《安全與情報研究》 第三卷第一期 中華民國 109 年 1 月
Security and Intelligence Studies, Vol. 3, No. 1. January 2020

《資恐防制法》與打擊金融恐怖主義的執法安全合作研究

黃秋龍

國防大學政治作戰學院政治系兼任副教授

摘 要

資助恐怖主義犯罪，固然有《洗錢防制法》、《資恐防制法》等相關法令可資適用。然而，資助恐怖主義犯罪，不僅侷限於對有形實體法益的加害、恐嚇、脅迫或財物財產上利益移轉；現實上，資恐犯罪藉由網路金融體系，已衍生為金融恐怖主義，即使非恐怖暴力襲擊的直接目標，也難免於恐怖金融犯罪危害，甚至使得恐怖金融活動在全球轉移或獲得非法利益。而今，金融恐怖主義不僅成為新興的恐怖主義運動方向與趨勢；而且，恐怖犯罪動機、行為樣態與結果，已呈現離散化，彼此因果關係模糊或隱匿，甚至出現向外跨境擴溢，卻無被害者之現象。本文研究的問題意識，即為檢視網路金融犯罪在資恐與金融恐怖主義之間的關聯性。進而，論述研究架構包括：首先，描述網路因素在金融與恐怖犯罪的相互作用現象其次，從資恐複合金融恐怖主義的情勢，說明資恐防制議題，為何已不再侷限於刑法或犯罪學領域，而是指涉到包括執法安全合作、全球治理與安全戰略等政策應用層面；第三，論證資恐防制做為打擊金融恐怖主義執法安全合作之前提，舉述《資恐防制法》主管機關法務部依調查局提報或依職權，指定制裁名單，並以調查局與美國、歐洲刑警組織等 31 個國家共同偵破「雪崩」(Avalanche) 殭屍網路犯罪案，解釋網路金融犯罪在資恐與金融恐怖主義之間，所存在的關聯性。從而，

確證資恐防制的執法合作及其法意實踐的必由之途。

關鍵詞：《資恐防制法》、金融恐怖主義、「雪崩」殭屍網路犯罪、執法安全合作

A Study on Terrorism Financing Prevention Act and Law Enforcement in the Fighting against Terrorism Financing

Huang, Chiu-lung

Adjunct Associate Professor, Department of Political Science, The Political Warfare Cadres Academy, National Defense University, Taiwan, Republic of China

Abstract

Although the Money Laundering Control Act and the Terrorism Financing Prevention Act can be applied for fighting terrorism-financing crime, this sort of crime is not only the violation of the substantial legal benefit or the transfer of property but also newly-emerged financial terrorism, which is conducted via the internet financial system. Those entities, which the terrorists do not target directly, can not prevent themselves from the damages and dangers caused by the financial terrorism, and as a result, the terrorists can transfer their properties and earn the illegal interest. Nowadays, financial terrorism has been the new tendency and trends of the terrorist; meanwhile, their motives, behaviors, and consequences have been decentralized. The causality is vague and the relationship between the criminals and victims may be transnational, or even victimless. Examining the correlation between financial terrorism and e-finance crimes is the question of this research. Further, the

framework is as below: describing the interaction between the internet, the finance, and terrorism crime is the first part. Secondly, this research will elaborate on why the fighting against terrorism financing is far beyond the regions of the criminal law and criminology but is involved in the cooperation of law enforcement, global governance, and security strategy. Thirdly, this research will argue the fighting against terrorism financing as the premise of countering financial terrorism. The investigation of the "Avalanche" botnet is a good example of this argument. The Ministry of Justice, the authority of the Terrorism Financing Prevention Act, designates the sanction list according to the report of the Investigation Bureau (MJIB), and cooperates with other 31 countries, inclusive of the United States and the European Police Office, to solve the case. This example not only shows the relation created by the e-finance between financial terrorism and terrorism financing but also manifests the necessary legal praxis approach from fighting terrorism financing by law enforcement cooperation.

Keywords: Terrorism Financing Prevention Act, financial terrorism, "Avalanche" botnet cybercrime, law enforcement cooperation

壹、前言

由於資助恐怖主義犯罪，經常係實體與網路虛擬空間的複合型犯罪，不僅對生命、財產、心理造成危害，也會導致飛安與關鍵基礎設施遭受恐怖襲擊；更進一步，網路空間有利於犯罪預謀訊息傳遞、集資募款、建制網絡、甄補組訓人員與蒐集資訊，並有利於隱密行動、提高效能，甚至進行恐怖宣傳、心理戰。質言之，資助恐怖主義犯罪所指涉的範疇，已不再侷限於刑法或犯罪學領域，而是指涉到危害國家利益，以及涉及跨部門、多領域的執法安全合作範疇，其政策應用包括司法互助、全球治理與安全戰略等國家利益表現形式。本文先對資助恐怖主義犯罪新興趨勢進行描述，進而提出其與安全議題相互複合之因素，期望能藉此提出新的研究範疇，做為資恐防制與執法安全合作的共同前提。

貳、問題範疇與研究概念架構

一、問題範疇

當前恐怖主義衍生成同時具有暴力危害、構成心理威脅，甚至侵害跨境管轄的抽象主權與實體法益之現象，亦即對於恐怖犯罪之理解，不能僅只侷限於暴力 (violence) 與實體層次，而且需要更進一步理解其犯罪動力，包括為何其行動能離散化運作；相對的，有些部分又組織性強度，甚至產生跨境威脅的高風險危害。概括而言，恐怖犯罪可視為犯罪型暴戾 (criminal insurgency)，不僅足以產生跨境影響力，甚至在全球擴張其非法利益。[1]

[1] Michael L. Burgoyne, "The Effectiveness of Counterinsurgency Principles

尤其，後 911 恐怖襲擊事件以來的恐怖危害，更讓執法單位意識到，情報執法安全在全境與國際層次的合作，已對執法優先順序與任務執行上，造成激變效應 (cataclysmic effect)，必須就恐怖主義藉網路空間與金融體系的新興危害，從地緣政治與執法合作戰略視角，在觀念與實踐上有所激變。因為，此效應反應恐怖危害之特性，即使非恐怖暴力襲擊的直接目標，都無法免於恐怖分子透過金融犯罪，在全球無差別的攻堅目標甚至獲得非法利益。從而，識者提出呼籲，應對金融恐怖主義危害，除了既有的防制洗錢、組建任務小組或特別單位之執法安全合作模式之外，也需要進一步瞭解有資助恐怖主義發展之情事。[2]

