保護資訊以及電腦網絡，阻止資訊攻擊，以及拒絕對手使用相同能力[10]。換言之，其概念同樣著重於空間之描述，即只要發生於網路空間中之戰爭即為網路戰。然而區分其與「網路行動」間之關係，本文認為兩者之間為上位及下位之關係，網路行動為上位，而網路戰只是網路行動的一種態樣，換言之，網路行動需要達到戰爭之程度，才可以被定義無網路戰，而至於其標準為何，本文認為涉及武力使用之標準為何，僅有達到武力使用之程度才有可能成為網路戰，對於此議題，本文將於後討論之。

最後，「資訊戰」(Info wars)則是近年來相當熱門之議題，像是「認知作戰」或是「散播假消息」都是資訊戰中常見的手法。就其定義學者 Steven Hildreth[11]定義為「通過影響對手資訊的程序、系統以及基於電腦的網絡，同時保護自己的資訊、基於資訊的程序、資訊系統和基於電腦的網絡，來實現資訊優勢的行動[12]」，而學者 Waseem Ahmad Qureshi[13]則於整理美國空軍以及參謀總長所提出之定義後給出自己的見解，其認為資訊戰為「利用資訊來實現對敵方的戰略或競爭優勢的技術。而要獲得這種競爭優勢，還需要確保充分的安全，使其不受對手的資訊行動的影響」。綜上所述，本文認為資訊戰屬於以利用資訊為主要手法而進行之戰爭或是衝突，其最常見手法為散播假資訊進而引發目標客體之對立以及恐慌。而就其定性，其屬於網路戰下之分支，即資訊戰只是網路戰之一種態樣。

二、 網路行動、網路攻擊、網路戰以及資訊戰間之關係

綜合上述定義，本文整理出一脈絡分析四個概念間之關係，首先就網路行動與網路攻擊間之關係，本文認為兩者為上下位之關係，即網路攻擊只是網路行動之一種態樣，一網路行動要達到武力攻擊之標準才有可能被稱網路攻擊。而網路行動以及網路戰之間之關係，兩者同樣為上下之關係，網路行動為一較廣義範疇，而網路戰為一下位概念，需網路行動達到可被稱為戰爭之程度才為網路戰。而就網路攻擊及網路戰間之關係，同樣是上位及下位之關係，網路攻擊要達到一定之程度才有可能被稱為是網路戰。而就網路攻擊以及資訊戰間之關係，網路攻擊有許多手法，只有在網路攻擊使用之手法涉及資訊相關時，其

[9] Steven Hildreth, Cyberwarfare, CRS Report for Congress[16](2001)

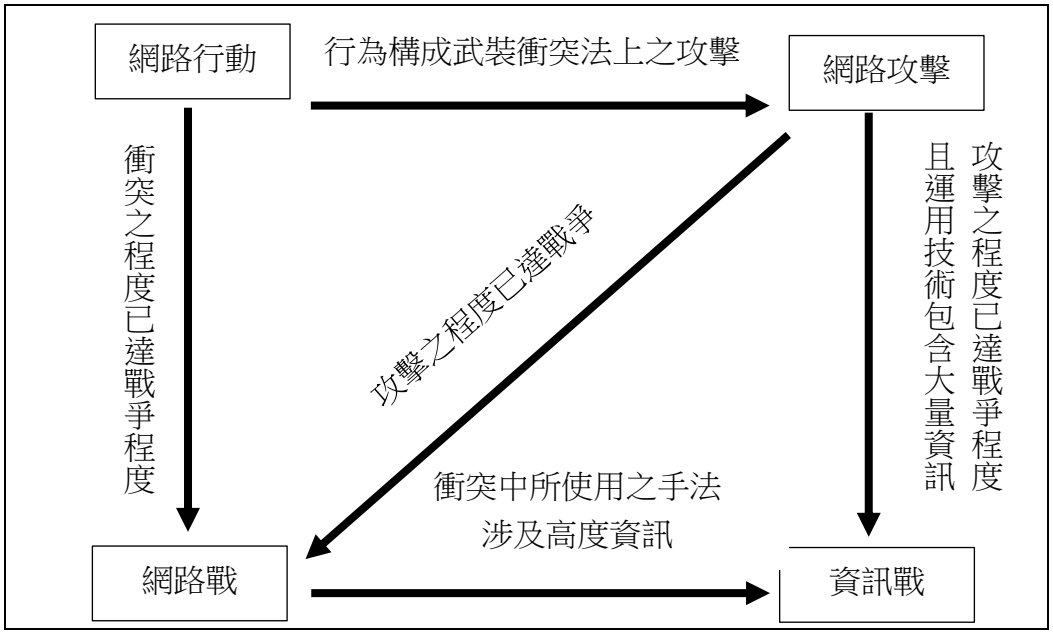
[10]本段原文為： defending information and computer networks, deterring information attacks, as well as denying an adversary’s ability to do the same.

[11] Steven Hildreth, Cyberwarfare, CRS Report for Congress[16-17](2001)

[12] 本段原文為：involves actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while defending one’s own information, information-based processes, information systems, and computer-based networks.”

[13] Dr. Waseem Ahmad Qureshi, Information Warfare, International Law, and the Changing Battlefield, 43 Fordham Int'l L.J. 901 (2020).

之間之衝突才有可能被稱為是資訊戰。最後就網路戰以及資訊戰間之關係，同樣是上位及下位之概念，資訊站只是網路戰中的一種態樣，最後本文以下圖畫出四者之間之交錯關係。



（圖一）網路行動、網路攻擊、網路戰以及資訊戰間之關係（本文自繪）

三、 相關案例之研析

（一） 2022 年烏俄戰爭之網路攻擊

1. 案例事實

就烏克蘭以及俄羅斯間之網路攻擊，最早可以追溯回 2005 年，而近期之攻擊則自 2013 年斷斷續續發展至今，像是俄羅斯方於 2015 年 12 月的 Black Energy 或是 2017 年 6 月的 Petya Virus，以及烏克蘭方於 2016 年 5 月發動之 "Prikormka 以及同年 6 月之 Channel One 都是自 2014 年烏俄衝突爆發後雙方網路攻擊間之著名事件。囿於篇幅，本文此處之討論將聚焦於自 2022 年 1 月 14 日後所發生之事件。

烏克蘭方主張自 1 月 13 日起，大量烏克蘭政府網站被換上用俄語以及波蘭語寫出「害怕吧，並等待最壞的結果」等文字，並且同時聲稱有大量個人資訊被洩露，其中受影響之政府機關包含俄羅斯之外交部以及國家安全與國防事務委員會(National Security and Defense Council of Ukraine)等 70 多個網站均受到攻擊，烏克蘭方認為此次之攻擊乃來自於俄羅斯官方，然而亦有觀點認為可能並非俄羅斯官方指使而是由俄羅斯之愛國駭客所為[14]。

2. 涉及法律議題簡析

[14] Ukraine cyber-attack: Russia to blame for hack, says Kyiv，網址：https://www.bbc.com/news/world-europe-59992531，最後瀏覽日期 2023 年 9 月 8 日。

在本案中，值得討論之國際法爭議有三，首先，就行為之分析，攻擊烏克蘭政府機關之網站之主體，為俄羅斯官方或是俄羅斯國中之民間愛國駭客在國際法上之咎責是否有所差異。接著對於受攻擊之烏克蘭政府網站，若其所受損害為網站上顯示非預期顯示之文字，是否構成武裝衝突法中之損害，涉及武裝衝突法中對於損害之認定。

（二） 2022 年 8 月境外攻擊我國政府網頁

1. 案例事實

於 2022 年 8 月美國眾議院之議長裴洛西（Nancy Pelosi）訪台，此行為可能引發中國政府之不滿，因此在其訪台之前後，IP 架設於我國之網站，不論是公務機關、學校甚至是民間機構之網站均遭受來自大量境外 IP 之攻擊，受害之機關包含國防部、外交部、台灣大學以及臺灣基督教長老會之網站[15]。其中此次事件中所使用之手法包含常見之 DDoS、假消息之散播、網站內容之置換。其中 DDoS 為在現今網路攻擊中最常見之手法，其方法為在短時間類利用大量之惡意嘗試，使目標伺服器以及周圍之設施無法承擔過大之流量，進而造成阻斷該伺服器之正常服務。而就內容之置換，像是臺灣大學教務處之網頁即被放上「世界上只有一個中國」的訊息。而就此一連串之行動，駭客組織 APT 27 主動聲稱承認乃其所為。

2. 涉及法律議題簡析

在本案中，值得討論之國際法爭議有三，首先，若案例中之攻擊真為 APT 27 所發動，即會涉及非國家主體(Non-State Actor)在國際法上之咎責地位為何以及國家是否有監管義務之責任，就此議題，目前仍未有深入之探討。接著，在案例中，涉及假消息之釋放，其是否屬於武力攻擊之一部份，不無疑問。而上述議題，本文亦將皆將於後文討論之。

