復興崗學報
民 106 年 12 月，111 期，1-26

新興網路恐怖主義的挑戰與因應對策：社會建構論的觀點

鄒文豐

淡江大學國際事務暨戰略研究所博士生

摘　要

隨網路恐怖主義持續發展，新型態的網路恐怖主義著重在透過網路教育徒眾、意識啟發，並「激進化」潛在支持者的「感召」層面，即透過「啟發」與「激進化」潛在的、具特定背景的人士，促成「孤狼式」恐怖攻擊。當前恐怖組織不僅可如過去運用網路進行宣傳、網路攻擊或其他犯罪行為，更可能使用網路攻擊關鍵基礎設施，成為國際社會的重大安全挑戰，基於網路恐怖主義的本質與特性，本文嘗試透過國際關係「建構主義」理論的「社會建構論」觀點，理解網路恐怖主義行為者的背景及動機，並認為應對新型網路恐怖主義威脅，應分別從國際、國家與社會層面著手，從根本上消除網路恐怖主義激進化潛在分子的機會，才是治本之道。

關鍵詞：非傳統安全、恐怖主義、激進化、心理威脅、社會建構論

Challenges and Response Strategies of Emerging Cyber Terrorism: From the Perspective of Social Constructivism

Wen-fengTzou

Doctoral Student, Graduate Institute of International Affairs and Strategic Studies,

Tamkang University

Abstract

With the continuing development of cyber terrorism, new types of cyber terrorism have focused on educating those potential supporters who have specific backgrounds through the Internet, inspiring their awareness and radicalizing their psychological side to form the lone-wolf terrorist attack.The current terrorists can use the internet not only to propagate, attack or other criminal acts, but also to assault crucial infrastructure, and this becomes a major security challenge for the international community.From the perspective of social constructivism in international relations, the author studies the innate characteristics of cyber terrorism, and the behaviors, backgrounds and motives of terrorists, believing that the best way of resolving the threat of cyber terrorism is to find and deal with cybercrime radicals through coordinated international, national, and social efforts.

Keywords：non-traditionalsecurity, terrorism,radicalization, psychological threat, social constructivism

壹、前言

美國情報與安全研究所(Institute for Security and Intelligence)研究員 Barry Collin 率先於 1996 年提出「網路恐怖主義」(cyber terrorism)，論述網路世界與恐怖主義結合所產生的高度威脅，引起各界對網路安全的重視(Collin, 1996)。其後，即有學者陸續在網路戰、網路犯罪、網路恐怖主義等領域，探討網路襲擊技術、方式與影響，並對網路恐怖主義訂定多種定義。

鑒於恐怖分子早期以駭客(hacker)手法，藉惡意軟體所行的電腦病毒癱瘓、竊密，或執行實體破壞等網路攻擊行動，已轉變為透過網際網路為訊息載體，進行人員招募、資金募集與理念傳布、威脅恫嚇的重要途徑，並透過心理感染、意識扭轉、精神施壓等方式發揮其「激進化」(radicalization)影響，新型網路恐怖主義已成為當前國際社會安全及秩序的重要危害。

特別是儘管「實體的」伊斯蘭國(ISIS)即將走向敗亡，然自 2016 年末接連出現的德國、土耳其、英國、俄羅斯、瑞典、埃及等暴力襲擊案件可知，兇嫌均由網路接觸 ISIS 極端主義思想，部分案件行動亦與 ISIS 網路聯指有關，而這些案件之後，ISIS 更大力於社群網站發動宣傳攻勢，企圖招募、吸引更多恐怖分子，顯見虛擬世界的恐怖活動發展已突變成型(Berger, 2017)。如 2017 年 5 月，英國內政大臣 Amber Rudd 就其國內年來恐怖攻擊事件，於歐盟內政部長會議表示，現今許多恐怖組織利用社交網路媒體為平臺，藉以招募成員並輔助行動，呼籲歐盟各國必須採取相應措施打擊此類網路恐怖主義，亦期望網路社群公司能設置更多屏障，防止恐怖分子藏身網路進行不法活動(BBC News, 2017A)。

儘管國際關係現實主義(realism)學者曾嘗試以「安全困境」(security dilemma)理論說明國際社會面臨的網路安全情勢(Stephen, 2017)，但國際社會與學界卻仍缺乏對新型網路恐怖主義成因與特徵的探究，並深入思索因應之道。因此，本文的問題意識即在於，新型網路恐怖主義較之於傳統恐怖主義與活動究竟有何不同？過去定義是否能清楚描繪新型網路恐怖主義的樣貌？而新型網路恐怖主義又將對國際社會帶來何種威脅與挑戰？因應對策該從何而生？

基於網路環境是遵循文化、思想、社會、宗教、政治與經濟等不同領域所

形塑的人為活動空間，新型網路恐怖主義則係鑲嵌於國際社會中的「現象」(Ciolan, 2010)，藉由學者 Ciolan 所提〈定義 21 世紀安全議題的網路安全：一個建構主義者的途徑〉(***Defining Cybersecurity as The Security Issue of The Twenty First Century: A Constructivist Approach***)一文得到的啟發，本文認為新型網路恐怖主義所涉及的是危害國際社會安全與秩序的問題，因此最適宜透過「建構主義」(constructivism)中，「社會建構論」(social constructivism)的觀點，分析新型網路恐怖主義的成因、發展及動機，並由此基礎研擬相關因應對策。本文首先藉回顧「傳統的」網路恐怖主義，對比新型網路恐怖主義的特點；其次，則在說明社會建構論的理論概要及其對網路恐怖主義的主張；再次，續就新型網路恐怖主義的挑戰，從社會建構論的觀點提出對策看法。

貳、網路恐怖主義的進化與發展

學界對恐怖主義仍未能有一致性定義，其原因不僅在於形成恐怖主義的背景、成因、動機複雜，亦在於遂行恐怖主義的目的、手段、方式無法一概而論。2004 年 10 月，聯合國安理會第 1566 號決議案曾將恐怖主義定義為犯罪行為，包括故意造成平民死亡、重傷或劫持人質，其目的在挑起一般民眾或特定人群的恐怖狀態，以恐嚇群眾或迫使政府、國際組織從事或不從事特定行為(United Nations Security Council, 2004)。事實上，恐怖主義就是一種基於政治、宗教或特定理念訴求的計畫性暴力攻擊，其對象包括政府、特定組織甚至平民，主要策略是要製造社會恐懼，藉此產生心理威脅與不安全感，達成其所欲目的，因此，恐怖主義活動也常會藉助媒體宣傳以擴大其效果(方天賜、孫國祥，2007)。

網路恐怖主義為傳統恐怖主義透過網際網路的應用行為，正如同網路資訊多元、豐富且龐雜的特性，自網路恐怖主義於 20 世紀末逐漸出現後，由於學者間採取的立場及觀點各有不同，學界對其定義大致均未脫離網路攻擊與恐怖主義的核心概念，惟仍未能有一致看法，也易與網路犯罪及資訊戰等意涵產生混淆，隨近年恐攻案件所顯示網路恐怖主義威脅層面、方式日益廣泛，其概念不僅需重新定義，更需符合現況特徵。