值得注意的是，「伊拉克與黎凡特伊斯蘭國」 (The Islamic State of Iraq and the Levant, ISIL or ISIS ；簡稱『伊斯蘭國』) 擴溢的特殊性，除了曾與蓋達組織 (Al-Qaeda) 形成相互爭勝犄角態勢，其危害樣態，更從傳統的爆炸、武器濫用與人員殺害之外，還包括古文物、器官販運，殘害人權、侵犯國際法、綁架、無差別殺害平民、大屠殺、法外處決、異族強制遷徙、性脅迫、童兵訓練。[3] 固然，「伊斯蘭國」目前走向式微，然而各類直、間接資助恐怖主義之危害，更易於產生交互影響。即使，蓋達組織在美國發動

against Criminal Insurgency: the Right Tool for the Job," *Small Wars Journal*, (February 11, 2012), pp. 2-3.

2 Nick Ridely, "Analyse This (and That): a Consideration of the International Role of Analysis," in Steven David Brown ed., *Combating International Crime: the Longer Arm of the Law* (London and New York: Routledge-Cavendish, 2008), pp. 212-213.

3 United States Department of State, *The Global Coalition to Defeat ISIL,* September 10, 2014, <http://www.state.gov/s/seci/index.htm> (2018 年 11 月 23 日查詢) .

反恐怖主義行動以來，曾因「伊斯蘭國」崛起陰影與轉向式微。而今，蓋達組織重整再次悄悄崛起，資助恐怖主義之危害亦隨之持續上升。

具體例證，例如遜尼派組織「沙姆解放組織」(Hayat Tahrir al-Sham) 已在 2017 年 8 月控制敘利亞北部城市伊德利布 (Idlib)，其實就是「重新包裝」過的蓋達組織。甚至，蓋達組織亦在布局成為比「伊斯蘭國」更溫和穩健的組織，以期捲土重來。「沙姆解放組織」加強控制伊德利布省多數地方，主要係趁政府治理匱乏與「伊斯蘭國」崛起之陰影，消滅或吸收多個暴亂組織，並以擅常網路經營的「伊斯蘭國」為榜樣，將其宣傳方式以碎片化意識形態傳播。「沙姆解放組織」可能聚集對「伊斯蘭國」最極端手段喪失興趣的追隨者，而成為後起之最重大威脅。然而，「沙姆解放組織」與「伊斯蘭國」最主要矛盾形式，表現在該組織採取「控制型實用主義」(controlled pragmatism)，來為其政權統治合理化。不僅用反政府勢力與蓋達組織意識形態純正性之爭，從網路空間進而轉向實用主義路線，藉與土耳其等國家關係正常化，征服周邊暴亂組織，又可利用對伊朗保持開放，進而牽制土耳其。同時，將最極端恐怖手段，改為低強度的綁架、暗殺或襲擊行動；而且，也讓國際人道救援組織進入控制區賑災。[4] 質言之，各類直、間接資助恐怖主義之危害，將易於產生交互影響，其儼然係複合型犯罪，既對實體與網路虛擬空間生活利益構成暴戾危

[4] Patrick Hoover and Omar Kebbe, "After Raqqa: the Next Jihadist Stronghold in Syria," *Terrorism Monitor*, Volume 15, Issue 18, September 22, 2017, <https://jamestown.org/program/after-raqqa-the-next-jihadist-stronghold-in-syria/>(2018 年 11 月 23 日查詢).

害，同時也伴隨政治、經濟與社會組成要素的衝突。

二、概念界定

暴戾 / 叛亂 (insurgency) 與暴力 (violence) 既存在差異又相互聯繫，暴力樣態主要是對生理或心理上造成的危害，有一定的主客體、加害與被害之因果關係。相對的，暴力固然是暴戾的一種表現形式。然而，美國國防部對暴戾界定為：「一種組織型運動藉由使用顛覆與武裝衝突，企圖推翻合法政府之行動。」事實上，暴戾的特殊屬性在於其持續與跨境，以及政治、經濟與社會面向的衝突。它不僅在危害一般市民與關鍵基礎設施，更在於引發政治、經濟與社會組成要素的衝突效應。從而，其所使用之暴力手段，旨在製造顛覆、社會崩潰以及政治運動 (如族群衝突、反政府行動、國家認同分裂)，引發國家或區域之政治社會秩序變動。因此，暴戾危害乃係戰爭與政治效應的相互聯繫又相互伴隨。應處暴戾危害，可視國家安全的主要表現利益。[5]

如此看來，當前資助恐怖主義犯罪，同時具有暴力危害、構成心理威脅，甚至侵害跨境管轄的主權抽象與實體法益之現象，其製造顛覆、社會崩潰以及政治運動效應，遠比其暴力手段來得重要。亦即對於恐怖犯罪之理解，不能僅只侷限於暴力與實體層次，而且需要更進一步理解其犯罪動力，包括為何其行動能離散化運作；相對的，有些部分又組織性強，甚至產生跨境威脅的高風險危害。概括而言，恐怖犯罪可視為犯罪型暴戾，其暴力手段

[5] Scott Moore, "The Basics of Counterinsurgency," *Small War Journal,* 2007, pp. 2-3, <http://smallwarsjournal.com/documents/moorecoinpaper.pdf> (2018 年 11 月 23 日查詢).

所侵害者，不僅只於可明確化的國家、社會、個人法益範疇；相對的，它還直、間接的對實體與網路虛擬空間生活利益構成暴戾危害，以及引發政治、經濟與社會組成要素衝突的複合型犯罪。

三、研究概念架構

固然，研究資助恐怖主義犯罪，可以從資本流動、犯罪過程與恐怖金融活動等三項範圍，歸納分析彼此交互或共同重疊之情形，來做為研究概念架構。[6] 然而，金融恐怖主義更關切的研究假定是，即使非恐怖暴力襲擊的直接目標，為何仍無法免於恐怖金融犯罪，在全球轉移或獲得非法利益。從而，本文也以此做為問題意識。換言之，欲瞭解金融恐怖主義對吾人之危害，其研究範疇應該從資助恐怖主義犯罪，為何對實體與網路虛擬空間構成複合型危害為出發點，進而分析恐怖主義危害擴溢之動力，及其與恐怖金融犯罪可能的關聯性。

因此，本文研究概念架構，包括從問題意識檢視所指涉之研究範疇，進而論證防制金融恐怖主義與執法安全合作的合理性。作者以為，重塑宏觀與微觀層面相互影響的犯罪學研究方法，也就是得重新檢視犯罪的類型、動力與情勢。[7] 因此，本文以資恐防制出發，並與執法安全應用相互呼應，研究概念架構 (conceptual framework) 包括：

---

[6] Frank G. Madsen, *Transnational Organized Crime*, (New York: Routledge Global Institutions, 2009), p. 104.