四、 小結

於此段落，本文首先釐清網路行動、網路攻擊、網路戰以及資訊戰四者間之關係為何，而本文認為，其中之關鍵為「網路攻擊」在國際法上應如何定性，因其之定義會決定個別事件是否構成「網路戰」以及「資訊戰」，因此本文將於下文主要以「網路攻擊」為討論主軸。除定義外，本文亦從兩個過去案例中，提出其中有待釐清或是值得研究之法律議題，皆將於下文討論，相關爭點包含：「不同主體在國際法上之咎責差異」、「自衛權之行使」、「國家是否有監管義務」以及「VPN 管轄權之處理」等問題，皆將於後面段落討論之。因此從上述關係之釐清中，本文認為應以網路攻擊為研究核心，進行探討，而以下將先探討網路攻擊在國際法上之定為為何。。

參、 網路攻擊在國際法上之定位

[15] 臺灣 8 月初因裴洛西訪臺而遭到網路攻擊的事件總覽，網址：https://www.ithome.com.tw/news/152491，最後瀏覽時間：2023 年 9 月 8 日。

一、 國際法上武力使用、武力攻擊以及網路攻擊的定位

目前國際法上對於武力使用以及武力攻擊之定義，並未有一統一之見解，因此可以從許多角度切入觀察。而以下本文將先就兩個概念之內涵進行定義以及劃分，接著對於二者之要件進行剖析，最後討論網路攻擊是否會該當上述二者，並同時從塔林手冊之規範分析網路攻擊之定位為何。

（一） 武力使用以及武力攻擊之定位

首先是「武力使用」，主要涉及之條文為聯合國憲章第 2 條第 4 項，該條指出個聯合國會員國在國際關係上不可以使用武力(Use of Force)。然而 Force 一詞所涵蓋之範圍深廣有所爭論，而學者認為若從《友好關係及合作之國際法原則宣言》切入觀察，可以認為此處之 Force 應該只包含軍事力，而不包含其他之性質，例如經濟或是政治性之壓力[16]，亦有學者[17]觀察聯合國歷來之實踐，認為武力使用應該只限於武裝力量(Armed Force)。

而「武力攻擊」，其主要涉及條文為《聯合國憲章》第 51 條，該條認為只有在受到武力攻擊之狀況下，才可以行使自衛權。其在條文中之用詞為”Armed Attack”，然而在該條文中未對「武力攻擊」之內涵進行描述，而有學者從國際習慣法觀察此條文，認為一國家只要對另一國家具有一定程度與範圍之攻擊使構成武力攻擊[18]。而學說上有學者對於「武力攻擊」之概念進行詳細之探討，其將要件[19]歸納為「國家或非國家使用武力」、「跨越政治邊界或是來自國外」、「攻擊已經發生或是接近」以及「具有嚴重性質或是國家對非國家團體進行控制或是介入」。實務上國際法院在 1986 年尼加拉瓜案中認為只有最嚴重的武力使用構成武力攻擊，乃採取「規模及效果說[20]」(Scale and Effects)。從此三個觀點觀察，似乎可以發現在對於武力攻擊之解釋中，均有提及對於程度之要求，只是描述有所不同。

從上述之實務條文以及學者見解中，本文觀察出目前國際法實務上對於武力使用以及武力攻擊之內涵雖尚未有統一且明確之標準，但似乎可以看出大致之規範輪廓。本文進而整理出「武力使用」以及「武力攻擊」之差異以及兩者之要件。

---

16 魏靜芬，網路攻擊、網路間諜及網路監控之國際法評價，軍法專刊，第 65 卷第 1 期，2019 年 2 月，頁 20。

17 姜皇池，國際公法導論，四版，新學林，2021 年，頁 783。丘宏達、陳純一，現代國際法，三版，三民書局，2012 年，頁 1106。

18 姜皇池，國際公法導論，四版，新學林，2021 年，頁 793。

19 余民才，武力攻擊的法律定性，法學評論（雙月刊）第 123 期，2013 年，頁 28。

20 CASE CONCERNING MILITARY AND PARAMILITARY ACTIVITIES IN AND AGAINST NICARAGUA (NICARAGUA v. UNITED STATES OF AMERICA) para. 187-201.

首先是兩者之差異，對於「武力使用」，目前大多是對採取對於行為之描述，認為只要一行為屬於軍事力之使用即為武力使用。而對於「武力攻擊」，從上述學者以及實務之解讀方式，大多有在定義中加入對於程度之要求，像是武力使用需達到「相當嚴重性」或是從武力的規模或是效果來觀察。總結來說，武力使用以及武力攻擊間最大之差異在於武力使用需要達到一定程度才會構成武力攻擊，換言之，本文認為武力行使及武力攻擊間為上下位關係，武力行使為上位概念，武力攻擊只是其下之子概念，兩者僅有程度上之差異[21]。

因此在要件上之探討，武力攻擊之構成要件等於是在武力使用之要件外再加上對於程度之檢驗，換言之，兩者之要件大致相同。而就武力使用之要件，本文認為有「武力之使用」外，亦須有隱藏性要件即「需有損害之發生」[22]。

首先就「武力使用」之要件進行分析，在此「武力」(Force)一詞之解釋，在傳統之武裝衝突法解釋下，多數見解認為僅限於「軍事力」(Armed Force)而不及於經濟力[23]。而目前多數學者亦採取此看法[24]，因既是在武裝衝突法之架構下，其規範範圍本應就限於武裝軍事行動相關，然而「軍事力」之內涵要如何解釋以及範疇為何，即有困難產生。按傳統以及各國之實踐，似乎只限於傳統之君武器才屬於軍事力之範疇，然而本文認為隨著科技發展演變，現代之作戰手法越來越多樣，若只限於傳統意義上之軍武器，新型態之作戰手法將成為規範上之漏洞，因此本文認為，對於軍事力之範圍劃分，應認為只要其使用之方式為作戰手法以及手段（Method and Mean of Warfare）之範疇且會造成損害者，即屬於軍事力之範籌。而所謂作戰手法以及手段，參目前國際紅十字會之定義

---

21 採取相同見解之國內學者為田力品教授，參：田力品，武裝衝突法對使用武力之限制，頁115，軍法專刊，第59卷第1期，2013年2月。

22 本文認為有此要件之存在原因在於因若從文義出發，似乎只要有行為即可。然而本文認為除有武力行使之外，仍需要有一定之損害結果發生才可構成武力使用，原因在於若只需行為即可構成，其打擊範圍有過廣之虞。雖然在目前聯合國憲章明定不得使用武力之原則下，為追求和平似乎應採取廣義之解釋較為妥適，即不須損害要件之存在。然而本文認為在武力使用禁止為原則之架構下，可見目前對於武力使用是採取嚴格之態度，因此應採取較為狹義之解釋，即需要有行為及結果才可以被稱為是武力使用較符合現行法之趨勢，否則可能要成合法之武力使用以及武力攻擊被過度限縮。而可以援引之法源為國家責任公約之規範概念，在該公約中，原則採取需有行為且有造成損害並可以歸責始需要負責，將武力使用之概念套入，若武力使用為不法行為則當然有原因上述公約中規定之可能，因此，可以看出損害亦為之必要要件，然而單從武力使用之字面上，難以得出此要件，因此為不逾越文義之解釋，故本文採取隱藏性要件之方式處理之。

23 對此基於篇幅問題，本文不將原因逐一列出，可以參閱：孟凡明、李國振，武裝衝突法與中國的實踐研究，中國政法大學出版社，2014年，頁18-19。

24 目前對於武力之使用，目前多數學者仍採取狹義之解釋方式，學者季華認為應只限於武裝或是軍事力量，學者丁麗柏及朱靜則是認為從聯合國憲章第2條第4款解釋之角度出發應只限於傳統武裝行為，參：季華，《塔林手冊》中有關於網路戰爭的武力使用問題－從國際法角度展開，江漢學術，第35卷第3期，2016年，頁31。丁麗柏、朱靜，《塔林手冊》對網路攻擊中“武力”的界定及反思，河北法學，第36卷第12期，2018年1，頁85。

[25]，其所指乃用於攻擊目的之武器以及其使用方式，而此類武器禁止之主要目的為禁止多餘之傷害以及不必要之痛苦[26]。在目前之架構下，只要是達成上述目的之作戰手法即會被禁止，而為避免新型態作戰手法無法被囊括，其援引第一議定書之第 36 條[27]締約國有評估新武器、戰爭手段或方法的合法性之義務。因此在此解釋之下，若將軍事力之範圍囊括作戰手法，亦可以將所謂武力之範圍做出清楚之劃分，亦可以藉由國家之評估義務事實納入新型態之武器。