一、「傳統的」網路恐怖主義

網路發展初始階段，因欠缺資訊傳遞相關規範與安全防護觀念，以及網路活動具有的隱密性、匿名性、跨越時空等特性，使網路成為重要犯罪管道，對資訊社會秩序產生重大危害，1990 年代後期以非國家行為者為主體的網路犯罪活動，是為早期「網路安全」研究的主軸。1996 年斯里蘭卡民族主義武裝組織「塔米爾之虎」(Liberation Tigers of Tamil Eelam, LTTE)針對斯里蘭卡駐外使館發動電子郵件病毒攻擊，被視為最早有紀錄的網路恐怖主義攻擊事件(Gordon, 2002)；此後，如 Barry Collin、Mark Pollitt 等學者，即先後論述網路與恐怖主義結合可能造成的安全威脅，開啟學界對網路恐怖主義的研究(Pollitt, 1997)，是年 12 月聯合國第 51 屆大會第 210 號決議亦提及：「各國必須高度重視恐怖分子利用電子產品、有線通訊系統與網路工具進行的犯罪行為」，顯示網路恐怖主義自 20 世紀末開始被視為恐怖活動的型態之一(Ariely, 2008)。

雖然當時研究聚焦於恐怖組織因政治動機而對電腦系統與程式、資訊傳遞與資料庫等進行的攻擊，但「911 事件」發生後，美國聯邦調查局(FBI)查出恐怖分子除以網路郵件進行聯絡，更運用網路途徑宣揚恐怖主義、募集資金、協調行動等，凸顯利用網路協助恐攻，不僅提高效率，更如 2000 年澳大利亞工程師以網路攻擊昆士蘭省廢水處理系統，致使大量水源遭汙染的案例(EastWest Institute, 2010)，恐怖分子以網路攻擊手段癱瘓、破壞關鍵基礎設施的威脅，已使各國認識到網路襲擊將可成為隱密性及執行效能均高，付出代價卻相對較低的恐怖行動。

學者指出，網路恐怖主義係為恐怖組織基於政治目的運用網路空間，而有兩類行為模式，第一是進行實質網路攻擊，類似於網路犯罪，可分為三個層次的威脅(Siboni, 2014)：

(一) 資訊層：針對一般電腦、網路服務的攻擊，目的在竊取資訊、破壞系統運行、造成不便或強迫宣傳，如 2004 年蓋達組織(Qaeda)企圖在矽谷公司(Silicon Valley Landsurveying Inc.)網路系統植入恐嚇影片的事件(Musharbash, 2004)。

(二) 系統層：針對電腦系統、資訊網絡與商務服務的攻擊，目的在造成社會重大損害並散布灌輸恐懼感，如 2012 年 11 月哈瑪斯(Hamas)旗下

駭客以「分散式阻斷服務攻擊」(DDoS)方式，癱瘓以色列特拉維夫證券交易所、國際銀行網路交易與航空公司網站，使其被迫中斷運作與服務(Khaleeli, 2014)。

(三) 實體層：試圖針對水力、電力、能源、交通、金融等關鍵基礎設施操作系統的網路攻擊；如歐盟官員曾指出，藉入侵「監控與數據擷取系統」(Supervisory Control and Data Acquisition)，各國核電廠、水壩、空中管制與地面交通中心均可能遭受網路恐怖攻擊(Lewis, 2014)。

第二是利用網路支援恐怖活動，主要是為籌集資金、洗錢或招募成員等。恐怖組織活動可分為資金募集、資金流動、人員募集、人員訓練、專業技能養成、攻擊準備及攻擊執行等階段(林泰和，2011)，而網路作為工具，扮演訊息載體、階段串連的重要角色。如與 Qaeda 有關的「全球紓困基金會」(Global Relief Foundation, GRF)、與哈瑪斯組織(Hamas)有關的「聖地救援暨發展基金會」(Holy Land Foundation for Relief and Development)及「可蘭文學中心」(Quranic Literacy Institute)等，支持者可於其網頁得知捐款訊息、進行信用卡網路捐款，再由恐怖組織透過網路進行資金分配與運用(Passas, 2007)。摩洛哥情報資深官員更指出，Qaeda 過去向來在清真寺等地點直接招攬成員，但如今90%的恐怖組織分子均依賴網路招募(Berger, 2015)，可知藉由運用宣傳策略，壯大組織亦已成為網路恐怖主義的重要部分。

二、「2.0 版網路恐怖主義」的定義

網路恐怖主義受到各國政府與學界注意後，安全機構及學者分別嘗試賦予其不同層次的定義，如 Ronald Dick 認為，網路恐怖主義係透過網路從事暴力行為，以導致生命、財產損失，威脅政府改變政策(Dick, 2002)；Clay Wilson 定義網路恐怖主義為具政治動機的非國家行為者或秘密人員，以電腦為武器，藉襲擊重大目標或影響他人為手段，迫使政府改變政策(Wilson, 2008)；Mark Pollitt 則表示網路恐怖主義是非國家行為者有預謀的經由網路途徑襲擊以非政府機構為主的單位，藉破壞資訊、電腦系統等，達成政治目的(Pollitt, 2011)。

在政府方面，FBI 定義網路恐怖主義為非國家行為者與秘密組織對資訊、計算機系統、演算程序及數據，所進行有預謀、具政治動機的蓄意攻擊，目

的在造成對象心理與物質的嚴重傷害，進而實現其訴求(Gordon, 2002)；美國國防部則認為網路恐怖主義是非國家行為者利用計算機及電信能力，針對資訊、電腦系統、電腦程式實施的犯罪行為，以造成暴力與對公共設施的破壞，製造社會恐慌，旨在影響政府或社會實現特定的政治、宗教或意識形態目標(Ariely, 2008)。

依此，Dorothy Denning 進一步指出，網路恐怖主義合併自恐怖主義與網路攻擊兩者的概念，係以非法攻擊方式威脅電腦設備、網路系統與資訊儲存安全，藉以恫嚇政府或其他組織、個人，達到特定政治或社會目的；此外，這種威脅可能造成人身安全、設施、財產的損害，並足以引發一定程度的心理恐懼(Saita, 2003)。Denning 的定義即為學界認為的「純粹網路恐怖主義」(pure cyber terrorism)。綜整網路恐怖主義的要件包括：

(一) 行為體係恐怖組織或相關團體、個人；

(二) 動機與目的係有特定的政治、宗教、意識形態訴求；

(三) 途徑與工具係透過網際網路達成目標；

(四) 目標係藉癱瘓資訊系統或國家關鍵基礎設施等實體破壞，造成社會經濟重大損失、製造大眾心理恐慌並藉此脅迫對象順從、放棄原有生活模式與政治價值觀。

由此可知，網路恐怖主義與駭客行為、網路犯罪及網路戰等，存在本質上的差異。首先，駭客攻擊與網路犯罪通常歸類為相同範疇，主要是出於個人目的或商業利益，以電腦及網路為工具的犯罪行為；其次，網路戰主要係指國家行為者運用電腦與網路所從事的破壞或攻擊行為(Lewis, 2012)。藉由對行為者動機、身分等不同面向的判別標準，網路恐怖主義的定義更能明確，只是前述定義著重在網路恐怖主義活動對資訊系統、硬體設施的直接危害與連帶心理威嚇，聚焦於攻擊目標，卻忽略在網路資訊傳導特性下，網路恐怖主義對其支持者或潛在受眾所可能產生直接的宣傳、心理感染與意識啟發(Inspired)效果，而間接發展出對社會安全秩序的危害。

