美國對承包商之網路安全認證

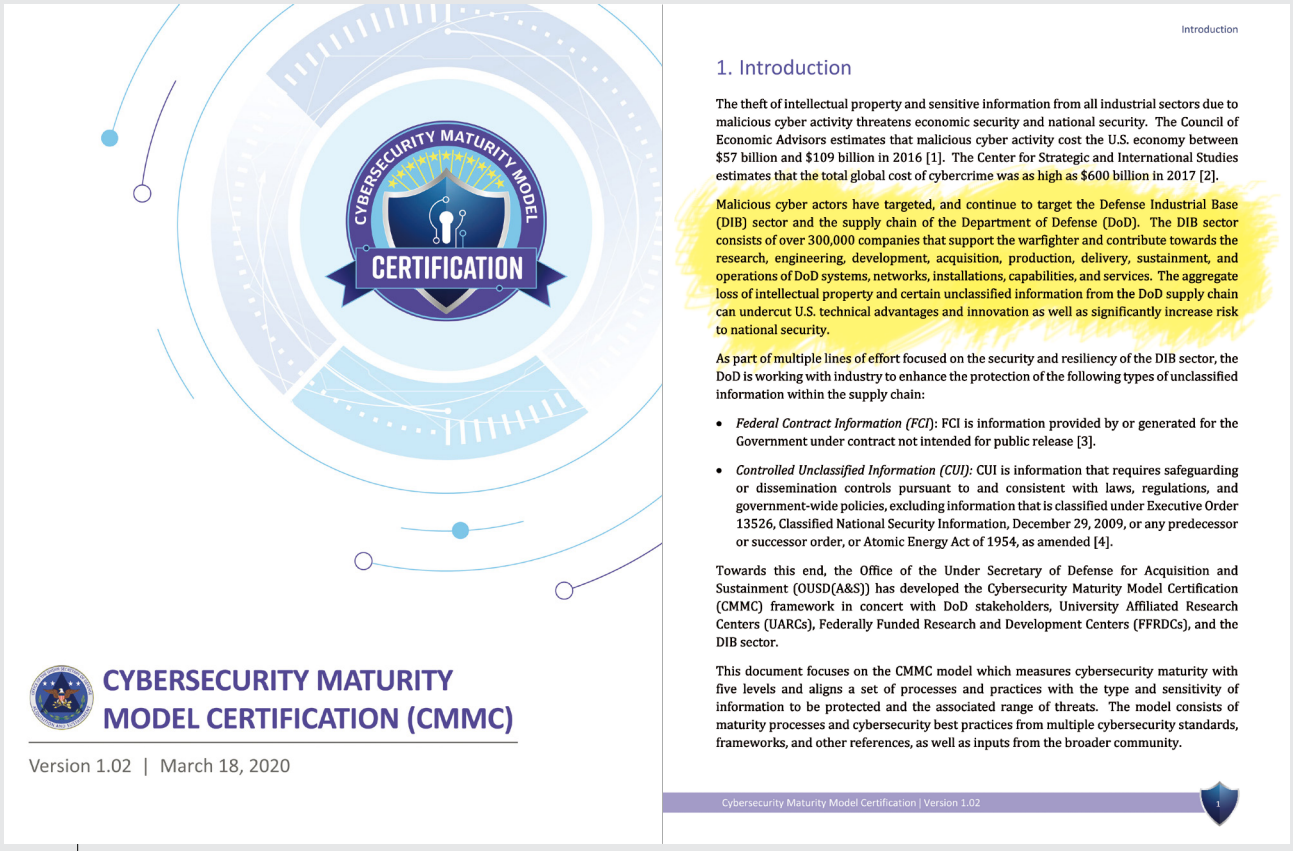
◆ 實踐大學副教授 ── 蔡裕明

美國國防部於 2020 年 2 月宣布，要求競標國防部合約的承包商，需符合《網路安全成熟度認證》（Cybersecurity Maturity Model Certification, CMMC）資格，且每 3 年需更新一次認證。未來，廠商必須取得不同等級之安全驗證，才能承包美國國防部的業務。