[7] Jay S. Albanese, "Choosing a Micro or Macro Perspective for Understanding Organized Crime: the Contributions of Ernesto Savona," in S. Caneppele, F. Calderoni eds., *Organized Crime, Corruption and Crime Prevention* (Switzerland: Springer International Publishing, 2014), p. 265.

（一）描述網路因素在金融與恐怖犯罪的相互作用現象；

（二）從資恐複合金融恐怖主義的情勢，說明資恐防制議題，為何已不再侷限於刑法或犯罪學領域，而是指涉到科際整合範疇，其政策應用包括司法互助、全球治理與安全戰略等層面；

（三）論證資恐防制做為打擊金融恐怖主義執法安全合作之前提，舉述《資恐防制法》主管機關法務部依調查局提報或依職權，指定制裁名單，並以調查局與美國、歐洲刑警組織等 31 個國家共同偵破「雪崩」(Avalanche) 殭屍網路犯罪案，解釋網路金融犯罪在資恐與金融恐怖主義之間，所存在的關聯性。從而，確證資恐防制的執法安全合作及其法意實踐的必由之途。

參、網路因素在金融與恐怖犯罪的相互作用現象

一、使安全危害產生加乘效應

隨著全球化之進程發展，令人感到弔詭的是，犯罪行為者顯然找到利用網路空間，展開新的攻擊或違法的獲利手段，並提高其行動與隱匿效果。如駭客網路襲擊經常伴隨著偷竊和傳播病毒行為，許多駭客的活動已開始從尋求刺激、炫耀技能的惡作劇，演變為利用網路技術從事經濟犯罪或政治活動。以往人們對網路犯罪都具有刻板印象，以為就是應用資訊技術對電腦、網路、資料庫進行非法襲擊，藉以發揮恐嚇、逼迫政府或社會，進而實現其政治企圖或社會目的。事實上，網路犯罪已危害傳統與非傳統安全領域，並產生複合效應。襲擊對象不僅限於軍事或政治之傳統安全標的，也可以針對金融、交通、電力、醫療衛生等非傳統

安全目標。而且，所應用之手段既有組織能力，也經常有特定目的與方向，甚至更為離散化，在遠端採取轉輾襲擊行動。因此，網路因素可視為新型態複合型犯罪要件，使得新興安全威脅產生加乘效應，其表現形式諸如：

（一）心理戰：散布、放大、誇張恐懼與無助感；凝聚恐怖分子主從關係；分化社會對政府之信心、破壞市場金融秩序。

（二）公共宣傳戰：吸引各界媒體注意，應用選擇性報導手法，採哀兵或自由訴求以搏取同情；加密通聯規避檢查；侮辱、妖魔化對手，暴力自我合理化。

（三）資料探勘 (data mining)：對襲擊目標（如交通設施、核電廠、公共建築、機場、港口），甚至反恐措施、病疫防制、金融運作等體系，預先蒐集大量相關資料，加以分類、排序、運算，以得到特定屬性之資訊。[8]

二、出現複合型犯罪的新興情勢

實體與網路複合型犯罪，除既有之組織特性與利用新興科技之外，其行為樣態又與電腦犯罪具有交互特性，甚至衍生到通訊、影音、智慧產權非實體空間，以及國家、關鍵基礎設施，而成為非以實體為侵害工具或客體的虛擬犯罪 (virtual crime)，抑或複合其他違法行為（如散播使用毒品訊息、毒品販運、詐欺、勒索、洗錢、妨害名譽、瀆職），從而超越經濟犯罪領域。首先，實體與網路犯罪之所以相複合，表明網路犯罪未必是組織犯罪，而是

[8] Gabriel Weimann, "New Terrorism and New Media," *Research Series*, Vol. 2, May 12, 2014, p. 4, <https://www.wilsoncenter.org/sites/default/files/new_terrorism_v3_1.pdf> (2018 年 11 月 23 日查詢).

能透過群組與個別交替之途徑，利用人性弱點，進行社會、經濟關係之連結與交易技術，藉由無線、遠端之網路空間特性，遂行區隔形式的犯罪。[9] 其次，新興科技與網路空間的散布迅速與隱密性，乃更容易衍生出與其相適應的模仿或自（誘）發型犯罪。例如操縱金融市場 (manipulation of financial markets)、產業間諜 (industrial espionage)、網路恐怖主義 (cyberterrorism)、涉毒恐怖主義 (narcoterrorism)，即係有組織與非組織型犯罪、侵害經濟與非經濟法益相互交替之複合型犯罪。

複合型犯罪將令人改變對跨境有組織犯罪之傳統認識，亦即過去以為該犯罪具有制式階層組織、自鄙為社會邊陲群體，人們通常都將之視為公部門執法問題，在防制犯罪上缺乏社會參與空間與效能感。而今，複合型犯罪不僅會應用網路空間與科技改變組織模式，且自視為上層社經人士足以對政治、法律、經濟政策產生影響，進而經營慈善事業、傳播媒體以左右視聽。[10] 甚至滲透合法企業，從事大規模武器與戰略資源買賣。[11] 質言之，複合型犯罪的新興情勢，不僅伴隨低罪惡感、造成無被害者現象，甚至已非單一政府、部門所能充分應對，抑或只做為洗錢防制、反毒、移民等個別議題所能包括。相對的，已必須對新興複合型犯

[9] Rob McCusker, "Transnational Organized Cyber Crime: Distinguishing Threat from Reality," *Crime, Law and Social Change*, Vol. 46, No. 4-5 (December 2006), pp. 258-262.

[10] Moisés Naím, "Mafia State: Organized Crime Take Office," *Foreign Affairs*, Vol. 91, No. 3 (May/June 2012), p. 109.