儘管 2010 年底發生的「阿拉伯之春」(Arab Spring)革命浪潮並非受網路恐怖主義的影響，然其引發大規模群眾抗爭的關鍵，即在網路於資訊、政治理念及價值觀方面的推波助瀾，顯見如臉書、推特、YouTube、Flickr 等網路社交工具對「網路世代」的重要影響力(程富陽，2012)。而之後 ISIS 坐大，亦與其高度運用網路宣傳、招募支持者以壯大組織密切相關(Callimachi, 2015)。事

實上，隨資訊技術普及，恐怖組織透過網路宣揚理念已為必然趨勢，如 Qaeda、Hamas，雖然理念訴求各有差異，但在生存空間面臨強大壓迫時，卻不約而同選擇運用網路維持發展，原因即在於一方面可借助網路的便捷性及隱蔽性，有利其遂行遠端聯繫及行動操控；另一方面，網路攻擊成本低廉與相對安全，卻有更高的破壞效能，也對恐怖組織深具吸引力。更重要的是，透過網路，恐怖組織得以進行宣揚理念、招攬成員、募集資金、散佈威嚇訊息等攻心作為，不僅帶來更大效益，亦為造成當前各國社會混亂與不安的重要潛因(Ariely, 2008)。

是以當前網路恐怖主義威脅，不僅在網路攻擊與造成附帶心理恐懼的層面，亦在於透過網路宣傳理念、號召支持，以及教育徒眾、意識啟發、「激進化」潛在支持者的「感召」層面。「啟發」意指具有宗教、種族或社會背景的人士，原已具有某種程度的攻擊傾向或反社會性格，在接受媒體宣傳、暗示或煽動後，獲得執行恐怖攻擊的概念或指導(Moore Tyler, 2016)。網路科技與社群媒體的興起即成為「啟發」的絕佳平臺，因為不需要人際間的實體互動，更不必加入恐怖組織，只要透過網路社群灌輸觀念，即可產生「激進化」的效果。而「激進化」通常是指採取一種被主流社會拒絕的世界觀，並以此將暴力合理化，藉以促使社會與政治現況的改變(Hafez and Mullins, 2015)。「啟發」與「激進化」並不一定有先後關係，但卻能產生相乘效果，與以往恐怖分子不同的是，當前的「啟發」與「激進化」不再透過組織聚會的型式，轉為多由線上論壇、影音網站及網路社群所促成，成為網路恐怖主義的最新型態。

因此本文認為，在此種動態威脅變化下，網路恐怖主義應重新定義為：「恐怖組織為達成特定目的，以網路為工具及載體，所遂行的實質攻擊、理念宣傳或心理攻勢、人員或資源募集，以及與恐怖攻擊相關的訊息聯繫、啟發與激進化行動者的行為」。

三、新型態特徵

自 2010 年以來，歐洲恐攻事件的增加，與阿拉伯之春引發的政治動盪、敘利亞內戰產生的系列影響，以及 Qaeda 中心弱化、網路社群媒體推波助瀾等有密切關聯(Nesser, 2014)。其中，從 2015 年開始，歐洲正面臨近 20 年來恐

攻威脅的最高峰，以 ISIS 為名，至少在 18 個國家直接執行或啟發 50 起恐攻事件，而多起連續恐攻發生主因，即為網路科技及社群媒體興起，使恐怖分子不再需要實際人際互動，只要經由線上論壇或影音網站，就可將西方穆斯林社群與極端宗教思想密切結合，而嚮往「聖戰」者也不必加入恐怖組織，其「激進化」過程往往發生在家中等私密地點，加上匿名特性，已構成歐洲社會治安的嚴峻挑戰(林泰和，2017)。歐洲刑警組織(European Police Office, Europol)進一步指出，恐怖組織網路媒體的啟發與激進化具有極高效率，特別是針對「孤狼式」恐怖分子的激進化更扮演關鍵角色，尤其 ISIS 最擅長使用網路社群媒體，以鼓勵恐怖分子從事「孤狼式」攻擊(European, 2016)。

學者分析恐怖分子受網路激進化的過程，係經由兩個層面的運作(林泰和，2016)：

(一) 網路成為被動資料庫，提供個人接受極端意識形態的管道，孕育對外在事件的憤怒；

(二) 網路社群的匿名特性可讓訊息提供者推動更激進暴力的想法，造成累積效應，激進化暴力極端主義至頂點。

正因網路特性可使恐怖分子不易受到偵測、防堵及追查，使得網路與恐怖主義匯流已是未來趨勢，恐怖組織不僅可如過去運用網路進行宣傳、攻擊關鍵基礎設施或從事其他犯罪行為，更可透過啟發與激進化手段促成「孤狼式」恐怖攻擊。歸納其特徵為：

(一) 成本低廉：僅須透過基本資訊設備與網路，即可傳遞訊息、宣傳理念及號召支持，即以駭客手法進行網路攻擊，亦無需依賴大量資金，就可獲得更大成效。

(二) 行蹤隱密：依靠網路虛擬特性，恐怖組織更易隱藏其中，使其難被察覺，而網路空間無遠弗屆，恐怖組織可於世界任何角落從事不法活動。

(三) 行動安全：網路恐怖活動無須耗費大量時間、金錢招募行動人員，其訓練門檻低，亦屬間接操作，使恐怖組織更易招攬及保留追隨者。

(四) 目標多元：網路恐怖活動的針對目標既可是政府、企業、個人、公共設施等實體，更可是心理意志、思想價值、生活型態等虛擬概念。

(五) 效益深遠：憑藉資訊傳播的影響力，任何恐攻事件抑或網路恐怖活動本身，均能透過網路宣傳推波助瀾而引起更大關注，更有助其宣揚理

念。

(六) 防範困難：現實世界對網路的依賴性與形成的脆弱性，已使恐怖組織更有可趁之機，其對實體設施、資訊體系乃至於社會心理、秩序等的破壞，也更難以事先防範。

可見，這樣的網路安全威脅已改變安全與衝突的社會結構、規範及參與規則，暴力的定義與平民、威脅來源的界線也都將模糊不清。具有此等特性的網路恐怖主義，更需要重新以政治、經濟、軍事、社會、教育、文化等綜合性思維評估安全對策。

參、社會建構論對網路恐怖主義的觀點

國際關係的建構主義理論發展有其脈絡，重要著作如 Alexander Wendt 著有「國際關係理論中的代理結構問題」(***The Agent-Structure Problem in International Relations Theory***) (Wendt, 1987)、「無政府狀態是國家的產物：權力政治的社會建構」(***Anarchy is what States Make of it: The Social Construction of Power Politics***)(Wendt, 1992)、「國際政治的社會理論」(***The Social Theory of International Politics***)(Wendt, 1999)，以及 Nicholas Onuf 的「我們製造的世界：規則及社會理論與國際關係中的規則」(***World of Our Making: Rules and Rule in Social Theory and International Relations***)(Onuf, 1989)、FreidrichKratochwil 的「規則、規範與決策條件：國際關係及國內事務的實踐與法理推論條件」(***Rules, Norms, and Decisions－On The Conditions of Practical and Legal Reasoning in International Relations and Domestic Affairs***)(Kratochwil, 1991)、與 Martha Finnemore「國際社會中的國家利益」(***National Interests in International Society***)(Martha, 1996)等，儘管學者們運用的脈絡及元素各有差異，卻共同構成了建構主義的內涵。