CMMC 介紹

CMMC 是美國國防部正在實施於規範國防工業基礎（defense industrial base, DIB）網路安全工作之標準。認證主要目的是在評估國防部承包商在網路安全領域的能力，適用於與國防部有直接接觸的主要承包商、執行合約的分包商和外國供應商。這將涵蓋國防部 30 萬家承包商。

由於美國每年平均因網路安全損失超過 6 千億美金，且執行國防部合約的分包商通常都是小型企業，大部分沒有完善的網路安全措施；且對駭客而言，攻擊第二線承包商比攻擊第一線的更具吸引力。由於承包商數量極多且計畫相當艱鉅，國防部要求由第三方評估組織來執行 CMMC 認證，國防部並會對該評估組織進行認證。



《網路安全成熟度認證》（Cybersecurity Maturity Model Certification, CMMC）主要目的是在評估國防部承包商在網路安全領域的能力。（Source: Office of the Under Secretary of Defense for Acquisition & Sustainment, https://www.acq.osd.mil/cmmc/draft.html）

CMMC 的認證級別

CMMC 有 5 項認證級別，各項級別彼此相依，即每項級別需遵守較低級別之規定，以驗證對網絡安全標準的遵守情況；另承包商須通過較低級別後，才能升級到下個級別。包括：[1]

級別 1：基礎防護（Basic）—保護「聯邦合同資訊」（Federal Contract Information，下稱 FCI）。例如公司必須使用防毒軟體或確保員工定期更改密碼，以保護 FCI。

級別 2：中等防護（Intermediate）—保護「受控非機敏資訊」（Controlled Unclassified Information，下稱 CUI）。CUI 為美國法規要求保護或傳播措施之任何資訊，但不包含機密資訊。例如，承包商需通過美國商務部國家標準技術研究院的 NIST 800-171，來保護 CUI。

[1] Abigail Stokes, M. C. (2020). The cybersecurity maturity model certification explained: What defense contractors need to know. CSO (Online), Retrieved from https://search.proquest.com/docview/2387511629?accountid=13838.

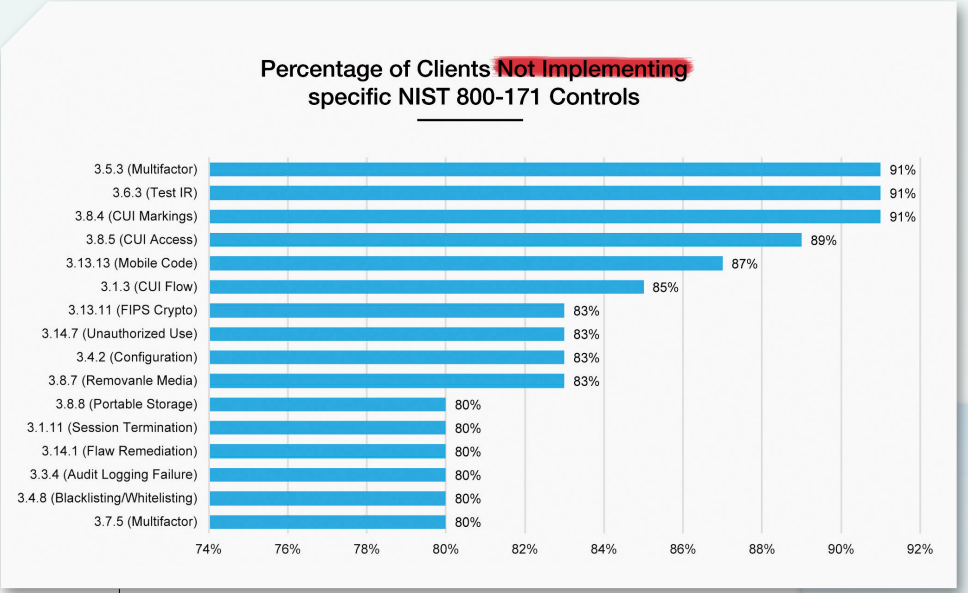
級別 3：良好防護（Good）—增加 CUI 之保護。公司必須制定制度化的管理計劃，以保護 CUI，包括所有 NIST 800-171 r2 安全要求以及附加標準。