[11] Jeanne Giraldo and Harold Trinkunas, "Transnational Crime," in Alan Collins eds. *Contemporary Security Studies* (Oxford: Oxford University Press, 2010), p. 431.

罪，出於共同安全意識，才有助於跨部門、多領域的共同合作防制危害擴溢。

肆、從網路治理因素探索資恐防制應用途徑

資恐犯罪藉由網路金融體系，已衍生為金融恐怖主義。然而，防制具有實體與網路複合型犯罪特性的金融恐怖主義，向來面臨著法制程序與網路治理手段之難題，公、私部門合作也存在著制度性或組織障礙。然而，應用不同學科與途徑，不僅建構出可行的務實經驗與政策理論倡議觀點，而且在實際的應對行動中，機關（構）內的跨部門合作，或不同政府機關的府際與非政府組織間的合作，都不斷探索出可供借鏡的良善治理經驗。從而，吾人有必要認識犯罪型暴戾危害可能再升高之情勢。[12] 進而，洞察網路治理因素，為何成為資恐犯罪與金融恐怖主義的中介變數，才有助於為執法安全合作建構共同前提和環境。

一、從法律適用歧異認識務實合作途徑

網路因素在實體與虛擬犯罪世界中相互影響、穿透的特性，除了會使得各方對法益保護出現法律適用歧異之外，而電訊監察與線上證據保全等執法合作程序，也會對基本人權、執法合作意願造成衝擊。[13] 尤其數位證據具有非實體的特性，雖然施以線上

[12] Paul Staniland, "Wither ISIS? Insights from Insurgent Response to Decline," *The Washington Quarterly,* Vol. 40, Issue 3 (Fall 2017), p. 35.

[13] Fausto Pocar, "New Challenges for International Rules against Cyber-crime," *European Journal on Criminal Policy and Research*, Vol.10, No. 1 (March, 2004), pp. 32-33.

查緝行動有助於證據保全，但卻會伴隨侵害個人財產、隱私權、通訊自由甚至引人入罪等疑慮之外，在實務上也會面臨證據蒐集、保存、分析與再輸出呈堂供證等等難題。因為，原始數位證據可被複製甚至改變，其真確性在分析與供證時，將會面臨許多質疑，例如病毒感染、無知狀態下的被存取的宣稱，都會影響原始數位證據之真確性以及當事人之意願與權益，從而造成訴訟過程難以預測的變易。另一方面，原供國防與情報部門應用的加密技術 (cryptography)，已能輕易的運用在資訊偽裝 (steganography) 技術上，也將使得原始數位證據真確性變易。資訊偽裝技術可將訊息 (message) 本身的存在性 (existence) 隱藏起來，讓人無從意識它的存在，甚至偽裝、虛擬成他人，導致數位證據之主體與真確性被模糊化甚至受到擅改、顛覆。[14] 類此盜用身分 (aggravated identity theft/ fraud) 之手法，即係網路犯罪不斷利用新興技術，發展出與網路空間相適應的具體案例。[15]

既然，各界在法律適用上還存在歧異，而且跨境 (域) 執法合作並不能改變其位階仍附屬於內國法化的現實，但為顧及彼此未來執法合作意願與舉證能力，必須有跨越傳統領域侷限的另類思考。例如，視個案採取「有效、比例與勸戒」(effective, proportionate and dissuasive) 權宜性制裁，或對侵害者課予相對社

[14] Peter Grabosky, "Requirements of Prosecution Services to Deal with Cyber Crime," *Crime, Law and Social Change*, Vol. 47, No. 4-5 (June 2007), pp. 211-212 and 219.

[15] Michael Levi, "White-collar, Organised and Cyber Crimes in the Media: Some Contrasts and Similarities," *Crime, Law and Social Change*, Vol. 49, No. 5 (June 2008), p. 371.

會與企業責任，甚至處以行政罰鍰。雖然，防制網路犯罪在司法管轄、執法合作等層面難題依舊，但仍有務實的合作途徑，在制度未及完備前，顯然更需要在政策與社會領域上積極倡議，透過更多非傳統領域的力量和參與，將有助於制度之建立與提升防制成效。所以，應用締約方對罪犯或引渡（該犯），若不引渡則就地起訴（該犯）的「或引渡或起訴原則」(aut dedre aut judicare)，將有助於跨越傳統法制之侷限與難題。因為，網路犯罪侵害之法益畢竟與國際戰犯、重刑犯（航空劫機、恐怖分子等）有所區隔，而此原則可以彈性調整網路犯罪審理的方式，不僅可以發揮政策與法律、視聽輿論與制裁效果區隔之綜合效應，也有助於提高網路犯罪侵害者受審意願與受害者救濟之實效；甚至，有利於保全線上證據，以及後續的情報支援合作。[16]

二、法制程序使應對機制產生侷限

就傳統、單一的司法管轄權實現觀點，固然可以對屬地型網路犯罪 (local cybercrime) 具有管轄權的合法宣告、進行裁判及有效執行。然而，非屬地型網路犯罪的行為主、客體與結果，經常會跨越傳統、單一的司法管轄權範圍，而產生數國牽連管轄的問題。同時，此類跨境網路犯罪 (transnational cybercrime) 對於傳統管轄權的對象與空間概念，也產生明顯的變易甚至流動。例如，相較於傳統犯罪行為態樣，跨境網路犯罪行為主、客體之間，未必是處於真實世界 (real-world) 空間中。網路空間之便捷與虛擬，固然有利於侵害者身分與犯罪行為之隱匿，而且其犯罪行為與真

[16] Fausto Pocar, "New Challenges for International Rules against Cyber-crime," pp. 34-35.