建構主義理論有三項主要論述，首先分析國際體系的基本結構與成員單位間的互動狀態，強調行為者與國際體系的互動關係；其次則將其延伸到對國際體系行為者自主能動性的重視，認為國際環境可透過行為者的互動實踐而產生改變，故國際環境具有「社會性」的取向；再次，則依此提出，國際關係的變化是可能的，其根源於行為者對國際體系的認知，並非僵化的依循國際社會是

無政府狀態的邏輯(秦亞青，2006)。其中，Onuf 於 1980 年代提出社會建構論相關論述，成為建構主義內涵的重要部分，主張國際體系的本質為一個社會結構，此結構在物質要素外，亦包含規則、規範與身分等理念領域的非物質性元素，國際體系結構與行為者間是一種相互構成的關係，應將物質主義解凍，將無政府狀態多元化，並將理念元素注入國際政治的理論範疇內(Onuf, 1989)。既以恐怖主義的主要行為者是非國家與次國家團體，而冷戰之後，恐怖主義多肇因於文化衝突，社會建構論認為國際體系中，對行為者的影響來自於認同與利益(Ciolan, 2010)，如何掌握安全研究中，文化與規則等非物質的理念因素，對理解危害國際社會安全與秩序的問題，並思索因應之道，將是相當重要的途徑，因此，本節將概述建構主義理論中，社會建構論的要旨，以及其對網路恐怖主義的看法。

一、理論概要

建構主義做為當前主流國際關係理論之一，提出對於將國際關係視為人際關係此種理論假設的反思，而從理解個人及社會關係開始，思考認同與利益的形成及互動過程，並將這樣的探索，投射到制度與國際層面上(Ciolan, 2010)。建構主義的理論觀點，在於審視國際關係的文化內涵，分析國際體系觀念結構對國家身份與利益的建構作用，並質疑無政府狀態等既有國際關係理論的基本假定，從社會互動角度提出新的國際關係研究議程，創建以「觀念」為主要內容的國際政治體系結構理論(Eriksson and Giacomello, 2004)。

Wendt 認為，國家認同與利益不是預先給定的因素，而是在國家之間的互動中得以建構的；主權、無政府狀態等國際制度同樣也是社會建構的結果。其將國際關係理論劃分為四個框架，包括(Wendt, 1999)：

(一)整體主義／物質主義理論，包括世界體系理論及新葛蘭西馬克思主義。

(二)整體主義／理念主義理論，包括英國學派、世界社會理論、後現代國際關係理論、女性國際關係理論等。

(三)個體主義／物質主義，包括古典現實主義和新現實主義。

(四)個體主義／理念主義，包括古典自由主義和新自由主義。

Wendt 將社會建構論界定為整體主義／理念主義理論，即在方法論上，呈現明顯的社會性質，強調整體對個體的作用，在國際關係領域，就是國際體系結構對國家的作用，重視國際體系文化，如共有知識、共有期望、共有觀念等對國家的意義。

社會建構論並不否認現實主義以國家為國際社會主要行為者的核心論點，但不同意國際社會必然將成為無政府狀態下的弱肉強食世界，而認為每個國家基於理解、價值與規範等理念因素，經由相互交往，形成互為主體的關係，並據此形成國際間的互動型態(Wendt, 1999)。是以國家間並不必然存在先天衝突、合作或共存關係，而取決於彼此如何認定對方，也就是無論合作與衝突，都不是無政府狀態國際社會的必然結果，現象如何，取決於國際社會成員如何建構彼此間的關係(秦亞青，2006)。

Onuf 指出，行為者與社會是相互構成的，在此過程中，「規則」發揮至關重要的中介作用，規則指導行為者的社會實踐，同時建構社會與行為者；以此推及國際體系，其與行為者之間就是一種相互構成的關係，此結構包括理念及物質要素，而無政府狀態是國際社會建構的結果，國際社會是一個具有規則的社會，規則造就並維持秩序，透過行為者之間的互動產生實踐活動，其所建立的觀念結構就會產生穩定作用(秦亞青，2006)。依此，共有知識等理念要素建構行為者的認同與利益，也就形成不同的安全態勢，如行為者間相互高度猜疑，慣於從負面觀點評估對方的行為動機及意圖，就會形成「安全困境」的社會性結構；相反的，若行為者間的共有知識使其能相互高度信任，即便存在利益衝突，也能透過協商途徑解決，就能形成「安全共同體」(security community)的社會狀態(Ciolan, 2010)。

社會建構論強調行為者與社會結構的互構，是雙方雙向的作用，行為者主體間的實踐活動，形成「互應邏輯」(logic of reciprocity)的機制(Ciolan, 2010)，一方面，行為者間的互動構成社會結構，社會結構也建構了行為者的認同及利益，在國際社會中，行為者可以是國家或非國家行為者，結構則是國際體系中的觀念分配或稱為「國際體系文化」。國際社會的無政府狀態就是經由這樣的過程建構的一種文化，雖然「現實主義」或「自由主義」(liberalism)等國際關係理論，都將無政府狀態作為先驗給定的國際體系結構，但在社會建構論的觀念中，依據行為者互動性質的不同，即可能存在多種無政府狀態文化，Wendt 即歸納霍布斯(Hobbesian)、洛克(Lockian)與康德(Kantian)等三種不同的國際體

系無政府狀態文化，做為建構主義重要的理論內涵(Wendt, 1999)。

霍布斯無政府文化是現實主義的邏輯，即以相互敵視、相互殘殺為特徵，是國家互存敵意、互為敵人的無政府文化；洛克無政府文化則不同，國家不再互視為仇敵，不以消滅敵人為目的，承認彼此都具有生存及擁有財產的權利，國家間的主要關係是競爭者的關係;康德無政府文化則是以國家間互為朋友為基本特徵的體系文化，國家不會使用暴力解決利益衝突，若友邦受到威脅，另一方會鼎力相助，實際上就是安全共同體的形式。Wendt 認為霍布斯文化已是過去，洛克文化是現在，而康德文化則會是將來國際社會的主導特徵；就社會建構論而言，既以物質性因素意義有限，社會結構形成與存在是行為者社會實踐的結果，其互動過程是社會結構存在的基本條件，則意味面對新興網路恐怖主義等非傳統安全議題，因安全實踐的邏輯與性質均已產生各種變化，並導致許多不同而難以預料的結果，更需要藉由社會建構論的不同觀點，提出新的安全典範框架(Ciolan, 2010)。

二、觀點主張

由於網路空間已被視為恐怖分子最重要的聚會場域，以交流、討論及分享其理念，此外，極端主義網站正在迅速擴張，為恐怖分子提供廉價、快速、隱蔽、高效的資訊途徑，透過運用網路部落格、論壇或社交媒體渠道，使恐怖分子得以傳播及辯論各種想法、技巧，甚至進行虛擬培訓，成為極端主義團體的虛擬訓練營(Cornish,Hughes and Livingstone, 2009)。如以歐境而言，大部分穆斯林社群長期無法與當地社會順利融合，且經常受到就業、就學與生活等各方面歧視，這樣的環境成為恐怖組織發展「聖戰意識」最佳的萌芽土壤，「啟發」與「激進化」則扮演其中的關鍵角色，從行為者間互動模式加以探討，一方面，恐怖組織利用暴力行為挑戰政府，另一方面再利用政府的強力反制，扮演被壓迫者角色，藉此取得反抗行為的正當性，使得發展網路恐怖主義對其不僅是重要的策略應用，也是協助達成目標最適切的執行工具(Ciolan, 2010)。