級別 4：主動防護（Proactive）—能防範「進階持續性威脅」（advanced persistent threats，下稱 APT）。APT 被定義為具有先進水平的專業知識和大量資源的對手，對手會使用多種媒介攻擊。公司必須實施審查與評估有效性之流程，並且建立其他強化作法，可以檢測並回應不斷變化的策略、技術和程序以及持續性的先進威脅。

級別 5：進階防護（Advanced）—具備檢測和回應 APT 攻擊之優化流程。公司必須在整個組織中採用標準化和優化的流程，以及其他強化資訊安全作法，以能夠回應 APT 攻擊等更為複雜的功能。

美國國防部強調，CMMC 為改變國防單位承包商內部網路安全文化（cyber-security culture）的開始，並需要對於不斷發展的威脅進行準備，而非僅是獲得 CMMC 的認證。國防部門的承包單位除要獲得 CMMC 的認證外，還得在組織內培養靈活性的網路安全文化，以確保在市場上獲得更佳競爭力。

圖 1　CMMC 的 5 項認證級別



美國網絡風險管理公司 Sera-Brynn 在 2019 年報告提及，國防部許多承包商未實施控制措施來保護國防部在網路上的機敏情報。（Source: DEFENSE TECHNICAL INFORMATION CENTER, https://ndia.dtic.mil/2020/2020manufacturing.html）

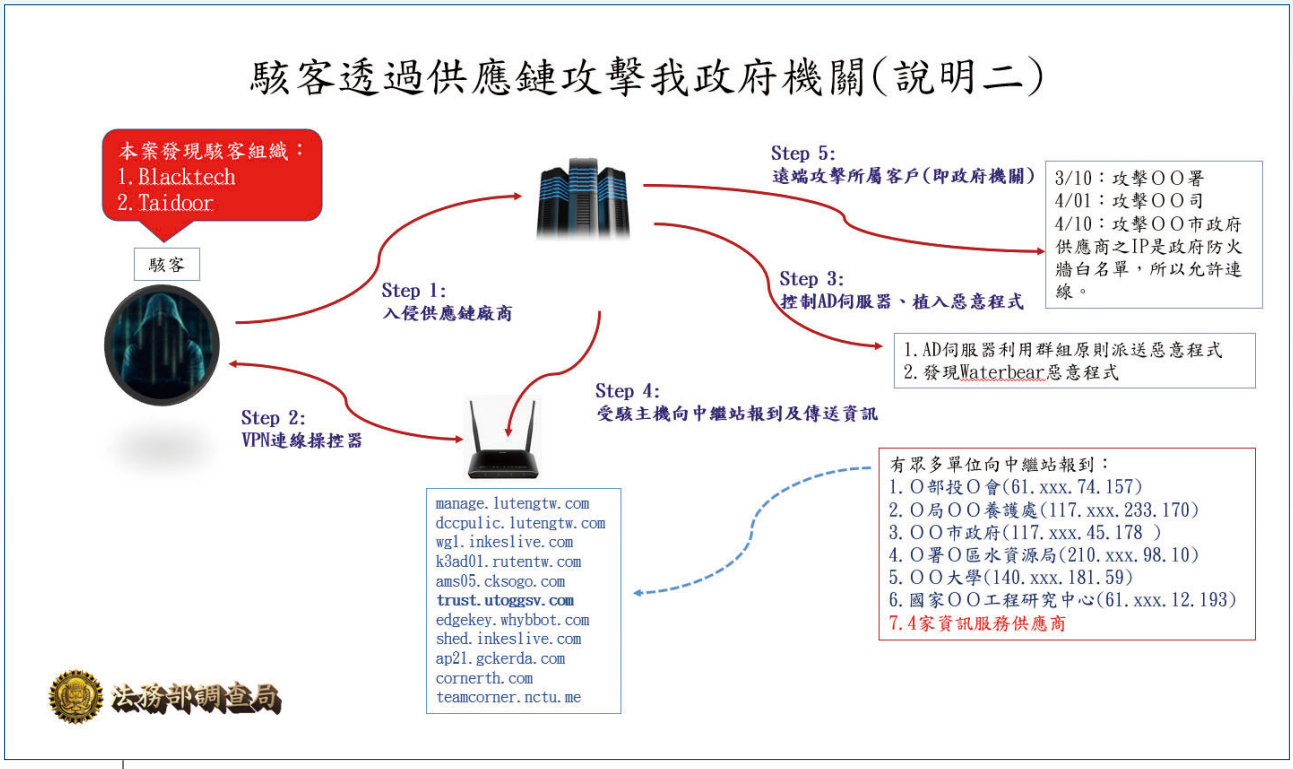
美國國防部負責採購的副部長洛德（Ellen Lord）表示，國防部注意到認證成本對於中小企業可能成為沉重的負擔，所以國防部將對小型承包商提供培訓機會，未來再擴及中型與大型國防承包商。