接著對於損害結果之認定，在傳統武裝衝突法中，皆主要著重於有物理上損害之情形，然而在新型態之作戰手法中，許多結果皆難歸類於物理損害，例如：虛擬空間中之設備破壞、心理上損害、經濟上無形之損失等結果皆難屬於物理上之損害。對此，本文認為面對此新型態之作戰手法所造成之損害，應將傳統對於損害之解釋進行擴張，即除了實際物理上之毀損外，功能上之毀損亦應包含在其中，對此學者 Cordula Droege[28]採取類似之解釋，其解釋主要針對網路戰，其認為在網路戰中之攻擊，除物理損害外，亦應包含功能上之損壞，例如：國家基礎建設之網路失靈。對此，可能有質疑認為本文所採取之見解過度擴張，然而本文實為參考《國家對國際不法行為的責任條款草案》（以下稱國家責任公約）第 31 條之精神進行擴張，在該條中，損害包含一國不法行為所造成之任何損害，而損害包含物質損害(material damage)以及精神損害(moral damage)，就此本文認為國家責任公約既已將損害之範圍擴及至物質上以及精神上，而功能上之損害或減損，從內涵分析，其可以屬於物質上之一部分，雖外觀上無損壞，但已造成其功能之減損，亦應屬於損害之範圍。

（二） 網路攻擊之定位

而就武力使用以及武力攻擊之概念進行釐清後，網路攻擊是否屬於武力使用抑或是武力攻擊目前在國際法上仍為一爭議問題，仍未有統一之見解，採否定見解者認為網路戰爭目前仍不構成違反武力使用之規範[29]。然而亦有採取肯定見解者，學者 Gary Solis[30]即認為網路攻擊屬於武力使用之一環，其從國際法院就核子武器諮詢意見第 39 段出發，認為武力使用應不限於特定種類之武器，因

---

[25] https://casebook.icrc.org/law/conduct-hostilities#footnote63_4nfz02z，最後瀏覽日期：2023 年 5 月 19 日。

[26] 第 35 條，該條指出在武裝衝突中，選擇作戰手法以及手段之權利不受限，但是禁止使用會引起過分傷害及不必要痛苦的性質的武器、投射物質以宜作戰方法以及目的在可能對自然環境引起廣泛、長期而嚴重損害的作戰方法或手段。

[27] 類似規範於塔林手冊中亦有規定，塔林手冊 2.0 版第 110 條有指出各國應保證其所使用之網路規範要符合武裝衝突法之規範。

[28] Cordula Droege, Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians,[Vol.94] International Review of the Red Cross, p560.(2012)

[29] 姜皇池，國際公法導論，四版，新學林，2021 年，頁 784。

[30] Gary G. Solis The Law of Armed Conflict[p539](2022).

此使用網路攻擊亦屬于武力使用之一環。而塔林手冊亦採取肯定之見解，在第69條本文及註釋中，其認為只要網路行動之規模相當於使用武力之非網路行動，即構成使用武力，並提出8個標準[31]以區別網路行動是否為使用武力之標準。而在手冊第92條[32]，有對網路攻擊之內涵進行更細緻之描述，其認為攻擊需要有「暴力」之因素含在其中，而此部分應從結果進行觀察，而就結果之部分，應不限於物理上之損害，且縱使未達成預期之損害，亦構成攻擊。

對此本文認為亦應採取肯定之見解而認網路攻擊有構成武力使用之可能，因在現今之作戰手法發展下，網路逐漸成為國家間攻擊之手段以及進行攻擊之空間。從國際法院之核子武器諮詢意見出發，使用武力之範圍適用於任何使用武力的行為，其內涵與本文上述之作戰手法範圍類似，因此若網路行動被以攻擊目的來運用，即成為網路攻擊，即等同上述肯定說見解之使用武力，因此應肯認網路行動在符合一定之狀況下，會是使用武力。然而在此解釋之下，僅能推出網路攻擊是屬於武力使用之一環，而就網路攻擊是否屬於武力攻擊，本文認為仍應採1986年尼加拉瓜案所採之規模及效果說。

綜言之，對於網路攻擊之定位，從本文對於武力使用之「武力」採取較為廣義之認定方式之下，可以認為網路攻擊至少屬於武力使用之範疇，然而是否屬於武力攻擊，按1986年國際法院之見解，僅當該攻擊達到一定程度時，才有可能被定性為武力攻擊，而兩者之區分實益除程度上之差異外，對於被攻擊之國家可以主張之行為亦有所差異，例如僅有受到武力攻擊程度者可以主張國際法上之自衛進行反擊，而在網路攻擊中是否可以主張，本文於後會深入討論之。

（三） 塔林手冊之劃分標準

從《塔林手冊》出發，其規範模式將網路攻擊分為三個層次，分別為「干涉」、「武力使用」以及「武力攻擊」。就干涉以及武力使用之區分，從條文[33]以及其註釋中可以看出，只要網路行動之規模以及效果可以與非網絡行動相提並論，而達到使用武力的程度時，就構成了使用武力，若未達使用程度則為干涉，區分之標準，其在註釋中有8個審查標準來判斷是否為武力使用。對此8個標準，有見解[34]指出其定性相當不確定，容易造成主觀恣意判斷，然而本文採

[31] 其列出之標準有：「嚴重性」(Severity)、「立即性」(Immediacy)、「直接性」(Directness). 「侵略性」(Invasiveness)、「效果可量化性」(Measurability of effects)「軍事性」(Military character)、「國家介入性」(State involvement 以及「推定合法性」(Presumptive legality)。

[32] MICHAEL N. SCHMITT, TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS[p415](2017)

[33] 在塔林手冊1.0版本為第10條，2.0版本為第69條。

[34] 朱路，論當代武裝衝突對國際法和戰爭法的挑戰，人民日報出版社，2022年，頁150。

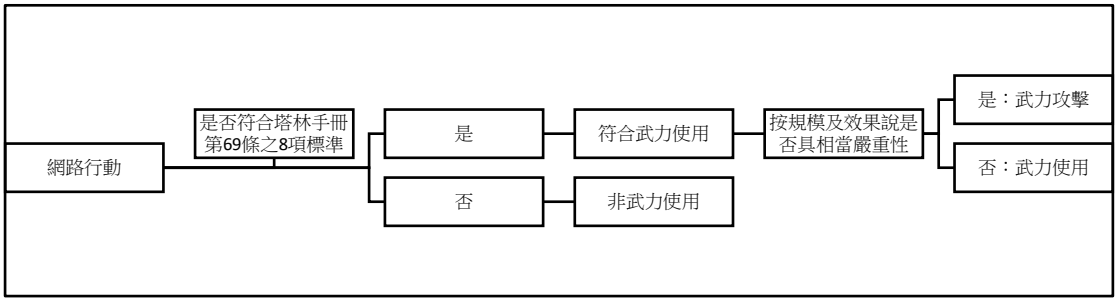
取不同看法，因在條文之註釋中已對於各個標準進行描述，已顯示規範建立者希望之方向，雖然缺乏實務案例之實踐，但至少已提供一明確方向。但對於網路攻擊[35]，其定義為一種網絡行動，無論是進攻或防禦性，其有理由預期會造成人員傷亡或物體的損害或破壞。對此處所述之損害，其在註釋中有指出損害之概念當然包含對個人造成的傷害和死亡，但基於武裝衝突法之人道目的，應將範圍擴大至相當於傷害之嚴重疾病和嚴重精神痛苦才是合理的。而對於虛擬空間之損害亦有描述，其認為若恢復功能需要更換物理上之零件，對功能的干擾即為損害。而若需要重新安裝系統或特定數據使目標網絡基礎設施重建其功能亦屬之。判斷重點在於只要喪失可用性即構成損害，其如何失效並不重要。因此對於損害之程度判斷，其似乎採取較為寬鬆之態度，然而並非毫無限制，其有特別指出，若是僅造成不便，並不屬於損害，但是若是被攔截而未造成實際損害之攻擊，其認為若無防禦措施，仍有可能造成必要的結果，因此其仍是攻擊。

從《塔林手冊》之立法模式可以看出，其應是採取國際法院之「規模及效果說」作為標準來進行規範，進而區分干涉、武力使用以及武力攻擊。區分干涉與武力使用之標準為是否符合其所列之 8 個標準，而區分武力使用以及武力攻擊之標準期未有明確指出，本文認為從文義觀察似乎為是否預期會造成人員傷亡或物體的損害或破壞，若會即為武力攻擊，若非則僅為武力行使，而其損害之範疇不僅限於物理上之損害，更包含功能以及可用性之減損。因此在個案中，欲區分該行為為武力行使或是武力攻擊，從塔林手冊之角度出發，需要以個案之規模及效果來判斷之而不可一概而論。

綜上所述，本文認為，在現今作戰手法隨科技快速演進下，就武力之使用以及損害之認定等相關定義以及法規範也要做出適當之解釋。對於武力使用之概念，本文認為在解釋上，對於所謂武力之解釋應擴張及有可能造成損害之作戰手法即可，而就程度上之判別，則交由損害之要件來判斷，應不只包含物理上之損害，功能上之減損亦應包含在其中，才能較完整規範到新型態之作戰手法。而就武力使用以及武力攻擊之區別，依目前現行之實踐，應個案判斷其行為所造成之損害進行分類。而就網路攻擊是否為武力使用或是武力攻擊，本文認為對於網路攻擊是否可以構成武力使用應採取肯定之見解，判斷標準可酌塔林手冊第 69 條所定出之標準，若無法符合前列標準，即非武力使用。而該行為是否構成武力攻擊，則採取「規模及效果說」之判斷標準，相關概念以下圖表