社會建構論指出，網路環境是繼文化、思想、宗教、經濟、社會及政治議程後最有吸引力的議題空間，而網路恐怖主義行為者的動機可由其主觀意識進行解釋，目的是要獲取戰略或政治優勢，或嚴重損害目標國家或特定族群所欲

維護的物質及心理利益(Cornish,Livingstone and Clemente, 2010)。其威脅主要包含幾種方式(Bogdanoski and Petreski, 2013)：

(一) 新興的網路恐怖主義網站幾乎不會提供任何有關暴力行動的訊息，相反的，主要在陳訴所遭受的迫害，並將本身及追隨者描述為外來勢力壓迫的受害者，以啟發並激化真正處於弱勢、離散族群與偏差認知的視聽觀眾。

(二) 如焚燒國旗或領導人圖像等，具煽動性與汙衊性的象徵政治符號也會在相關網站上播放，這類對於形象與受眾信心的傷害將更甚於金融風暴。

(三) 社會建構論提出「鏡中自我」(looking glass self)的概念，也就是行為者的行動將反映其他行為者的反應；網路恐怖主義行為者的網路攻擊行動，反映的是可能其民族、宗教與信念自豪感受西方價值侮辱的結果(Eriksson and Giacomello, 2004)。

面對這樣的國際安全情勢變化，社會建構論認為，過去「安全」被認知為國家及政府的義務，依賴的是對外政策或情報社群與軍事能力，然而，對於當前關鍵基礎設施、各類網路社群及社會秩序面臨的威脅，國家及政府不再能提供必要的安全保障，維護國際與內部社會安全，已成為人類社群的共同責任，促進次級團體及個人行為者參與網路安全行動，將與國際、國家間確保數位環境穩定一樣重要(Eriksson and Giacomello, 2004)。社會建構論亦認為，行為者身份認同的形成，是在特定情況下透過社會化發展的集體理解結果(Wendt, 1999)，行為者的行為與反應，受到其對所處環境的感知，包括技術物質及感受理念的影響；此外，威脅也是一種經過互動過程的感受理念建構，如關於網路安全議題，許多攻擊場景是在假設中創造出來的，因為從個人、特定社群、資訊電子產業到各種國家機構，這些不同的利益相關者參與安全政策制定及執行的進程，必然將強調其觀點與利益，乃至於對構建未來網路空間環境的看法，是以今日的安全觀更重視的是想像中的威脅(Eriksson and Giacomello, 2004)，制定安全政策的新框架將是論述能力的表現，而非以往常規的政策制定程序(Baylis, Smith and Owens, 2011)。

社會建構論亦以「本體性安全」(ontology security)的觀念，指出倫理、道德與價值認同有助於形成社會中的凝聚力(Wendt, 1999)，自身安全是本體性安全的核心，每個個體都需要能使本身行動與互動的穩定圖像，如果這個圖像與

身分認同的概念被移除，將使其對所處環境感到擔心(Mitzen, 2006)。網路恐怖主義利用的正是社會由本體性安全生成的兩大恐懼，對隨機與劇烈傷害的恐懼，以及對資訊服務失控的恐懼(Eriksson and Giacomello, 2004)，由於在網路空間，暴力的社會結構與平民、戰鬥人員間的界限是模糊的，使得新型態網路安全威脅改變過去的社會衝突結構，以及其中的規範和參與規則，因此，因應新興網路恐怖主義的威脅，社會建構論思考的是如何透過行為者詮釋世界的認知思想，建立一套穩定的利益與身分認同結構制度，而這套制度只有藉由行為者的社會化過程與參與集體認知才能產生影響(Ciolan, 2010)，網路安全制度的形成，必須是行為者共同合作以建立新的網路規範及國際立法，才能保護國際社會免受網路恐怖主義的危害。

肆、如何因應挑戰

網路恐怖主義的快速發展導因於兩大方面，首先是西方國家於中東長期進行的反恐戰事，固有打擊恐怖組織成效，但對消弭恐怖主義與極端思想仍待持續努力，在如 Qaeda、ISIS 等恐怖組織生存空間受到壓縮的態勢下，反而刺激其轉往虛擬空間繼續發展的動能；其次，也由於國際各地恐怖攻擊不斷，復以西方國家複雜政治、經濟與難民問題難解，益加激化社會矛盾，許多移民社群無法與當地社會順利整合，在長期飽受歧視的狀況下，更為網路恐怖主義中的理念激進化提供絕佳的受眾，既與網路恐怖主義形成相互鼓勵的循環，在大批具有作戰經驗的「聖戰士」逃返歐洲後，勢將對國際反恐形勢投下更多變數。

一、發展趨勢及未來挑戰

2015 年 12 月美國加州聖伯納汀諾恐攻事件的受害者家屬，於 2017 年 5 月向美國聯邦法院控告谷歌(Google)、推特及臉書，指控這些社群網路公司涉嫌為 ISIS 提供平臺，從而導致恐攻兇嫌得以從中模仿、發動暴力襲擊，其辯護律師進一步表示，這些網路公司長年輕率提供帳號，使恐怖組織能利用社群網路進行極端主義宣傳、籌集資金與招募新成員。我國國家安全局 2017 年「國

際恐怖攻擊事件態樣分析暨我國世大運反恐作為」報告則指出，「廉價高效」是當前恐攻手法的最新趨勢(立法院，2017)，ISIS、Qaeda 等恐怖組織即藉網路宣傳號召支持者運用車輛、刀斧等各類工具發動「孤狼式」恐攻，尤其年來已有上千名 ISIS 分子返回母國，在社群媒體難以掌控的情況下，倘若擴大網路社群極端主張的「激進化」影響，勢將形成各國反恐作為的嚴峻挑戰。

而在歐洲之外，學者認為，其他如印尼、馬來西亞與菲律賓等東南亞地區，雖然到目前為止遭受恐攻的程度仍無法與歐洲或中東相提並論，但漸有更多跡象顯示，ISIS 等恐怖組織在東南亞的發展潛力已不容忽視，ISIS 甚至架設名為「alfatihin.com」的網站，以馬來西亞語吸引人們注意，並透過網路宣傳手段，鼓勵支持者效仿「孤狼式」戰術發動襲擊，凸顯未來東南亞地區特定社群人士遭「啟發」與「激進化」可能已大幅增加(BBC News, 2017B)。印尼反恐主管官員 Hamidin 亦指出，網路進步更加助漲恐怖組織活動，且使政府當局更難掌握與監控(BBC News, 2017C)。