美國建置 CMMC 之必要性

美國網絡風險管理公司 Sera-Brynn 在 2019 年報告提及，國防部許多承包商未使用多重要素驗證（Multi-factor authentication）、通過事故應變測試等控制措施，以及僱用未經訓練的員工，或運作較差的修補程式管理（patch management），來保護國防部在網路上的機敏情報。

2018 年 6 月美國海軍承包商遭駭客入侵，導致飛彈研發之機密細節外洩。（此照片為示意圖，非當事潛艦）

此外，近年美國許多機構歷經多次網路入侵，從美國五角大廈到國土安全部，駭客甚至進入「氣隙網路」（air-gap network）機密系統或關鍵基礎設施的工業控制系統（Industrial control system, ICS）等。例如：2018 年 6 月美國海軍承包商遭駭客入侵，致美國潛艦所使用的超音速反艦飛彈之研發細節外洩。2018 年 10 月，駭客入侵外包商系統，借道進入國防部網路，導致 3 萬名員工的差旅資料外洩等事件。這些事件讓美國國防部意識到，不僅



去年 8 月調查局發現政府部門及其資訊服務供應商有遭滲透之問題。（圖片來源：法務部調查局）

需要慎選國防部門的承包商，也應同時注意這些公司僱用的二級和三級分包商。

他山之石　可供借鏡

我國曾於前（2019）年破獲新北市某間工程公司利用承包國防工程機會刺探機密，去（2020）年 8 月調查局新聞發布，發現政府部門及其資訊服務供應商有遭滲透之問題。是以，我國現階段應盤點國防部門之網路承包商，並要求或輔導其等符合國際相關網路安全規範與程序，亦可要求承包商定期報告遭受網路威脅與攻擊狀況，或仿效美國國防部所提出之 CMMC 網路安全認證標準，要求國防部門的承包商注意其網路安全與加強人員培訓，並防範承包商內部可能的「內賊」問題。

現今全球正戮力抵抗新冠肺炎之際，駭客也將攻擊重點轉向醫療院所或疫苗等研究機構。未來我國除應持續關注國防單位承包商的網路安全能力外，更需要留意駭客針對醫療院所或疫苗研發單位承包商之可能攻擊或竊取資料等行動。

美國會大廈暴動 赤裸揭露極右翼之國安威脅

◆ 調查局專門委員 — 陳能鏡

一場暴動，摧毀美國民主基石與傳統價值，更揭露極右翼激進主義正帶來直接且立即之國安威脅。

（Photo Credit: The deadly Capitol Hill riots, https://www.flickr.com/photos/30478819@N08/50818647218）