[35] 在塔林手冊 1.0 版本為第 30 條，2.0 版本為第 92 條。

示之。



（表一）網路行動、網路攻擊與武力使用及武力攻擊之關係（本文自繪）

二、 網路攻擊在國際法的相關適用

對於網路攻擊在國際法上之規範適用，本文擬分為兩部分進行探討，以下將分為和平時期以及武裝衝突時期進行探討。會如此區分之原因在於在國際法之適用上和平時期以及武裝衝突時期所適用之法律體系不同，僅有在武裝衝突狀態時，才有武裝衝突法體系下規範之適用。而就兩者之區分界線，目前大多認爲是以程度以及狀態來區分，換言之，原則上通常大多時間都是適用和平時期之法律，即武裝衝突法外之法律，而只有在雙方達到武裝衝突狀態時才會適用武裝衝突法之相關規範。[36]而就兩者區分之界限，學者[37]多以 1995 年前南斯拉夫國際刑事法院 Tadic 案之判決理由為判斷標準[38]，在該判決段落 70，法院區分國家間以及非國家間之武裝衝突，若是國家之間只要訴諸武力即是武裝衝突，然若是非國際性，即一國之政府與有組織之武裝團體之間或是這些團體之間相互需要存在持久之武裝衝突(protracted armed violence)，其提出之標準為「持續性」以及「同步性」。而國際紅十字會提出不同之見解[39]，其認為在國家間即非國家間的武裝衝突並無程度之要求，而對於武裝衝突狀態之開啟則採取「開第一槍理論」，只要有國家先開啟第一槍及進入武裝衝突狀態。目前前者為多數見解，後者則為少數見解。而本文認為兩者亦有可採之處，少數見解有擴張武裝衝突狀態之虞，但保護較為完善，多數見解則是待雙方進入一定武裝衝突狀態才始適用武裝衝突法，較不容易誤判情勢，但何謂訴諸武力仍有釐清之必要。

---

36 賈兵兵，國際公法：和平時期的解釋與適用，一版，清華大學出版社，2015 年，頁 440。Gary G. Solis The Law of Armed Conflict[p129] (2022).

37 賈兵兵，國際公法：和平時期的解釋與適用，一版，清華大學出版社，2015 年，頁 441。Gary G. Solis The Law of Armed Conflict[p132] (2022). Dr U C Jha. Dr K Ratnabali. The Law of Armed Conflict: An Introduction[p47] (2017)

38 Dr U C Jha. Dr K Ratnabali. The Law of Armed Conflict: An Introduction[p48] (2017)

39 Knut Dörmann, Liesbeth Lijnzaad, Marco Sassòli and Philip Spoerri, COMMENTARY ON THE FIRST GENEVA CONVENTION Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field [p109] (2016)

因此本文採取折衷之見解，對於武裝衝突狀態之開啟，應有單方先訴諸武力，而到達一定狀態後即成為武裝衝突，而一定狀態之判斷標準則由個案情形判斷之，然至少需超越前述構成武力攻擊之判斷。即雙方之駁火或交戰狀態按規模及效果說要逾越具相當嚴重性，即進入武裝衝突狀態。

而於細究兩個時期所適用之相關規範前，有一概念需先釐清，即本文前段所探討之武力使用以及武力攻擊，並非只會發生在武裝衝突時期，而是兩個時期皆有可能會發生，因就和平時期以及武裝衝突時期之區分，是以該時間點之狀態作為區分之標準，而武力使用以及武力攻擊大多是對於單一行為之定性，兩者之概念大不相同，因此較正確之理解方式為武力使用以及武力攻擊是在和平時期或是武裝衝突時期可以運用之作戰手法，換言之，網路攻擊是和平或是武裝衝突時期所使用之手段，於此先敘明。而承前段落之結論，網路攻擊是否構成武力使用或是武力攻擊乃是以個案之情況判斷之，個別行為所適用之法律應以當時所處狀態判斷之，因此以下將分別論述網路攻擊和平時期以及武裝衝突時期所適用之規範為何。

而就下述國際法之適用順序，如本文於研究方法部分所述，按國際法院規約第 38 條，法源可分為主要法院以及輔助法源，前者包含條約、國際習慣以及一般法律原則，而後者則包含判例以及各國權威最高之公法學家學說，而在適用上則以前者為優先。

（一） 和平時期

在和平時期，與武裝衝突時期最大之差異在於其並無武裝衝突法之適用。因此在進入武裝衝突狀態之前，並無援引武裝衝突法之可能。因此在若在和平時期進行網路攻擊，無論其性質是屬於武力使用或是武力攻擊，在進入武裝衝突狀態前，均不可適用武裝衝突法。因此在規範適用上，本文認為僅能以《國家對國際不法行為的責任條款》下之國家不法行為架構檢驗之。

對於不法以及不當行為之理解，不當行為為一上位概念，其下可分為國際不法行為以及國際罪行。而兩者之關係，只要不符合國際罪行，就會落入國際不法行為之範疇。而若國家為主體，因國際罪行在國際刑事法院規約之架構下只追究個人之責任，因此在網路攻擊之狀況中，只要國家進行網路攻擊不構成前述之 4 個罪行[40]，受害方只能以主張該行為為不法行為進而主張賠償。然而若主體為非國家主體，在國際法層次上只有符合國際罪行時才有追究之可能，而

[40] 按照國際刑事法院規約，構成國際罪刑者限於：「嚴重違背對於維持國際安全與和平且具有根本重要性之國際法義務」、「嚴重違背對於維護各國人民自決權利且具有根本重要性之國際義務」、「大規模嚴重違背對保 護人類具有根本重要性之國際義務」以及「嚴重違背對於維護任何保全人類環境具有根本重要性之國際義務」。

無國家責任公約之適用。而就責任成立之檢驗架構，本文將於下一章節與塔林手冊綜合論述及比較，於此不加贅述。

（二） 武裝衝突時期

而若雙方或是多方之之交戰狀態已進入武裝衝突階段，即有武裝衝突法－海牙公約體系以及日內瓦公約體系[41]之適用，而除前述法體系外，塔林手冊中亦有對武裝衝突時期做出特別之規範，以下分述之。

若網路攻擊在武裝衝突狀態被使用，即需遵守武裝衝突法中之規範，而武裝衝突之性質為國際性或是非國際性之區分在現今日漸模糊，因日內瓦公約之共同第 3 條以及習慣國際人道法的規定使非國際性之武裝衝突亦須要適用武裝衝突法中之規範。像是原則性之規範，包含：區分原則、必要性原則、比例原則以及人道原則。即代表在武裝衝突之狀態中，網路攻擊在攻擊時需要區分所攻擊之客體為何，目標只能限於軍事性之目標，且就其攻擊之手段需要符合必要性，而其造成之損之不應超過所期待之軍事利益，並且不可施加於合法軍事目標之必要行為以外之傷害以及破壞行為。

在武裝衝突狀態中，網路攻擊需要是武裝衝突法之規範範疇才有上述原則之適用餘地。然在現今之武裝衝突法下並無明確規範網路攻擊，因此是否能藉由解釋之方式使其適用即有討論之實益，除本文於上提到以第 36 條承認新作戰手法之方式外，塔林手冊中從解釋海牙第四公約之角度出發，因在其前言有指出在更完善之規範制定之前，各國可以有必要聲明在公約中沒有被囊括之情況仍應受國際法之規範，因此根據此原則之解釋，如果在武裝衝突期間行使網路攻擊，即可以適用武裝衝突法之規範，以避免規範上之漏洞。

而塔林手冊中有關於武裝衝突時期之規定位於第 16 章以下，其內容包含對於武裝衝突之一般性規範以及對於攻擊行動中之相關規定，詳細之內容，其實與現今之武裝衝突法大致相同，其中對於攻擊客體以及作戰手法有做出更為詳細之描述。只是規範之適用場域為網路。而其在第 80 條規定在武裝衝突中進行網路行動應該遵守武裝衝突法，在該條之註釋中即明確表示若塔林手冊中之規範並未規範到之個別詳細規定，應回歸武裝衝突法之適用。

因此綜上所述，在適用上，在和平時期，網路攻擊之規範適用在責任追究上只有在國家為主體時可以適用國家責任公約，而非國家主體時，只有個人可以依據國際刑事法院規約被咎責。而在武裝衝突時期，本文認為仍應以日內瓦以及海牙公約為主要適用之法規範，而在無網路攻擊之相關法明文下，只能藉由解

[41] 就兩者之整體規範觀之，日內瓦體系主要是規範給予戰爭受難者必要保護之體系公約，而海牙公約體系則是規範作戰手法以及手段。

釋將塔林手冊之規範套入適用。

肆、　對於塔林手冊之反思以及國家責任之探討

一、　塔林手冊之現今規範及相關爭議概述

塔林網路行動國際法手冊(Tallinn Manual on the International Law Applicable to Cyber Operations)(以下簡稱塔林手冊)是最早於 2013 年由許多國際法專家所完成國際法手冊，而目前最新之版本為 2017 年所發布第二版之塔林手冊。而就兩個版本之差異，在於第一版主要是討論武裝衝突時期之適用規範，而第二版則加入和平時期所適用之規範。而該手冊主要之主張為現行國際法已經完全可適用網路戰爭，無需再創造新的法律[42]，而對於該手冊在國際法上之性質，本文認為因不論是參與塔林手冊第一版或是第二版編纂者均為學者，且於兩版手冊之前言中[43]，亦表示其為以小組為單位來撰寫並不代表編者之母國政府立場，故依照國際法院規約第 38 條之規定，應定性為輔助法源中之「各國權威最高之公法學家學說」。按目前國際法實務對於國際法法源之適用，其順序屬於主要法源之條約、習慣法以及一般法律原則之後，與法院判例相同。