歐盟安全情報機關研究認為，在國際反恐戰爭中，以軍事武力摧毀恐怖組織總部及殲滅首腦或領導階層，並不能代表真正勝利，反而將會增加外部對其支持與同情，使得國際恐攻威脅指數上升，如由 ISIS 潛回原生國家的「聖戰士」就極有可能與本土受激進化的恐佈分子結合，共同執行恐攻任務，使傳統恐怖攻擊轉變為網路恐怖活動的形式(Ec.Europa.Eu, 2016)。假使國際恐怖主義朝此趨勢方向發展，在恐怖分子四散逃逸的情況下，這些恐怖組織既需要化整為零躲避追緝，亦必須依靠極有限資源持續宣揚極端理念，並為日後再度發起恐怖攻擊進行準備，包括隱密聯繫、獲取資金、招募成員，或直接進行網路恐怖攻擊等，則網路恐怖活動勢將憑藉其特質而成為未來危害國際社會安全的主要隱憂，網路恐怖主義的力量也可能更為強大。其變化動向及對未來恐怖攻擊型態帶來的挑戰與影響包括：

(一) 駭客手段與傳統恐攻相結合：2014 年歐盟執行委員會(European Commission)「網路安全報告」即已提及，透過技術提升，恐怖組織已有部分能力藉由網路途徑攻擊歐洲各國的資訊、金融、水電、能源、交通等關鍵基礎設施(Cyber Security Report, 2014)在當前各國實體防護日漸嚴密，組織計畫性恐攻漸難執行的情況下，轉由虛擬途徑攻擊關鍵基礎設施，以達人員傷亡、經濟損失、引發社會秩序動盪等恐攻效果，仍將為網路恐怖主義的重要型式。

(二) 針對特定族群強化主張宣傳：在穆斯林與移民等社群於西方社會仍受歧視的背景下，即為極端主義提供絕佳的傳播土壤，且衍生的激進意識可能還會延續數代，由接受 ISIS 信念的西方國家本土暴力分子結合返國聖戰士共同發起恐攻行動的案例可以推算，恐怖組織將更會大力於虛擬世界針對關鍵受眾宣揚極端主張，以獲得所需支持。

(三) 針對一般社群渲染恐攻威脅：依歐盟安全情報機關情資指出，法國安全部門平均每日可偵破一起恐攻未遂案，其本土激進分子至少已達 1 萬 5 千人以上，且激進化期程急速縮短，顯示即與網路資訊煽動有關(Ec.Europa.Eu, 2016)，而中東持續動盪不安，持續滋養伊斯蘭宗教激進主義，將成為西方國家社會的長期威脅，未來相關恐怖組織勢將以此製造一般社群心理壓力，以達吸引支持者加入等相應目標。

(四) 鼓動「孤狼式」恐攻襲擾：自 2015 年起，咸認為最具殺傷力的恐怖組織 ISIS，不僅派遣「聖戰士」策劃及執行恐攻，亦積極透過網路平臺擴大宣傳、啟發及激進化效果，鼓動發起「孤狼式」玉石俱焚的恐怖攻擊，在新型網路恐怖主義著重啟發與激進化各地潛在支持者的情況下，本土原生，而非恐怖組織正式成員的「孤狼式」攻擊勢將成為未來恐攻的主要型態，且攻擊目標將大多為其熟悉的地理環境及範圍(林泰和，2015)。

(五) 執法查緝更加困難：網路及社群媒體均為恐怖組織用以宣揚訴求、組織行動、蒐集情報、號召攻擊、傳遞訊息、招募成員等，因其具有高度隱密性及管道多元性，在防範與查緝方面原本即有相當困難性，復以如啟發與激進化的過程，均可為個人空間等私密地點，較之以過去的反恐工作，面對新型網路恐怖主義勢將更難偵查預防。

相對於實務，學者並從理論觀點出發，認為國際網路安全情勢將因「安全困境」變得更為複雜，隨網路恐怖主義發展，又將使此困境難以擺脫。原因在於，無論是何種型態的網路攻擊者，對資訊系統可能造成的損害即已較防禦更為容易，新型態網路恐怖主義中的「激進化」及「啟發」又更難遏止，而各國在資訊戰領域實現合作的結構性限制，更反映此種「網路安全困境」的制約，一方面，網路攻擊幾乎可瞬間進行，具有投入成本極低，報酬率卻極高的特性；另一方面，網路攻擊也是發動「不對稱戰」的有力工具，弱勢行為者對資訊先進國家所造成的潛在破壞威脅是巨大的，但弱勢行為者卻沒有類似條件可形成

「互惠攻擊」。此外，「安全困境」並非處理網路安全問題的唯一障礙，如識別攻擊來源的能力、確認國際合作效力，以及定義威脅等問題也將更為難解，又如歐洲各國政府期望能在箝制言論自由與防堵恐怖主義間保持平衡，紛紛研討網路管制、介入與言論自由、大眾隱私權的分際，惟宣示加強網路管制與介入的做法，卻很可能只會將恐怖分子推向網路更難察覺的角落，平添管制的困難，因此，改進網路安全技術與澄清國際合作的安全政策，才是減低網路恐怖主義威脅最有希望的途徑。

二、社會建構論的因應對策

以當前的國際反恐態勢而言，完全消弭恐怖攻擊依然遙不可及，然而，未來避免網路恐怖主義效應擴散與減少其危害則是可行的，關鍵在於各國資訊安全機制能否與時俱進並且通力合作，而治本之道，終究還是要從瞭解網路恐怖主義本質著手，擬定完善防護對策，並消除易生宗教極端主義的環境，才能逐步瓦解恐怖主義根源。基於網路環境是遵循文化、思想、社會、宗教、政治與經濟所形塑的人為活動空間，透過社會建構論的分析，將更能貼近其問題，並研擬根本性的因應策略。

依社會建構論的觀點，新興網路恐怖主義行為者的主要目的，就是在藉由大幅損害國家與社會的利益以實現本身主張，威脅方式並不僅限於過去以駭客手法為主軸或藉資訊網路科技壯大、支持恐怖活動的範疇，還包括啟發與激化認知偏差受眾、顛覆國家與政府形象、激起復仇的「聖戰」信念等，面對這樣的變化，需要所有社會社群共同參與網路安全行動，消除容易造成誤解感知的社會環境，並強化對本身社會的信心，藉由建立利益與身分認同的結構性制度，形成網路安全機制中的規範及國際立法，才能消弭網路恐怖主義的危害。

社會建構論認為，行為者身分是從特定事件經社會化發展所形成的集體認同概念，其行動及反應來自於對環境看法的影響，對社會結構威脅的形成尤其如此(Ciolan, 2010)，以人際關係方式思考，考量行為者的身分、行為動機背景與互動過程，可做為因應新型網路恐怖主義的安全典範，應從幾個不同層面著手：

(一) 國際層次，建立以合作對抗威脅為導向的國際建制：2015 年歐盟「司

法與內政」委員會發表「里加宣言」，指出反恐工作必須加強因應恐怖主義、激進化、恐怖分子招募與資助等四大面向的國際合作(European, 2016)，均與網路恐怖主義有關，在此基礎上，更應納入國際組織、非政府組織，以形成國際建制，針對網路恐怖主義進行國際立法、建立共同標準、分享情報資訊等工作，更重要的是，形成網路世界的國際性文化與集體認知，以使國際網路社會成為有秩序的社會。

(二) 國家層次，融合各行為者共同維護網路安全：儘管對於網路治理存有加強控制與限制，講求「網路主權」的觀點，然亦有推動利益攸關各方形成共識，以治理網路的觀點(Ciolan, 2010)。是以國家應與民間社會、私營部門及技術專家共同合作，採取清晰靈活的網路安全政策，並提高監測能力與推動政府機構間的合作，制定完整的策略及機制，提高資訊安全標準，以應對網路恐怖主義的技術層面威脅。