實世界有一定差異，但這種虛擬犯罪，是否屬於犯罪行為確實存有爭議；甚至無罪推定原則 (presumption of innocence) 能否有效防制網路犯罪也有待商榷。[17] 儘管爭議仍在，但是有關未經合法授權的電腦存取、截取電腦通訊技術、資料毀損或重製，與阻礙或干擾電腦合法使用等行為，則是一般實體法所普遍禁止者。實際上，數位技術型的虛擬犯罪，適用傳統刑法也有一定的普遍性與彈性。例如，傳統的竊盜罪雖以實體與佔有為其構成要件，然而數位技術型的竊盜行為，除了可能與文本 (text)、影像傳輸、影音、多元媒體 (multimedia) 複製等虛擬行為結合之外，它衍生在竊取商業機密上，兩者都同樣是屬於非實體侵害的虛擬犯罪。其適用傳統的竊盜罪，應該具有相當彈性。至於，對兒童或被描繪為兒童的人，應用數位科技從事影音圖像等色情描繪之兒童色情 (child pornography) 犯罪行為，在國際上適用刑法處罰則具有相當普遍性，甚至是屬於刑罰重罪。[18]

可見，網路因素反映出新的治理概念，不僅指涉犯罪構成要件與法律適用等跨法域問題，也涉及一個網路犯罪同時涉及數方（或部分）具有管轄權的跨境管轄權衝突難題。可行的應對經驗是成立跨境委員會，採取平等參與，就行為主客體籍別、法益侵害程度與拘提、搜索、扣押等強制處分作為，相互協商管轄優先順位。然而，值得注意的是，其中可能同時伴隨潛在的正負面效應。諸如，取得非第一順位管轄權者，通常後續合作意願都偏低；

[17] Susan W. Brenner, “Cybercrime Jurisdiction,” *Crime, Law and Social Change*, Vol. 46, No. 4-5 (December 2006), pp. 190-193.

[18] Peter Grabosky, “Requirements of Prosecution Services to Deal with Cyber Crime,” p. 209.

協商管轄也會造成救濟效果過於離散，跨境求償可能對受害者造成二度傷害；偵查、拘提司法互助所投入之資源，未必能與期望程度、權益保護救濟取得平衡。而以受害人數與金錢做為管轄優先順位之常用協商標準，當遇上需另行考量非經濟因素時（如涉及間諜行為、攻擊關鍵基礎建設與傳播媒體、教育設施等），則會讓應對網路犯罪之效果產生易變。再者，各方對網路犯罪行為之適用法律也未必能取得一致，經常導致審判、制裁、救濟效果不相對稱，自然會影響追訴效果。[19]

如此看來，共同合作打擊網路犯罪即使還存在著不確定性，其實也就是傳統訴訟程序，能否應對新科技環境衝擊之能力問題，或者做為公、私部門如何構想出新的應對方法之考驗。在可行的經驗中，包括研發更有效的資料保護技術；針對高科技相關犯罪，發展進而實現情報資料庫與可靠的資料登錄系統。例如，英國設有國家高科技犯罪防制小組 (British National Hi-Tech Crime Unit)，歐盟也在 2003 年 11 月 14 日為警察與司法部門在證據保全上，啟動合作架構決定 (framework decision)，亦為跨域資恐防制合作創造條件。[20] 由於，公、私部門合作應對網路犯罪，將在電腦軟、硬體的生產與商業利益以及防制政策上獲得實惠，使原來不確定性問題與公、私部門組織性障礙以及社會階層、地理疆界，得以跨越甚至創新價值。[21]

---

[19] Susan W. Brenner, " Cybercrime Jurisdiction," pp. 197-205

[20] "Cybercrime," *European Commission*, November 2018, <https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime_en > (2018 年 11 月 23 日查詢).

[21] Rafael Wittek, "Governance from a Sociological Perspective," in Dorothea

伍、資恐防制的制度創新與應用

為防制涉及實體與網路空間的資恐複合型犯罪，顯然需要進一步檢視公部門傳統合作模式的問題範疇。即使再先進的國家，或具有高度動員能量的政府機關與社會部門，也許已具備整合的制度與能力 (capability)，但還涉及如何使各種不同能力者，發揮彼此執法安全合作的職能空間 (capacity)。

一、資恐防制成為防制金融恐怖主義執法合作之前提

近年來，國際社會有鑑於恐怖主義對於各國構成極大威脅，防制洗錢金融行動工作組織 (Financial Action Task Force, FATF)，曾發布防制洗錢及打擊資助恐怖主義與武器擴散「 四十項建議」(Forty Recommendations)，以做為各國遵循之依據。然而，我國雖非 FATF 會員，惟自 2006 年起，即以「亞太洗錢防制組織」(The Asia/Pacific Group on Money Laundering, APG) 會員身分參與 FATF 會議。[22] 在國際社會不願見跨境 (域) 合作防制恐怖犯罪出

Jansen ed., *New Forms of Governance in Research Organizations: Approaches, Interfaces and Integration* (Dordrecht: Springer, 2007), pp. 75-78.

[22] 「防制洗錢金融行動小組」(Financial Action Task Force on Money Laundering, FATF) 成立於 1989 年，總部設於法國巴黎，現有 37 個會員，旨在打擊國際洗錢犯罪，設立相關規範與策略。該組織所制訂之「四十項建議」(Forty Recommendations) 及「關於恐怖主義財源之九點特別建議」(Nine Special Recommendations on Terrorists Financing) 為國際反洗錢工作之準則。「亞太洗錢防制組織」(The Asia/Pacific Group on Money Laundering, APG) 成立於 1997 年，秘書處設於澳洲，現有 41 個會員。旨在有效執行及強化國際打擊洗錢犯罪及資助恐怖分子之國際標準。我國為創始會員之一，2008 年至 2010 年擔任政策指導工作

現漏洞的前提下，我國參與 FATF 會議的務實模式，不僅為我國實踐跨境 (域) 執法安全合作創新職能空間，也更進一步彰顯我國做為國際良善夥伴的能力。亦即，將執法安全合作，具體落實在內國法化，使我國打擊資恐之防制體系更趨完備，不僅從爰參考 FATF「 四十項建議 」、聯合國國際公約及安全理事會相關決議，到制定《資恐防制法》，並於 2016 年 7 月 27 日公布施行。事實上，我國於 104 年也適時修正《刑法》沒收新制，於 2016 年 7 月 1 日施行，不僅舊法之沒收為從刑，修正後之沒收則為獨立之法律效果，並從原適用「行為時」的法律改以適用「裁判時」的法律，而得「溯及既往」。再者，也擴大沒收主體及沒收客體之範圍，修正後刑法之沒收，犯罪行為人以外之自然人、法人或非法人團體，無正當理由提供或取得供犯罪所用、犯罪預備之物或犯罪所生之物，得沒收之；而且修正後刑法將犯罪利得擴及：違法行為所得、其變得之物或財產上利益及其孳息，以及縱使欠缺有罪的主刑判決，亦也可為單獨沒收之宣告。[23]