而塔林手冊之現今規範，其分為四大部分，分別為網路空間一般國際法[44](General international law and cyberspace)、特殊領域[45]之國際法以及網路空間(Specialized regimes of international law and cyberspace)、和平時期之網路活動[46](International peace and security and cyber activities)以及網路武裝衝突法[47](The law of cyber armed conflict)。其中本文所探討之重點－網路攻擊及武力使用相關爭議之相關規範集中於第三部分以及第四部分。就和平時期之網路行動，規定涉及使用武力、自衛以及集體安全，規範大多源自聯合國憲章中之相關規定。而第四部分之規定，則是將武裝衝突法－日內瓦以及海牙法體系之規範加入其中，例如：區分原則、作戰手法、受攻擊者及應保護者之規範、占領以及中立等相關規定。而各自條文之規範，囿於篇幅，本文即不逐一介紹，而只於下列出本

---

42 MICHAEL N. SCHMITT, TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS[p3](2017). 對於此觀點，雖然目前在國際法上仍有不同見解，但是多數見解均認為國際法規範可以直接適用於網路戰爭或是相關網路行動，相關文件包含：United Nations, “Reports of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security,” UN Doc. A/68/98, para. 19.(2013)

43 MICHAEL N. SCHMITT, TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS[p2](2017). MICHAEL N. SCHMITT, TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE S[p11](2013).

44 塔林手冊第 1 章至第 5 章。

45 其所謂之特別領域包含國際人權法、外交領事法、海洋法、航空法、外部空間法以及國際電信法，分別列於第 6 章至第 11 章。

46 塔林手冊第 12 章至第 15 章。

47 塔林手冊第 16 章至第 20 章。

文於閱讀塔林手冊之過程中發現規範上之漏洞。

首先是非國家主體之歸責問題，此爭議之發想源自於 2022 年 8 月境外攻擊我國政府網頁之案件，就該次行動之主體為駭客組織 APT 27 聲稱其所為，然而在國際法上是否可以被咎責有探討之餘地。接著是有關於 VPN 管轄權之爭議問題，塔林手冊在第一部分之第一章以及第三章有對於主權及管轄權之範圍做出規範，然而在現行虛擬私人網路(virtual private network)逐漸被廣泛之運用下，使許多網路攻擊行為可以藉由 VPN 而使非由本國 IP 發出攻擊，而是跳到他國 IP 來發動攻擊，對此在塔林手冊第 60 條在規範國家有監管義務之情形下，究竟何國家有管轄權不無疑問。最後則是有關於自衛權之爭議。而上述爭議，本文將於本節之後續段落分析之。

二、 國家責任之探討

就國家責任之探討，本文所探討之範圍不僅止於狹義之國家責任，而是廣義之國際責任[48]。而使用國家責任之用詞在於因目前國際法上對於責任之探討大多以國家為探討之主體，因此在探討上多以國家責任(State Responsibility)稱之，而本文以下除探討國家為主體之情形外，亦會探討非國家主體(Non-State Actor)之情形，於此先敘明。而就討論順序，本文擬先從現從法律之角度出發，分別討論國家以及非國家主體在和平時期以及武裝衝突時期之適用規範為何。而後再從塔林手冊之角度出發剖析此爭議。

（一） 現行法體系下之探討

就國際法上之主體，若以我國學者見解採取簡單之二分法分類，可分為完全主體以及不完全主體，而完全主體僅有國家，其他國際法上主體均為不完全主體。而就國際法之建制過程，也可以看出此分類之影子，因在傳統之國際法見解中，多認為是國際法是唯一主體。所以目前國際法之規範主體大多以國家為規範主體。因此在責任歸屬上，似乎難以對非國家之主體(Non-State Actor)咎責。

首先是國家，在和平時期，其可以依據國家責任草案進行責任之追究。首先就國家責任公約，本文認為其性質是嫁接之條款或是一討論之平台，操作流程為先定性為國家行為屬於該草案之規範範疇，而於確立其屬於規範範疇之後，再藉由該草案之依據，連結至有相對應行為或是義務之公約，再藉由該公

[48] 本文於此處之用詞為國際責任，而非傳統國際法中之國家責任，說明說下：在傳統見解認為國家為國際法上之唯一主體之見解中，因主體需要享受權利並負擔義務，因此理所當然認為國際法上只有國家可以被咎責。然而在近代國際法中，隨著規範的發展，實務以及學者認為只要是國際法上之主體即可以在國際法上之享受權利並負擔義務，也是國際責任的承受主體，因此越來越多學者對於國際法上之認定，改用國際責任之用詞稱呼之。

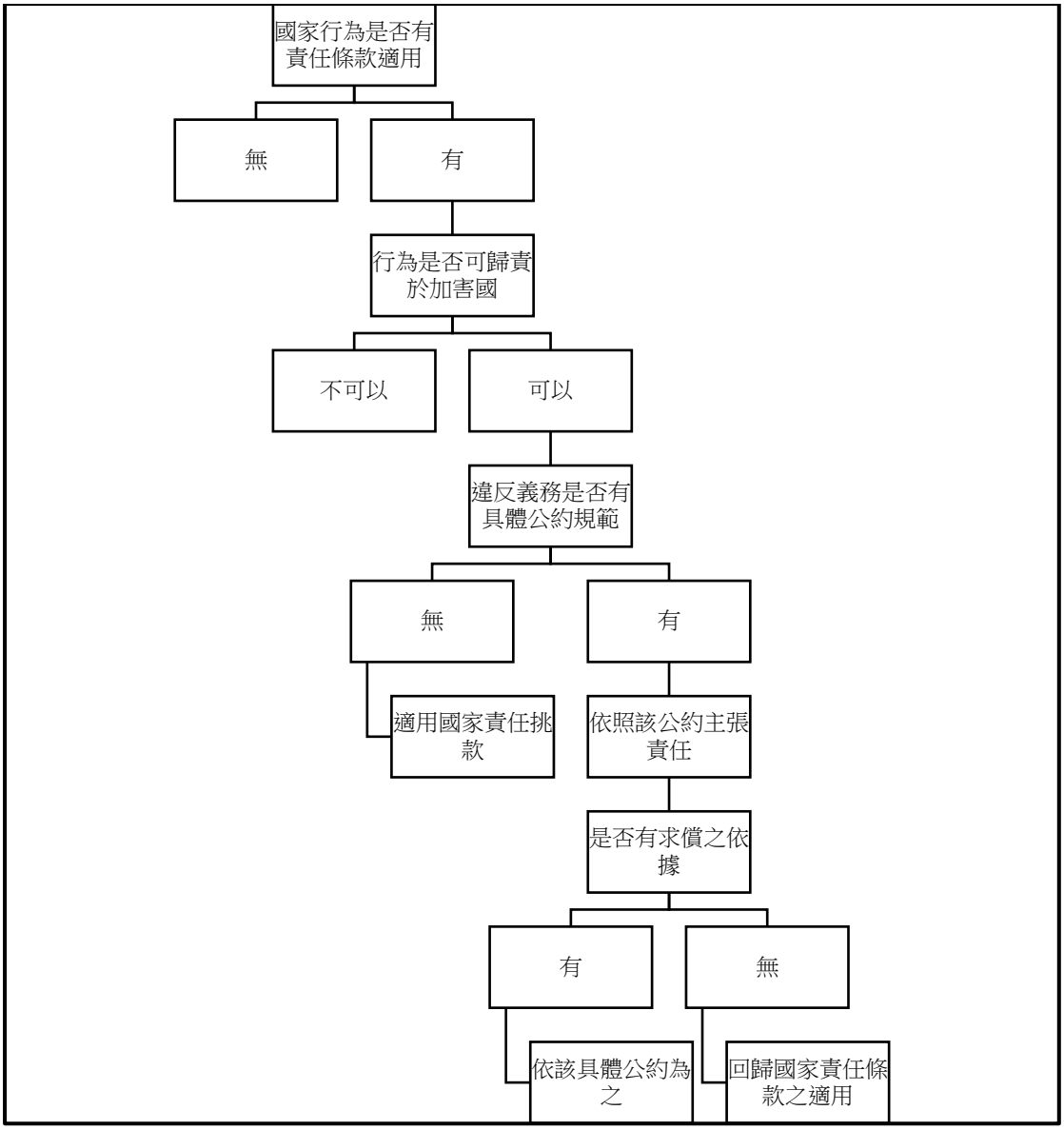
約對該行為進行相關之評價。因此適用前提為該行為需構成不法行為，而不法行為之成立要件，有二元、三元以及四元論[49]之討論，而本文認為上述三說均有可採之處，但各自亦有缺陷，二元說之觀點忽略損害要件，會有打擊過廣之嫌，三元說中之過失為何種程度之過失，有討論之餘地且易有爭論，因此加入主觀要件恐生更多爭議，而四元說較為可採，其有加入對於損害要件之之判斷，但其有本文認為應取消之主觀要件，因此本文採取綜合之看法，認為就國際責任之成立要件為「行為可歸責於國家」、「行為違背該國之國際法義務」以及「會產生損害之結果」。其中對於損害之認定，目前國際法上仍多指物理上之損害，但本文城前開之討論，認為就損害之認定做出一定放寬，除物理上之損害，亦應包含功能上之損害，以減少規範上之漏洞。