(三) 社會層次，消弭恐懼與歧視的不安全感：社會建構論觀點認為，網路恐怖主義將對社會形成兩大恐懼，分別是對隨機且劇烈的暴力攻擊的恐懼，以及對資訊技術的恐懼，亦為資訊技術已經在某種程度取代人的地位，形成可能失控的威脅，只有消除對所處環境的焦慮及不確定感，才能形塑自我安全的信心。面對網路恐怖活動從低階到高階，從實體到心理的網路攻擊或宣傳效應、理念傳導，應加強民眾有關網路道德及安全使用網路的教育，並消除容易使個人激進化的社會環境，如改善貧窮、遏制歧視、提供教育與工作機會，促進善治、人權、民主、經濟繁榮、文化對話等(European, 2005)，使不同社群間得以進行長期整合，拔除激進化的著力點。

綜合而論，在實務上，應對網路恐怖主義發展的難題在於，儘管如美軍網路司令部已著手癱瘓 ISIS 透過網路散播、招募、傳遞指令的能力，但從 ISIS 仍可連續在西歐、中東各地發動恐怖攻擊的情況看來，ISIS 網路指揮與招募鏈幾乎可在遭截斷同時重新運作，因此，當恐攻已演化為組織個人化、地域分散化、時間無常化等「廉價高效」型態時，立法管制過濾社群媒體資訊的做法，已有相當必要。此外，未來設計反制措施以有效應對新型網路恐怖主義，必須將網路媒體視為打擊恐怖主義的合作對象而非阻礙，一方面對於網路媒體公司，應商討篩檢、刪除極端與煽動性言論或恐攻相關內容的因應策略，另一方面，則應發展高端先進的演算機制，以快速偵測恐攻言論及建立通報機制。通

報機制包含國際建制、各國政府與民間企業的三角合作機制，是國際社會未來反制新型網路恐怖主義，以及防止恐怖組織、恐怖分子藉網路串聯所需努力的重點方向，必須投注更多資源使其逐步完善，方能真正有效遏止新型網路恐怖主義的發展與蔓延。

伍、結論

本文首先回顧網路恐怖主義的起源。網路恐怖主義自 1990 年代出現後，早期著重在訊息傳遞、網路攻擊等技術型態活動，911 事件後，則因 Qaeda、Hamas 等恐怖組織遭受重大打擊，轉為借助網路成本低廉、相對安全，以及便捷、隱蔽等特性，而發展成用以宣揚理念、招攬徒眾、募集資金、散佈威嚇訊息等以攻心為主的網路恐怖主義。儘管學界對其定義仍未能有一致看法，然隨網路恐怖主義持續發展，不僅在於過去網路攻擊與造成附帶心理恐懼的層面，亦在於透過網路教育徒眾、意識啟發、「激進化」潛在支持者的「感召」層面，基於當前威脅形勢，本文重新定義網路恐怖主義的概念為：「恐怖組織為達成特定目的，以網際網路為工具及載體，所遂行的網路攻擊、理念宣傳或心理攻勢、人員或資源募集，以及與恐怖攻擊相關的訊息聯繫、啟發與激進化行動者的行為」。

其次，網路恐怖主義是依循政治、經濟、社會，而主要是宗教與文化因素形成的非傳統安全議題，故嘗試藉國際關係建構主義理論中的社會建構論，分析網路恐怖主義。依社會建構論的觀點，新興網路恐怖主義，主要就是藉損害國家與社會利益以實現本身主張，威脅形式係以啟發與激化認知偏差受眾、顛覆國家與政府形象、激起「聖戰」復仇信念等，需要所有社會社群共同參與網路安全行動，消除歧視的社會環境結構，並藉由建立利益與身分認同的結構性制度，形成網路安全機制中的規範及國際立法，力圖消弭網路恐怖主義的危害。

最後，本文以社會建構論的主張為基礎，研擬因應對策，應從國際、國家與社會層面著手。在國際層次上，須納入國際組織、非政府組織等國際社會及網路領域的共同行為者，建立以合作為導向的國際建制，並進行國際立法、建立共同標準、分享情報資訊，形成網路世界有秩序的國際性文化與集體認知；

在國家層次上，必須融合國家、民間社會、私營部門及技術專家等各行為者，共同制定策略及機制，以應對網路恐怖主義的技術層面威脅，維護資訊網路安全在社會層次上，則應著重於消弭恐懼與歧視的不安全感，從根本上消除網路恐怖主義激進化潛在分子的機會，才是治本之道。

若從恐怖組織觀點思考網路恐怖活動，日後其既需化整為零躲避追緝，亦必須依靠極有限資源持續宣揚極端理念，並為再度發起恐攻進行準備，而只要其以網路攻擊方式造成國際社會傷害的可能性存在，則各國就不敢掉以輕心；另外，網路恐怖活動乃為恐怖組織最廉價且有利的作戰方式，既以向特定族群受眾傳達經過選定的資訊，強化情感認同、理念支持，並鼓動對象加入組織，甚至接受號召「起義」，再以相關事件的渲染、證成其教義，形成心理攻勢的循環，如「啟發」與「激進化」即為這樣的過程，其實也是不同形式的宣傳戰與心理戰。依此，網路恐怖主義勢將憑藉其特質而成為未來國際社會安全秩序的威脅與挑戰，然長期而言，其未來是否將有其他形式的變化發展，又會對國際社會造成何種影響，值得學界持續關注。

參考文獻

(一)中文

方天賜、孫國祥(2007)。民族主義與恐怖主義。張亞中編，**國際關係總論**(207-208)。臺北：揚智出版社。

立法院(2017)。立法院第 9 屆第 3 會期外交及國防委員會第 14 次全體委員會議。**立法院網站**：http://www.ly.gov.tw/01_lyinfo/0109_meeting/meetingView.action?id=83991 。檢索日期：2017.06.16

林泰和(2011)。國際恐怖主義的資金流動。**問題與研究**。50：1，98-103。

林泰和(2015)。**恐怖主義研究：概念與理論**。臺北：五南出版社。

林泰和(2016)。近期歐洲恐怖主義發展之研析。**問題與研究**。55：4，113-127。

林泰和(2017)。歐洲反恐戰爭正要開打。**中時電子報**：http://www.chinatimes.com/newspapers/20170605000444-260109。檢索日期：2017.06.20。

秦亞青(2006)。**文化與國際社會：建構主義國際關係理論研究**。北京：世界知識。

程富陽(2012)。析論中東阿拉伯之春的衝擊與影響。**國防雜誌**。27：1，18-29。

(二)英文

Alexander E. Wendt(1987), The Agent-Structure Problem in International Relations Theory, http://www.jstor.org/stable/2706749. Accessed 3,October,2017.

Alexander E.Wendt(1992), Anarchy is what States Make of it: The Social Construction of Power Politics, http://www.jstor.org/stable/2706858. Accessed 3,October,2017.

Alexander E. Wendt(1999), ***Social Theory of International Politics***, Cambridge:CambridgeUniversity.