我國《資恐防制法》相關法令之制定或修正，其旨趣乃在對應跨境執法安全合作與國際接軌、順應各國強化洗錢防制的全球趨勢，一方面在強化打擊跨境電信詐欺與人員運鈔洗錢等犯罪行

小組北亞區代表，2010 年加入「捐贈與技術協助工作組」（DAP），並自 2011 年起參與 APG 提供其太平洋島國會員及觀察員提升防制洗錢及打擊資助恐怖分子能力之計畫。請參見，中華民國外交部，〈國際警政組織〉，《中華民國外交部》，<https://www.mofa.gov.tw/igo/cp.aspx?n=4933DB35000610C4> (2018 年 11 月 23 日查詢)。

[23] 《中華民國刑法》，《全國法規資料庫》，107 年 3 月 13 日，<ttps://law.moj.gov.tw/Law/LawSearchResult.aspx?p=A&t=A1A2E1F1&k1=%E5%88%91%E6%B3%95> (2018 年 11 月 23 日查詢)。

為，再方面則有助於提高我國在防制涉及恐怖主義的網路、金融、洗錢犯罪的貢獻。近期，為爭取 APG 第三輪評鑑有好成績，行政院會於 2018 年 9 月 13 日，通過《洗錢防制法》與《資恐防制法》部分條文修正案，送立法院審議，其中除了擴大法遵適用對象到「指定之非金融機構事業及人員」，並增加罰鍰；受金融制裁對象也擴大，被制裁者直接或間接控制的財物或財產利益，例如被制裁者自己持有的財產不得移轉，請親友代為持有，或者以信託等方式持有的財產都會受到限制。[24] 進而，於同年 11 月 7 日經立法院修正發布，既充實《洗錢防制法》第 6 條，規定金融機構應訂定防制洗錢注意事項，並對指定之非金融事業或人員進行課責。[25] 同時，亦為完備《資恐防制法》第 9 條，資助恐怖活動、恐怖組織或恐怖分子者，有期徒刑，併科罰金之刑事責任之規定，增訂第 5 條之 1 規定 (主管機關在指定制裁名單前得不通知該個人、法人或團體陳述意見之機會)，以及修正第 7 條及第 10 條規定 (依規定辦理通報者，免除其業務上應保守秘密之義務；資恐犯罪為《洗錢防制法》所稱之特定犯罪)。[26] 從而，也有助於具體落實法遵文化與觀念是資恐防制的根基，亦使「指定之非金融機構事業及人員」成為擴大對象，把內稽內控的程序教育訓練與審

[24] 〈爭取 APG 第三輪評鑑成績 政院通過洗錢防制法、資恐防制法修正案〉，《中時電子報》，2018 年 9 月 13 日，<https://www.chinatimes.com/realtimenews/20180913002901-260407> (2018 年 11 月 23 日查詢)。

[25] 《洗錢防制法》，《全國法規資料庫》，2018 年 11 月 7 日，<https://mojlaw.moj.gov.tw/LawContent.aspx?LSID=FL006664> (2018 年 11 月 23 日查詢)。

[26] 《資恐防制法》，《全國法規資料庫》，2018 年 11 月 7 日，< https://mojlaw.moj.gov.tw/LawContent.aspx?LSID=FL081466> (2018 年 11 月 23 日查詢)。

查納入法制規範，並增訂裁罰。[27]

除上揭《資恐防制法》相關法令之制定或修正，《資恐防制法》也成為資恐防制跨境執法安全合作的重要法律依據。依《資恐防制法》第 4 條規定，「主管機關（法務部) 依法務部調查局提報或依職權，認個人、法人或團體有下列情事之一者，經審議會決議後，得指定為制裁名單，並公告之。」從「下列情事之一者」所指，包括：(一) 涉嫌犯（《資恐防制法》) 第 8 條第 1 項各款所列之罪，以引起不特定人死亡或重傷，而達恐嚇公眾或脅迫政府、外國政府、機構或國際組織目的之行為或計畫；(二) 依資恐防制之國際條約或協定要求，或執行國際合作或聯合國相關決議而有必要；前項指定之制裁名單，不以該個人、法人或團體在中華民國領域內者為限等內容看來，[28] 資恐防制顯然是防制金融恐怖主義執法合作之前提。

二、以確證資恐防制合作做為《資恐防制法》法意實踐的必由之途

從資恐防制是防制金融恐怖主義執法合作之前提，以及考察資恐犯罪藉由網路金融體系，衍生為金融恐怖主義的現實看來，防制網路金融犯罪在資恐與金融恐怖主義之間的關聯性，更成為國際社會打擊金融恐怖主義的執法安全合作重要議題。從而，確證資恐防制的執法安全合作，將係《資恐防制法》法意實踐的必

[27] 〈爭取 APG 第三輪評鑑成績 政院通過洗錢防制法、資恐防制法修正案〉。

[28] 《資恐防制法》，《全國法規資料庫》，2018 年 11 月 7 日，< https://mojlaw.moj.gov.tw/LawContent.aspx?LSID=FL081466> (2018 年 11 月 23 日查詢)。

由之途。

例如，我國法務部調查局因偵辦網路犯罪及數位鑑識能力，深獲美國、歐洲刑警組織 (Europol)、歐洲檢察官組織 (Eurojust) 肯定，經其邀請共同偵辦代號「雪崩」(Avalanche) 的跨境網路集團犯罪。該集團專門從事散布惡意程式與建立受駭中繼站之訊息傳遞平臺，進行針對性地攻擊網路銀行，估計在德國境內即已造成 600 萬歐元的損失，而透過「雪崩」進行的網路駭侵更造成全球數億歐元的經濟損失。「雪崩」平臺之所以特別，在於它使用「雙重快速導流技術」，該技術是使用快速轉換 IP 方法，提供強大的躲避技術，以防範執法機關的追查，因這種複雜的設定，使得「雪崩」平臺受到國際駭客集團的歡迎。2016 年 11 月 30 日 13:00(UTC)(臺灣時間 21 時) 全球同步執行收網。本案歷經 4 年調查，德國公訴檢察署及當地警局 (Lüneburg)，聯合美國、歐洲刑警組織 (Europol)、歐洲檢察官組織 (Eurojust)，以及全球等 31 個執法機關瓦解該網路犯罪集團。本次行動，顯示藉由全球各公、私人機構及執法機關共同合作，可以提供政府、企業及人民一個更安全的網路環境。[29] 由此我國實務經驗看來，所謂跨境執法安全合作，並非要「整合」組建特別的機關，而是在於如何促進跨部門多領域的有效交換資訊與情報之技術，以及解決問題的機轉或方案。