而就後續之法律效果，進行不當行為之國家有義務停止該不法行為，並承諾或是不重複進行該不法行為，除此之外，責任國更應該對其所造成之損害負損害賠償責任[50]。而責任可以分為恢復原狀 (restitution)以及賠償(compensation)，此二者應有先後順序之存在，從條文觀察，首先應恢復原狀，在無法恢復之狀況下，則應由責任國賠償行為所造成之損害，而在無法達成前述兩者之情形下，責任國則應採取抵償(satisfaction)，而抵償之方式包含承認不法行為、表示遺憾、正式道歉，或其他合適之方式。而就詳細之請求流程，本文以下圖表示之[51]。

[49] 二元說之看法認為國際責任之構成要件有行為可歸責於國家以及行為違背該國之國際法義務。三元說之看法為基於上述二元說之要件再加上主觀上要有過失。四元說則是基於三元說之要件再加上損害之存在。

[50] 國家對國際不法行為的責任條款草案第 34 條。

[51] 楊尚博，論海上民兵於國際法上的相關爭議－以中國海上民兵為探討核心，頁 48，海洋委員會補助大專生研究計畫，2022 年 10 月。



（表二）國際責任追就流程圖（資料來源：楊尚博，論海上民兵於國際法上的相關爭議－以中國海上民兵為探討核心，頁 48）

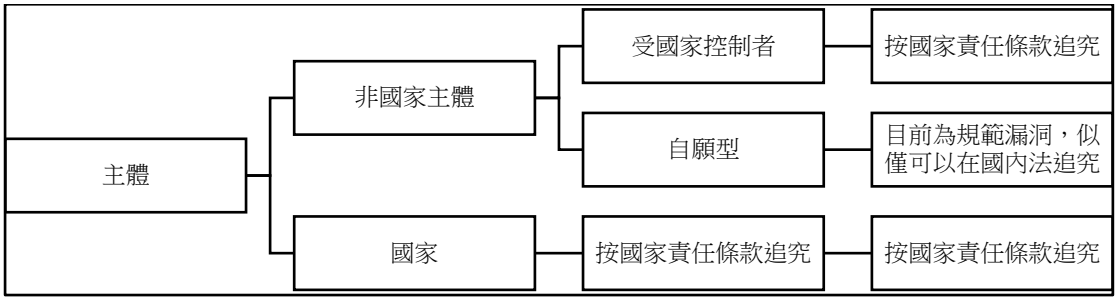
因此在網路攻擊之案例中，首先須判斷該行為之性質是否構成武力使用以及武力攻擊，若是，其行為即違反聯合國憲章第 2 條第 4 項之義務。而受害之國家可以依據上述架構對行為國進行主張以及求償。

而若是國家於武裝衝突時期，在其行為違反武裝衝突法下之規定時，國家可以同樣藉由操作上述架構對行為國進行主張以及求償，兩者之差異只是因行為時之狀態不同而主張之法律有所不同。

然若是非國家主體(Non-State Actor)，其在國際法上之責任追究即富有爭議，而於進行分析前，就非國家主體之討論大致可以分為兩個部分，就目前學者之討論，大多是集中在受國家有效控制(Effective Control)之非國家主體，而就此類非國家主體，因其受國家一定程度之控制以及指使，因此在咎責上有國家責任草案之適用，並無爭議。然而本文認為除此類之外，仍有一類非國家主體

其特性乃自願性從事行為，因其不受國家指使，故無國家責任草案之適用餘地，為一規範上之漏洞。對於此漏洞，在和平時期，本文認為在現行國際法缺乏相關咎責機制之規範下，似僅能以各國國內法相關之機制進行請求，以我國訴訟實務為例，目前外國法人在我國已有提起訴訟之地位，因此在網路攻擊之案件中，受害國若要追求進行攻擊之非國家主體之責任，應可以向該主體所在之國家提起相關之訴訟以利主張及求償。

然而若在武裝衝突狀態，從法律層面觀察，基於日內瓦公約第二議定書之規定，有學者認為目前國際法承認叛亂份子、恐怖份子以以及武裝團體之直接責任[52]，然其未明確指出條文為何，本文推測其所指為第 6 條，在該條文中，第一項明確指出其適用有關於武裝衝突中刑事罪行之追訴以及懲罰，其對於主體之用詞為”No one”，在此解釋下，似乎可以將非國家主體納入其中，然而目前對於此條文之解釋似乎仍只侷限於自然人，因此在責任追究上，似乎只能以個人之方式追究，而無法追究整個團體之責任，且其前提為需要有武裝衝突，因此在此解釋下，似乎排除單方發動網路攻擊，或是在武裝衝突初期之情形，因此在武裝衝突時期自願性之非國家主體，在武裝衝突法之架構下有被咎責之可能，只是要件較為嚴苛。



（表三）國家以及非國家主體之國際責任追究圖（資料來源：本文自繪）

（二） 塔林手冊架構下之探討

《塔林手冊 2.0》中有提及之主體包含國家、國際組織、武裝部隊成員、自發抵抗之民眾、間諜、傭兵以及平民。但其於規定網路攻擊主體時，卻限縮至國家、國家指揮下非國家主體以及國際組織。在此規範模式下，自主性發起網路攻擊之團體因其行為無法歸責於國家因此不符合手冊中第 17 條之規定，因此只能將其可以歸納為第 91 條平民，但是無法被視為武力攻擊之發動主體，在咎責上仍為規範漏洞。因此若其發起網路攻擊，受害者在國際法上似無法請求追究責任。對此，本文認為因此處涉及責任上之追訴，在責任追究上應要有明確之請求基礎較為妥適，因此不宜過度擴張解釋責任主體，較適宜之解決方式為將非國家主體明文納入規範。

網路攻擊之案件在塔林手冊下之檢驗，本文認為承前述之推論，其性質在本文之定位下雖屬於輔助法源中之「各國權威最高之公法學家學說」，但按海牙第四公約之前言，似乎可以推論出各國可以以實踐或聲明之方式進而將塔林手

[52]Mohammad H. Zarei Azar Safari, The Status of Non-State Actors under the International Rule of Law: A Search for Global Justice[p238] (2015)

冊視為國際法義務之一環[53]，似乎進而可認如果有塔林手冊中規範之違反，即可認為是國際義務之違反進而有國際責任之產生，相關之義務包含第 14 條之國際不法網路行為、第 69 條之禁止使用武力或是威脅、第 17 章中對於攻擊客體以及作戰手法之規定，細節包含區分原則、比例原則等原則都可以被視為是國際法上之義務，因此所有前述規則之違反，即有國際責任之產生。因此像是本文主要探討之網路攻擊，在符合武力使用之定義下，即會違反塔林手冊第 69 條之禁止使用武力原則，而需要負擔國際責任。然而此見解目前在討論中尚未有人主張，因在目前多數之實踐下，對於義務之賦予仍以明文法為主，若非以法律、強行法或是一般法律規範賦予義務，其合法性以及正當性會受到很大之挑戰，因此在目前之實踐下，僅能將塔林手冊定性為輔助法源較為妥適且無爭議，但其對於國家並無拘束力亦無法賦予其國際法上之義務。

綜上所述，若國家為發動網路攻擊之主體，在其行為達到武力行使之程度時，不論是在和平時期亦或是武裝衝突時期，受害國均可以依照國家責任公約進行求償，只是其主張規範有所不同。然若是非國家主體時，若其行為乃受國家之控制或是指使，其責任亦可以依國家責任公約進行追究，惟若其為自願性發起行為而不受國家控制或指使時，其咎責為目前國際法上未有完整之規範體系。對此，本文認為在目前法體系下，相較於在國際法上主張，在國內法進行主張以及求償為較為可行之方案。原因在於目前國際法上司法審判機制對於主體之開放程度較低，在多數體系中，僅有國家可以作為主體，多數非國家主體可使用之程序為準司法方式之仲裁，且多用於商務案件，因此在國家責任上使用仲裁作為手段較不妥適且為少見。因此在國際法體系中難以追究時，本文認為使用國際私法為一可嘗試之方法。相較於國際法，各國之國內之司法體系對對於主體之認定較為寬鬆且為開放，目前在國際私法上亦有許多國家會利用他國司法程序進行追訴。因此在面對此新興爭議時，本文認為現行方法下，適用國際法為一暫時可行方式。而就長遠觀之，非國家主體所為之網路攻擊只會越來越頻繁，因此將其明文納入國際司法審判體系中為較長遠之解決方式。而對此，本文認為可以先由各國國內法之立法實踐開始，進而在越來越多國家實踐後有國際組織做成決議將其明文化，在形成一定國際實踐後進行規範為較妥適之方式。