Anne Saita(2003). Dorothy Denning: Leading authority on cybercrime, information warfare, http://searchsecurity.techtarget.com/feature/Dorothy-Denning-Leading-authority-on-cybercrime-information-warfare. Accessed 2,April,2017.

Barry C. Collin(1996), The Future of Cyber-Terrorism: Where the Physical and Virtual Worlds Converge,***Proceedings of 11th Annual International Symposium on Criminal Justice Issues***, Chicago:The University of Illinois.

BBC News(2017A),WhatsApp must not be place for terrorists to hide,***BBC News***, http://www.bbc.com/news/uk-39396578. Accessed1,April,2017.

BBC News(2017B).Maute rebel group: A rising threat to Philippines, ***BBC News***,http://www.bbc.com/news/world-asia-40103602. Accessed31,July,2017.

BBC News(2017C).Indonesia has good anti-terror capability,***BBC News,***http://www.bbc.com/news/av/world-asia-35320359/indonesia-has-good-anti-terror-capability. Accessed31,July,2017.

Clay Wilson(2008). Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, https://fas.org/sgp/crs/terror/RL32114.pdf. Accessed 2,April,2017.

EastWestInstitute(2010),***Russia, the United States, and Cyber Diplomacy: Opening Door,*** New York: EastWest Institute.

Ec.Europa.Eu(2016), Protecting freedom and security of Europe and its citizens, http://ec.europa.eu/transparency/regdoc/rep/3/2016/EN/C-2016-8631-F1-EN-ANNEX-17-PART-1.PDF. Accessed 8,April,2017.

European(2005),The European Union Counter-Terrorism Strategy: Prevent、Protect、Pursue、Respond, http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2014469%202005%20REV%204.Accessed 8,April,2017.

European(2016). European Union Terrorism Situation and Trend Report (TE-SAT) 2016,https://www.europol.europa.eu/activities-services/main-reports/european-union-terrorism-situation-and-trend-report-te-sat-2016.Accessed 4,April,2017.

Finnemore, Martha(1996),Constructing Norms of Humanitarian Intervention, Peter J. Katzensteined, ***The Culture of National Security: Norms and Identity in World Politics***,New York: Columbia University.

Gabi Siboni(2014),The Threat of Terrorist Organizations in Cyberspace,***Cyberspace and National Security***, Haim Levanon St: Institute for National Security Studies.

Gil Ariely(2008),Knowledge Management, Terrorism, and Cyber Terrorism, Ann Shaver & Heidi Hormel eds, ***Cyber Warfare and Cyber Terrorism,*** Hershey: Information Science Reference.

HadleyJ.Stephen (2017). Toward a New Strategy: Building 'Situations of Strength',***A National Security Strategy for the United States***, U.S. Washington: Brookings Institution.

HomaKhaleeli(2014), Domestic terrorism: Isis housewives told how to prepare battle snacks, ***The Guardian***, 2014(5), http://www.theguardian.com/world/shortcuts/2014/nov/05/isis-housewives-told-to-prepare-battle-snacks. Accessed 16, July, 2017.

Ionela Maria Ciolan(2010),***Defining Cybersecurity as The Security Issue of The Twenty First Century: A Constructivist Approach***, Romania Bucharest:National University of Political and Administrative Sciences.

J.M. Berger(2015). How terrorists recruit online, https://www.brookings.edu/blog/markaz/2015/11/09/how-terrorists-recruit-online-and-how-to-stop-it/. Accessed5, April, 2017.

J.M. Berger(2017), How ISIS Games Twitter,***The Atlantic***, 18(3), http://www.theatlantic.com/international/archive/2017/06/isis-iraq-twitter-social-media-strategy/372856/. Accessed 16, July, 2017.

James A. Lewis(2012), Thresholds for Cyberwar, http://csis.org/files/publication/101001_ieee_insert.pdf.Accessed 20, June, 2017.

James A. Lewis(2014), In Defense of Stuxnet,***Cyberspace and National Security***, HaimLevanon St: Institute for National Security Studies.

JenniferMitzen(2006), Anchoring Europe's civilizing identity: abits, capabilitiesand

ontological security, ***Journal of European Public Policy***, 13(2),pp.43-61.

Johan Eriksson&GiampieroGiacomello(2004), ***International RelationsTheory and Security in the Digital Age***, Montreal: International Studies AssociationConvention.

JohnBaylis, Steve Smith and Patricia Owens(2011), ***The Globalization ofWorld Politics***, New York: OxfordUniversity Press.

Kratochwil, Freidrich V.(1991), ***Rules, Norms, and Decisions ─ On The Conditions of Practical and Legal Reasoning in International Relations and Domestic Affairs***, Cambridge: Cambridge University.

Mark M. Pollitt(1997),A Cyberterrorism Fact or Fancy?, ***Proceedings of The 20th National Information System Security Conference***, Czech Kojetínská:Czech Space Research Center.

Mark M. Pollitt(2011). What is Cyber-terrorism?, http://www.inforwar.com/mil_c4i/stark/cyber_Terrorism.html.Accessed2, April, 2017.

MitkoBogdanoski&DragePetreski(2013), Cyberterrorism: globalsecurity threat, **Contemporary Macedonian Defence**, 13(24), pp.54-72.

Mohammed Hafez & Creighton Mullins(2015),The Radicalization Puzzle: A Theoretical Synthesis of Empirical Approaches to Homegrown Extremism,***Studies in Conflict & Terrorism***, 38(11), pp.96-110.

MooreTyler(2016),Christmas terrorist plot foiled in Australia, ISIS-inspired suspects arrested, https://www.rt.com/news/371333-australia-christmas-terrorist-plot/. Accessed 5, April, 2017.

Musharbash(2004). US-Firmen-Website für Qaida-Botschaftgehackt, http://www.spiegel.de/politik/ausland/0,1518,304473,00.html. Accessed4, April, 2017.

NicholasOnuf(1989), ***World of Our Making: Rules and Rule in Social Theory and International Relations***, Columbia, SC: University of South Carolina.

Nikos Passas(2007). Terrorism financing Mechanisms and Policy Dilemmas, Jeanne K. Giraldo& Harold A. Trinkunaseds, ***Terrorism financing and State***

Responses–A Comparative Perspective, Stanford: Stanford University Press.

Paul Cornish, David Livingstone and Dave Clemente(2010), ***On CyberWarfare***, London: Chatham House.

Peter Nesser(2014),Toward an Increasingly Heterogeneous Threat: A Chronology of Jihadist Terrorism in Europe,***Studies in Conflict & Terrorism***, 37(5), pp.150~166.

Ronald L. Dick(2002). Testimony of Cyberterrorism, https://archives.fbi.gov/archives/news/testimony/cyber-terrorism-and-critical-infrastructure-Protection. Accessed 4, April, 2017.

Rukmini Callimachi(2015), Paying Ransoms, Europe Bankrolls Qaeda Terror, New York Times, http://www.nytimes.com/2014/07/30/world/africa/ransoming-citizens-qaedas_r=1. Accessed 20, September, 2017.

Sarah Gordon(2002),***Cyberterrorism?***, U.S. Cupertino: Symantec Inc.

United Nations Security Council (2004), Adopted by the Security Council at its 5053rd meeting, on 8 October 2004, http://daccess-ods.un.org/access.nsf/Get?Open&DS=S/RES/1566%20(2004)&Lang=E&Area=UNDOC. Accessed20, June, 2017.