三、體現網路安全跨域治理的內涵

[29] 〈調查局與美國、歐洲刑警組織等 31 個國家共同偵破『雪崩』殭屍網路案〉，《法務部調查局》，2016 年 12 月 1 日，<https://www.mjib.gov.tw/news/Details?Module=1&id=236> (2018 年 11 月 23 日查詢)。

進一步認識網路安全跨域治理議題，不僅有助於發現公私協力，可產生的相互引領、增強、支援、交替的安全治理內涵，更能為鞏固防制暴戾的效果相互融合。包括警務情報蒐集、執行傳達護送任務，逮捕偵辦暴戾共犯削弱其網絡，維護公共秩序，保護重要人士，維護關鍵基礎設施與邊境管制安全等等。凡此網路跨域治理策略，將對防制暴戾行動的任何時程而言，產生引領、增強、支援、交替的戰略內涵。[30]

例如，香港特別行政區政府香港警務處網絡安全及科技罪案調查科 (CSTCB)，即充分體現網路跨域治理的內涵。不僅負責處理有關網路安全的事項及調查科技罪案，還專責處理電腦法理鑑識及防止科技犯罪的工作。該科更與本地及境外執法機構建立緊密聯繫，打擊跨境科技犯罪和分享情報。採用多機構合作模式，加強市民對電腦及網路保安和使用社交媒體所帶來風險的意識。加強與其他執法機構合作，打擊科技犯罪。在處理和調查科技犯罪方面，加強專業知識的統合及分享。網絡安全組協作隊係隸屬網絡安全及科技犯罪調查科，負責制訂和推行防止科技犯罪的工作，務求加強市民對防止科技罪案的認知。[31] 再者，美國聯邦調查局，曾於 2015 年間，偵破經由私營企業提供境外網路駭客盜取美國軍事與聯邦個人資料，企圖給予「伊斯蘭國」協助進行獵殺美國官員之案例。該案體現跨部門與多領域的網路安全治理的

[30] Kuldeep Kumar, *Police and Counterinsurgency: The Untold Story of Tripura's COIN Campaign*, (New Delhi: SAGE Publications India, 2016), p. 14.

[31] 〈網絡安全及科技罪案調查科 (CSTCB)〉，《香港特別行政區政府香港警務處》，2018 年 7 月，<https://www.police.gov.hk/ppp_tc/04_crime_matters/tcd/tcd.html> (2018 年 11 月 23 日查詢)。

融合內涵，有效防制網路與暴戾犯罪，以及恐怖主義與情報滲透的混合性網路襲擊 (hybrid cyberattack)。[32]

由上揭實務可見，跨域治理之所以能創新網路安全合作範疇，除了對涉及犯罪或恐怖活動之資訊與情報，進行編（轉）譯、分析及傳遞之外，更可融合他類資訊，例如威脅因素、公共安全、公共衛生、社會服務業、公共建設工程，進而發揮先制、確認、預防與監測犯罪或恐怖活動之效果。也就是說，跨域治理的知識理論，同時產生執法安全與合作行動策略上的雙重應用價值。一方面，它顯然有助益於吾人判斷犯罪或恐怖活動之型態與情勢；再者，可對特定重案產生跨域融合力量。因此，各界參與實體可以相互融合之意義，乃更具有獨特的啟發性。既可快速確認各類新興威脅，也對涉及科際整合、能動時效與跨域社群的特殊需求，提供解決問題之方案。甚至，可以支援各類預警資訊分析，改善緊急事態與常態行動資訊傳遞之效能。從而，犯罪資訊與網路治理交叉融合的分析過程，對官員、專家而言，即可由非法毒品活動、洗錢、詐欺、身分盜用（identity theft）等資訊之融合傳遞，提高對恐怖犯罪判斷之準確率。然而，卻不致因此取代情報或執法機關職能，或與其他部門產生疊床架屋之難題。[33]

---

[32] Amanda Ziadeh, “FBI is Fighting Hybrid Cyberattacks: Terrorism, Foreign Intelligence Threats and Traditional Crimes are Coordinated with Hackers,” January 3, 2018, <https://www.governmentciomedia.com/fbi-fighting-hybrid-cyberattacks> (2018 年 11 月 23 日查詢) .

[33] U.S. Department of Justice, “Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era,” June 9, 2015, p. 13. <https://it.ojp.gov/documents/fusion_center_guidelines_law_enforcement.pdf> (2018 年 11 月 23 日查詢).

未來網路安全跨域治理，其內涵並不在於如何重新「整合」組建特別的機關，而是在於體現跨部門多領域的有效交換資訊與情報之技術，以及解決問題的機轉或方案。尤其，網路安全跨域治理議題的實踐，藉由政策倡議與公私協力之培力(empowerment)，將可產生彼此相互引領、增強、支援、交替的安全治理內涵，更能與鞏固防制犯罪型暴戾的效果相互融合。

陸、結論

本文從網路金融犯罪在資恐與金融恐怖主義之間的關聯性，做為問題意識的發想。在描述網路犯罪因素中，不僅發現該因素將使安全危害產生加乘效應，甚至伴隨犯罪型暴戾。其中，資助恐怖主義犯罪即係新興犯罪型暴戾，既對實體與網路虛擬空間構成複合型危害，同時又成為恐怖主義運作之動力，激化恐怖金融犯罪的危害擴溢。然而，在國際社會不願見跨境 (域) 合作防制恐怖犯罪出現漏洞的前提下，資恐防制議題已不再侷限於刑法或犯罪學領域，而是指涉到包括執法安全合作、全球治理與安全戰略等政策應用層面。尤其，資恐防制做為打擊金融恐怖主義執法安全合作之前提，以及國際社會普遍認知到資恐犯罪藉由網路金融體系，衍生為金融恐怖主義的擴溢危害，更需要彼此超越主權紛爭、採取務實模式。從而，有助於創新我國實踐跨境 (域) 執法安全合作的職能空間，也進一步彰顯我國做為國際良善夥伴的能力。