美國國會大廈暴動案定調為恐怖攻擊事件

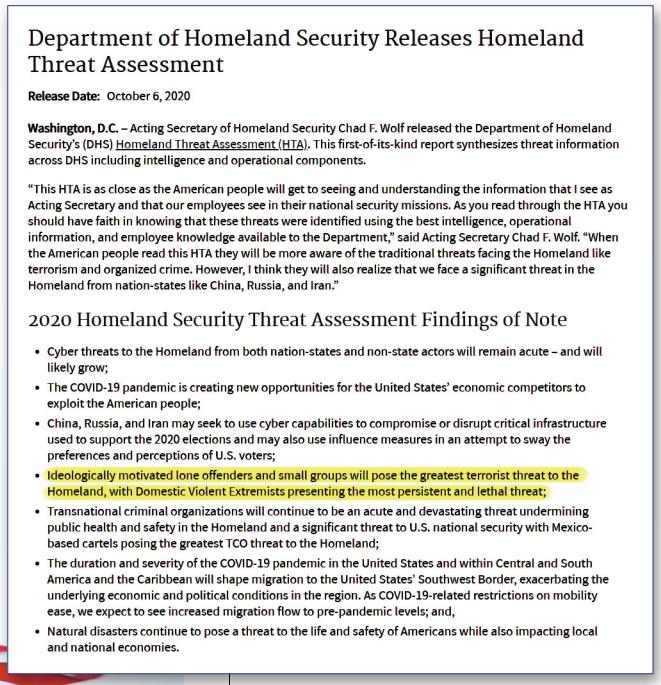
1 月 6 日在美國前總統川普、前紐約市長朱利安尼等人鼓動下，上千川迷攻占美國國會，中斷總統大選結果認證程序，破壞設施機具，甚至有人偷走眾院議長手提電腦，企圖轉賣俄羅斯情報機關等。事後經美國執法機關調查發現，極右激進民兵團體、陰謀論網路運動，如布加洛（Boogaloo Bois）、驕傲男孩（Proud Boys）、匿名者（Qanon）等團體高度介入本案，隨即定調為恐攻案，並擴大偵辦。

美國國土安全部於去（2020）年 10 月發布的年度「國土安全威脅評估」報告指出，內部暴力激進主義者正帶給美國國土安全最持續、最致命的威脅。此次國會恐攻案只是更赤裸揭露，極右恐怖主義不但澈底摧毀民主價值，更已帶給國家安全直接且立即的威脅。

川普的部分支持者認為美國大選不公，於是闖入美國國會，中斷國會認證總統大選結果的程序，試圖反轉選舉結果。（Photo Credit: Tyler Merbler, https://www.flickr.com/photos/37527185@N05/50821278936）

極右恐怖主義在歐美威脅日增

恐攻死亡人數自 2014 年起，已連續 5 年呈下降趨勢，但西歐、北美、紐西蘭與澳洲等西方民主國家，極右翼恐攻案件數



Department of Homeland Security Releases Homeland Threat Assessment

Release Date: October 6, 2020

Washington, D.C. – Acting Secretary of Homeland Security Chad F. Wolf released the Department of Homeland Security's (DHS) Homeland Threat Assessment (HTA). This first-of-its-kind report synthesizes threat information across DHS including intelligence and operational components.

"This HTA is as close as the American people will get to seeing and understanding the information that I see as Acting Secretary and that our employees see in their national security missions. As you read through the HTA you should have faith in knowing that these threats were identified using the best intelligence, operational information, and employee knowledge available to the Department," said Acting Secretary Chad F. Wolf. "When the American people read this HTA they will be more aware of the traditional threats facing the Homeland like terrorism and organized crime. However, I think they will also realize that we face a significant threat in the Homeland from nation-states like China, Russia, and Iran."