三、 其他相關爭議

[53] 本處前言乃指前言之第 8 段落，原文為:Until a more complete code of the laws of war has been issued, the High Contracting Parties deem it expedient to declare that, in cases not included in the Regulations adopted by them, the inhabitants and the belligerents remain under the protection and the rule of the principles of the law of nations, as they result from the usages established among civilized peoples, from the laws of humanity, and the dictates of the public conscience.中譯為：在頒布更完整的戰爭法規之前，締約各國認為有必要聲明，凡屬他們通過的規章中所沒有包括的情況，居民和交戰者仍應受國際法原則的保護和管轄，因為這些原則是來源於文明國家間制定的慣例、人道主義法規和公眾良知的要求。本文認為按此前言，在頒布更完整有關網路戰爭之相關法規之前，各國可以以聲明之方式，使規章中未包含（即塔林手冊有關於網路攻擊之部分）對其產生拘束力。

而除國家責任外，在目前之塔林手冊架構下，仍有許多待解爭議，本文已於本節第一部分簡述，於此將詳細分析之。

（一） 國家主權義務範圍兼論 VPN 之爭議

網路為一虛擬空間，其在法律上之定位為何不無爭論，目前按聯合國於 2004 年所成立之政府專家小組（Group of Governmental Experts，GGE）於 2015 年的討論中，各國已承認其對於領土的資訊以及通訊科技(Information and Communication Technology）擁有管轄權[54]，而此概念也於《塔林手冊 2.0》貫徹並且更為詳細描述，在《塔林手冊 2.0》第 1 條先明文指出國家主權原則適用於網路空間，而第 2 條以及第 3 條又區分內部以及外部主權，內部主權所指為「一國對於其領土內之網路基礎設施、人員以及網路活動之主權」，而外部主權所指為「一國可以於國際關係中自由進行網路活動」。從此二條文可以看出學者對於國家主權之範圍，已從傳統之領陸、領海以及領空擴張至網路空間。而也因網路空間具有主權後，手冊之第 4 條為禁止侵犯他國主權於網路空間之實踐明文化。

從上述見解可以得知，目前之趨勢為網路空間為國家主權所及，因此國家對於其領土內之網路設施有主權存在，其主權雖不可被他國干預，但其行使主權需要遵守其在國際法上所擁有之義務。因此將網路攻擊之概念置於此討論，若網路攻擊是從一國之 IP 位置所發起，該國對於該 IP 有其主權存在，而其責任以及義務於第 60 條指出，規定國家對於非政府實體之網絡活動有監管義務，且其網路行動必須遵守相關責任以及賠償制度。

基於此條規定，可以認為國家對於其國內之網路 IP 運用似有監管義務之存在，其所援引之概念為《外太空條約》（Outer Space Treaty）第 6 條、第 7 條以及國際電信聯盟之無線電規則第 18 條第 1 項，在上述規則建構下，網路之使用涉及發射到太空之衛星，且發射國因其自然人或法人因其空間物體對其他國家造成損害負有國際責任。換言之，國家對於國內之網路 IP 運用似有監管義務並且若其有不作為需要負連帶責任。對此，本文認為塔林手冊之規定，明文規定了國家對於網路主權之範圍為何，並明確指出國家負有之義務為何，彌補了一部份目前法制上之缺陷，賦予國家一定之監管義務，有助於網路空間之規範發展。

從條文之規範中可延伸探討，純粹私人行為是否可以因此歸責於國家，從歸現行規範之觀點出發，國家責任公約第 11 條表示非代表國家之人所行使之行

[54] United Nations, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174 para.27 (2015)

為不視為國家之行為，但同時國家有保證他國不在己國之管轄範圍內受到個人行為之侵害之義務，就此，在國際法上有發展出國家之「適當注意義務[55]」，而此義務目前也已被充分實踐。從此法理延伸，似乎是賦予國家有不作為之責任，然而，本文認為此責任對國家過苛且不實際，因國家雖然提供其國內之人民使用網路，但若賦予其完全之監管義務，容易使國家為達成義務而以國安政策為由剝奪人民使用網路之權利，限制人民之自由，因此較妥適之方式為從主觀進行限制，只限於國家有重大過失或是故意之情形始得為之。

而在 VPN 之狀況中，行為人會藉由應用程式或是其他方式自由選擇其所欲使用之 IP 位置，因此若其發動網路攻擊，被選擇之國家似乎位於被動之地位，因此國家之責任歸屬為何有討論之實益。就此本文認為仍應由 VPN 所在國負有責任，原因在於，從塔林手冊之觀點出發，國家對於架設在其境內之網路設施有監管義務，因此其對於 IP 之使用亦負有監管義務，且通常其所顯示之 IP 位置會是其虛擬位置，而非其真實位置，因此若要追究其原所在（真實所在）位置之國家責任在舉證上有相當大之難度，使受害者主張以及其求償上之困難。因此使 VPN IP 所在國負擔責任較為妥適。然承本文於前之見解，國家之責任主觀要件應限於國家有重大過失或是故意之情形，否則有責任過重之嫌。

總結上述，本文認為賦予國家監管義務唯一良善設計，為從其背後法理探討，有課予國家過重責任之嫌，反而容易使國家過度限制，因此對於此義務之要求，應從主觀要件上進行修正，只限於在國家有監管義務但是卻因故意或是重大過失不為之時，才可以賦予其責任。而 VPN 之情形，本文從塔林手冊現行規範出發，認為為免舉證困難，應由 VPN IP 所在國負擔責任較為妥適。

（二） 自衛權之主張爭議

就自衛權之爭議，目前國際法上較大之爭執點在於網路攻擊是否可以自衛權，對此本文認為主要之爭議在於目前國際法上可以主張自衛權之前提為聯合國憲章第 51 條之武力攻擊，而網路攻擊是否屬於武力攻擊極為本爭議需要解決之問題。而承本文於前述第二章之定義，網路攻擊是有構成武力使用之可能，而判斷標準為塔林手冊第 69 條之標準。因此在其以為武力使用之前提下，在「規模及效果說」下，若其符合相當嚴重性，該網路攻擊即構成武力攻擊。在此之下，受攻擊之國家即有主張自衛權之可能。惟在自衛權之行使，仍有比例原則之使用，即其手段仍應符合必要性以及適當性。

[55]對此學者李壽平所做出定義為國家在國際法上有義務採取適當注意來防止國內之私人不法行為損害外國人之合法權益。如果國家疏於自己的管理職能，沒有盡到自己應盡職責來防止個人侵害行為而導致損害結果之發生，國家就要因違背適當注意義務而承擔國際責任，參李壽平，現代國際責任法律制度，頁 74，武漢大學出版社，2003 年 1 版。

因此在受到網路攻擊時是否有主張自衛權之可能，仍應取決於其所受攻擊之程度，若其所受攻擊僅達到塔林手冊中所指干涉或是武力使用之程度，該受害國無主張自衛權之餘地，然若其所受攻擊已達到武力攻擊之程度，該國家即可以主張自衛權。

四、 前述案例研析之本文見解

（一） 烏俄戰爭

在本案中涉及之國際法問題有三，首先，因在該戰爭期間，攻擊烏克蘭政府機關之網站之主體，不僅有俄羅斯官方，亦有俄羅斯國境內之民間駭客，就其相關責任之咎責，承本文於前之論述，若主體為俄羅斯，其咎責之法依據為國家責任公約，然若是民間駭客，則需要區分其是否有受政府之控制，若有，其責任同樣可以依據國家責任公約進行追究，然若是自願性駭客，在現行法體系下，進能依各國之國內法求償。接著是因攻擊而使該國網站上顯示非預期顯示之文字，是否構成國際法上之損害，涉及國際法上對於損害之認定，對此，傳統之見解在解釋上多侷限於物理上之損害，但近來有力見解認為解釋上應該擴及功能上之損害，因此若採取較近期之見解，若因攻擊而使網站顯示非預期顯示之文字屬於損害，可以依據國家責任公約進行求償。

（二） 2022 年 8 月境外攻擊我國政府網頁

在本案中涉及之國際法問題有三，首先，若案例中之攻擊真為 APT 27 所發動，即會涉及非國家主體(Non-State Actor)在國際法上之咎責地位為何以及國家是否有監管義務之責任，就此議題，承本文於前之討論，APT 27 在國際上為非國家主體並無疑問，但在咎責層次，則須先區分該次攻擊是否有受到政府之指示以及控制，若其有受控制，在理論上，可以依據國家責任公約追究其背後國家控制之責任，然若是自願性發起攻擊，在目前之架構下只能以國內法以及國內法院進行主張。接著，在案例中假消息之釋放，其是否屬於武力使用或是武力攻擊之一部份，有討論之實益，承本文於前之討論，傳統見解認為只限於物理上之軍武，而本文採取較為擴張之見解，認為只要是作戰手法即可囊括之，只要用於攻擊目的之武器以及其使用方式即屬之，然而釋放假消息是否符合上開作戰手法之定義，本文應採取否定之見解，因就單純適用釋放消息之行為，實難以認定其具有攻擊之目的，且就損害之認定，釋放假消息之損害時難以物理或是功能量化之，因此應採取否定見解較為妥適，以免過度擴張。