（收稿：2018 年 10 月 23 日；第一次修正：2019 年 1 月 10 日；接受：2019 年 12 月 23 日）

參考文獻

一、中文部分

（一）報紙

中時電子報，2018/09/13。〈爭取 APG 第三輪評鑑成績 政院通過洗錢防制法、資恐防制法修正案〉，《中時電子報》，<https://www.chinatimes.com/realtimenews/20180913002901-260407> (2018 年 11 月 23 日查詢)。

（二）網際網路

中華民國外交部，〈國際警政組織〉。臺北市，中華民國外交部。<https://www.mofa.gov.tw/igo/cp.aspx?n=4933DB35000610C4> (2018 年 11 月 23 日查詢)。

全國法規資料庫，2018/03/13。《中華民國刑法》。臺北市：全國法規資料庫， <ttps://law.moj.gov.tw/Law/LawSearchResult.aspx?p=A&t=A1A2E1F1&k1=%E5%88%91%E6%B3%95> (2018 年 11 月 23 日查詢)。

全國法規資料庫，2018/11/7。《洗錢防制法》。臺北市：全國法規資料庫，<https://mojlaw.moj.gov.tw/LawContent.aspx?LSID=FL006664 > (2018 年 11 月 23 日查詢)。

全國法規資料庫，2018/11/7。《資恐防制法》。臺北市：全國法規資料庫，<https://mojlaw.moj.gov.tw/LawContent.aspx?LSID=FL081466> (2018 年 11 月 23 日查詢)。

法務部調查局，2016/12/01。〈調查局與美國、歐洲刑警組

織等 31 個國家共同偵破『雪崩』殭屍網路案〉。新北市：《法務部調查局》，<https://www.mjib.gov.tw/news/Details?Module=1&id=236> (2018 年 11 月 23 日查詢)。

香港特別行政區政府香港警務處，2018/07。〈網絡安全及科技罪案調查科 (CSTCB)〉。香港：《香港特別行政區政府香港警務處》，<https://www.police.gov.hk/ppp_tc/04_crime_matters/tcd/tcd.html> (2018 年 11 月 23 日查詢)。

二、英文部分

（一）專書

Kumar, Kuldeep, 2016. *Police and Counterinsurgency: The Untold Story of Tripura's COIN Campaign*. New Delhi: SAGE Publications India.

Madsen, Frank G., 2009. *Transnational Organized Crime*. New York: Routledge Global Institutions.

（二）專書論文

Albanese, Jay S. 2014. "Choosing a Micro or Macro Perspective for Understanding Organized Crime: the Contributions of Ernesto Savona," in S. Caneppele, F. Calderoni eds., *Organized Crime, Corruption and Crime Prevention*, Switzerland: Springer International Publishing. pp, 263-268.

Giraldo, Jeanne and Harold Trinkunas. 2010. "Transnational Crime," in Alan Collins eds. *Contemporary Security Studies.* Oxford: Oxford University Press. pp. 428-426.

Ridely, Nick. 2008. "Analyse This (and That): a Consideration of

the International Role of Analysis," in Steven David Brown ed., *Combating International Crime: the Longer Arm of the Law*. London and New York: Routledge-Cavendish. pp. 205-213.

Wittek, Rafael. 2007. "Governance from a Sociological Perspective," in Dorothea Jansen ed., *New Forms of Governance in Research Organizations: Approaches*, *Interfaces and Integration*. Dordrecht: Springer. pp. 77-106.

（三）期刊論文

Brenner, Susan W. December. 2006. "Cybercrime Jurisdiction," *Crime, Law and Social Change*, Vol. 46, No. 4-5, pp. 190-193.

Burgoyne, Michael L. February 2012. "The Effectiveness of Counterinsurgency Principles against Criminal Insurgency: the Right Tool for the Job," *Small Wars Journal*, pp. 1-7.

Grabosky, Peter. June 2007. "Requirements of Prosecution Services to Deal with Cyber Crime," *Crime, Law and Social Change*, Vol. 47, No. 4-5, pp. 201-223.

Levi, Michael. June 2008. "White-collar, Organised and Cyber Crimes in the Media: some Contrasts and Similarities," *Crime, Law and Social Change,* Vol. 49, No. 5, pp. 365-377.

McCusker, Rob. December 2006. "Transnational Organized Cyber Crime: Distinguishing Threat from Reality," *Crime, Law and Social Change,* Vol. 46, No. 4-5, pp. 257-273.

Naím, Moisés. May/June 2012. "Mafia State: Organized Crime Take Office," *Foreign Affairs*, Vol. 91, No. 3, pp. 100-111.

Pocar, Fausto. March, 2004. "New Challenges for International Rules against Cyber-crime," *European Journal on Criminal Policy and Research*, Vol.10, No. 1, pp. 27-37.

Staniland, Paul. Fall 2017. "Wither ISIS? Insights from Insurgent Response to Decline," *The Washington Quarterly*, Vol. 40, Issue 3, pp. 29-43.

（四）網際網路

European Commission. November 2018. "Cybercrime," <https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime_en >. (2018 年 11 月 23 日查詢).

Hoover, Patrick, and Omar Kebbe. September 22, 2017. "After Raqqa: the Next Jihadist Stronghold in Syria," *Terrorism Monitor,* Volume 15, Issue 18, <https://jamestown.org/program/after-raqqa-the-next-jihadist-stronghold-in-syria/> (2018 年 11 月 23 日查詢).

Moore, Scott. 2007. "The Basics of Counterinsurgency," *Small War Journal*, <http://smallwarsjournal.com/documents/moorecoinpaper.pdf> (2018 年 11 月 23 日查詢).

United States Department of Justice. June 9, 2015. "Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era," <https://it.ojp.gov/documents/fusion_center_guidelines_law_enforcement.pdf> (2018 年 11 月 23 日查詢).

United States Department of State. September 10, 2014. "The Global Coalition to Defeat ISIL," <http://www.state.gov/s/seci/index.

htm> (2018 年 11 月 23 日查詢).

Weimann, Gabriel. May 12, 2014. "New Terrorism and New Media," *Research Series*, <https://www.wilsoncenter.org/sites/default/files/new_terrorism_v3_1.pdf> (2018 年 11 月 23 日查詢).

Ziadeh, Amanda. January 3, 2018. "FBI is Fighting Hybrid Cyberattacks: Terrorism, Foreign Intelligence Threats and Traditional Crimes are Coordinated with Hackers," <https://www.governmentciomedia.com/fbi-fighting-hybrid-cyberattacks> (2018 年 11 月 23 日查詢).