五、 小結

總結本章所述，首先是塔林手冊之制定，其確實為新型態之網路作戰制定出初期之規範，使目前在國家或是非國家主體在處理網路相關爭議時有相關規範可以參考，而就總體規範之評價，本文認為現今版本（第二版）之內容已有

一定之完整性，值得肯定。惟塔林手冊目前最大之爭議在於因其在國際法之法源僅屬於輔助法源中之各國權威最高之公法學家學說，在適用順序上落在較次要之地位，且其目前充其量僅為一研究報告，對於各國並無強制之拘束力，因此若要求國家遵守，在現今之狀況下仍有一定之難度。

而就塔林手冊之內容，雖已有一定之完整度，但仍有許多有待釐清之問題，像是 VPN 之在管轄上爭議仍有待釐清。而在網路攻擊之國家責任主張，本文區分和平時期以及武裝衝突時期、國家或是非國家主體之狀態分別進行探討，而大多之狀況均可以國家責任公約進行追究，僅有在自願性發起行為而不受國家控制或指使時，其咎責為目前國際法上之有待釐清之處，仍有待更明確之規範制定。

伍、 結論

網路空間逐漸成為近代國家間角力之空間，隨著科技之發展，網路也逐漸成為各國之作戰手法，而發展至今，仍未有完整且具有拘束力之規範出現。而塔林手冊目前國際上唯一針對網路空間中之行動進行規範之文件。本文以網路攻擊為核心出發探討在國際法上針對此議題以及趨勢應該如何處理。首先是，網路攻擊是否屬於武力使用以及武力攻擊，就此，本文認為傳統見解之解釋過於狹隘，在規範制定速度趕不上相關技術發展時，應在解釋上採取較為寬鬆之態度，故本文任文網路攻擊在符合一定之要件下，應認為其屬於武力使用之一部份，而是否屬於網路攻擊則是其程度而定。而就其所適用之規範，應區分和平時期以及武裝時期來分別探討。最後是咎責問題，本文認為在目前之法架構下，不論是國家或是非國家主體在多數狀況下，均可以依照國家責任公約以及相關國際法規範上就由學理之推論進而咎責之，僅有在非國家主體自願性發起攻擊時為一規範漏洞，有填補之必要。然而目前最急迫之問題為，上述之規範以及學說論述在國際法上對國家之並無強制拘束力，因此學理探討之形式價值遠大於實務之實質意義。

對為未來，本文認為網路空間成為未來衝突空間以及手法已是不可避免之趨勢，相關規範之制定已迫在眉睫，我國亦需要注意相關法制之發展。雖然在規範之建制同時，在實務上對於相關責任追究之舉證責任在實務運作上仍然又相當大的困境，但規範之建置仍然刻不容緩。其中較為快速之方法即為賦予塔林手冊一定之拘束力，使各國有規範可循，而就賦予其拘束力之方式。就長期觀之，最佳之方式為若各國可以以簽署條約之方式為之，能賦予塔林手冊對各國有條約性質之拘束力。然就較為實際之層面出發，由國際組織以作成決議之方式來賦予拘束力不失為一折衷辦法，聯合國在 2022 年所發布之德里宣言，於該宣言中主要是以打擊恐怖主義以使用新型態技術為討論核心，其中其對於跨

國之合作方式多有著墨，因此以國際組織決議為之為本文認為近期較為可行之方式，使網路攻擊能受到一定程度之控制，然而決議之拘束性較條約及薄弱許多。而就達成此類決議之性質及發展，本文認為可考慮承接德里宣言之性質在聯合國之架構下進行發展，從近期聯合國相關規範之發展，多將網路攻擊相關事務歸於反恐辦公室（Office of Counter-Terrorism）進行處理，因此在現今已逐步發展的趨勢下，可交由反恐辦公室進行決議，而於達成一部份共識後，可以聯合國大會決議之方式決議之。將其然而就長期而言，將其規範體系化為最妥適之處理方式，使在相關事件發生時能有相關規範可以援引並且適用，因此就規範之相關發展而言，本文認為可以藉由逐步發展宣言之方式，逐漸累積成可以明文且體系或是法典化之規範，而內容部分，可以參考目前塔林手冊中之相關規範，進行初步之研擬，而因網路攻擊及資安在未來將成為各國國防相當重要的一部分，未來勢必在方式以及態樣上勢必會有更新之發展，因此逐步將相關規範明文化，將有助於各國逐漸思考並研擬對於網路攻擊之應對措施以及相關行動之合法性考量，有助提整體網路空間相關規範之發展，對於世界之網路維安盡一份心力，逐步建立較為安全之網路空間。

參考文獻

一、 英文書籍

Dr U C Jha, Dr K Ratnabali, The Law of Armed Conflict (Delhi, Vij Books India Pvt Ltd,2018)

Gary D. Solis, The Law of Armed Conflict (Cambridge, Cambridge University Press, 2022)

Hans-Joachim Heintze, Pierre Thielborger, From Cold War to Cyber War (Switzerland, Springer, 2016)

Knut Dörmann, Liesbeth Lijnzaad, Marco Sassòli And Philip Spoerri, Commentary On The First Geneva Convention Convention (i) For The Amelioration Of The Condition Of The Wounded And Sick In Armed Forces In The Field(Cambridge, Cambridge University Press,2016)

Michael N. Schmitt, Tallinn Manual 2.0 On The International Law Applicable To Cyber Operations(Cambridge, Cambridge University Press,2017)

Mohammad H. Zarei Azar Safari, The Status of Non-State Actors under the International Rule of Law: A Search for Global Justice(England, Ashgate, 2015)

Rain Liivoja and Tim McCormack, Routledge Handbook of the Law of Armed

Conflict (New York, Routledge, 2016)

二、 英文期刊

Cordula Droege, Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians,[Vol.94] International Review of the Red Cross.(2012)

Dr. Waseem Ahmad Qureshi, Information Warfare, International Law, and the Changing Battlefield, 43 Fordham Int'l L.J. 901 (2020).

Steven Hildreth, Cyberwarfare, CRS Report for Congress(2001)

三、 英文案件及報告

CASE CONCERNING MILITARY AND PARAMILITARY ACTIVITIES IN AND AGAINST NICARAGUA (NICARAGUA v. UNITED STATES OF AMERICA) (1986)

United Nations, "Reports of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," UN Doc. A/68/98. (2013)

United Nations, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174. (2015)

四、 中文書籍

王祥山，非國際性武裝衝突的國際人道法適用問題，一版，中國人民大學出版社，2011 年。

丘宏達、陳純一，現代國際法，三版，三民書局，2012 年。

丘宏達、陳純一，現代國際法，四版，三民書局，2021 年。

朱路，論當代武裝衝突對國際法和戰爭法的挑戰，一版，人民日報出版社，2022 年。

李壽平，現代國際責任法律制度，一版，武漢大學出版社，2003 年。

孟凡明、李國振，武裝衝突法與中國的實踐研究，一版，中國政法大學出版社，2014 年。

姜皇池，國際公法導論，四版，新學林，2021 年。

賈兵兵，國際公法：和平時期的解釋與適用，一版，清華大學出版社，2015 年，

五、 中文期刊

丁麗柏、朱靜，《塔林手冊》對網路攻擊中“武力”的界定及反思，河北法學，第 36 卷第 12 期，2018 年 12 月，頁 82-87。
田力品，武裝衝突法對使用武力之限制，軍法專刊，第 59 卷第 1 期，2013 年 2 月，頁 107-120。
余民才，武力攻擊的法律定性，法學評論（雙月刊）第 123 期，2014 年 1 月，頁 17-28。
季華，《塔林手冊》中有關於網路戰爭的武力使用問題－從國際法角度展開，江漢學術，第 35 卷第 3 期，2016 年 6 月，頁 28-34。
魏靜芬，網路攻擊、網路間諜及網路監控之國際法評價，軍法專刊，第 65 卷第 1 期，頁 18-30。

六、 研究報告

楊尚博，論海上民兵於國際法上的相關爭議－以中國海上民兵為探討核心，海洋委員會補助大專生研究計畫，2022 年 10 月。

七、 網路資料

Ukraine cyber-attack: Russia to blame for hack, says Kyiv，網址：https://www.bbc.com/news/world-europe-59992531，最後瀏覽日期 2023 年 9 月 13 日。
臺灣 8 月初因裴洛西訪臺而遭到網路攻擊的事件總覽，網址：https://www.ithome.com.tw/news/152491，最後瀏覽時間：2022 年 9 月 8 日。
ICRC, Conduct of hostilities，網址：https://casebook.icrc.org/law/conduct-hostilities#footnote63_4nfz02z，最後瀏覽日期 2023 年 9 月 8 日。