2020 Homeland Security Threat Assessment Findings of Note

- Cyber threats to the Homeland from both nation-states and non-state actors will remain acute – and will likely grow;
- The COVID-19 pandemic is creating new opportunities for the United States' economic competitors to exploit the American people;
- China, Russia, and Iran may seek to use cyber capabilities to compromise or disrupt critical infrastructure used to support the 2020 elections and may also use influence measures in an attempt to sway the preferences and perceptions of U.S. voters;
- Ideologically motivated lone offenders and small groups will pose the greatest terrorist threat to the Homeland, with Domestic Violent Extremists presenting the most persistent and lethal threat;
- Transnational criminal organizations will continue to be an acute and devastating threat undermining public health and safety in the Homeland and a significant threat to U.S. national security with Mexico-based cartels posing the greatest TCO threat to the Homeland;
- The duration and severity of the COVID-19 pandemic in the United States and within Central and South America and the Caribbean will shape migration to the United States' Southwest Border, exacerbating the underlying economic and political conditions in the region. As COVID-19-related restrictions on mobility ease, we expect to see increased migration flow to pre-pandemic levels; and,
- Natural disasters continue to pose a threat to the life and safety of Americans while also impacting local and national economies.

美國國土安全部於 2020 年 10 月發布的「國土安全威脅評估」，報告中提到具意識形態的犯罪者和小團體最可能對本土構成恐怖威脅，而國內暴力極端分子則是最持久和致命的威脅。（Source: U.S Department of Homeland Security, https://www.dhs.gov/news/2020/10/06/department-homeland-security-releases-homeland-threat-assessment）

及死亡人數反現成長趨勢，右翼恐怖主義威脅是否高於伊斯蘭聖戰主義威脅，近年來已成熱門討論議題。

依據「經濟與和平研究所」（Institute for Economic & Peace）統計資料，自 2002 至 2019 年，全球死於恐攻案人數為 23 萬 6,422 人，其中 1,215 人死於發生在西方國家之恐攻案，僅占 0.51%；這 1,215 人中，814 人死於聖戰恐攻案，286 人死於極右翼恐攻案，其餘則死於民族自決、分離主義、環保、動保、極左翼等恐攻案。

另 2019 年西方國家所發生的恐攻案，63% 為極右或極左恐攻案，其所造成的死亡人數占死亡總數的 90%，其中右翼恐攻案共 49 件，其造成死亡人數占比為 82%。

前述統計數字說明，極右翼恐怖主義對西方國家之威脅已超過伊斯蘭激進主義。

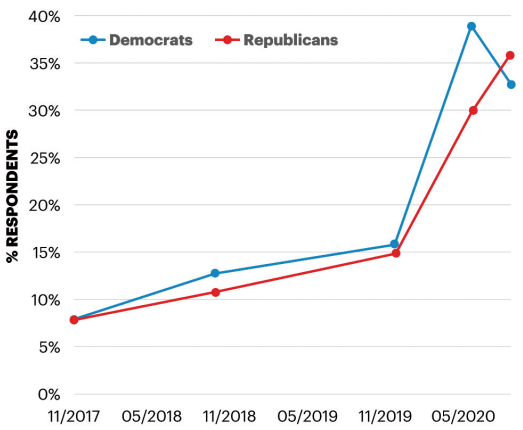
美國政客對以暴力行為來達成政治目的之接受度提高

美國近年由於資源分配不均、政府治理不彰、資訊流通不自由、他人權利不尊重、貪瀆盛行等負面因素，讓美國政治氣候發生重大變化：政治對立加深、政治暴力加劇，甚至政治人物對以暴力行為來達成渠等政治目的之接受度提高。民調顯示，共和及民主 2 黨對於以政治為最終目的之暴力接受度，在 2019 年 11 月底均約為 15%，而至 2020 年 9 月止，民主黨已達 33%，共和黨更高達 36%。

FIGURE 4.16

People who feel that violence is justified in advancing political goals, United States, 2017–2020

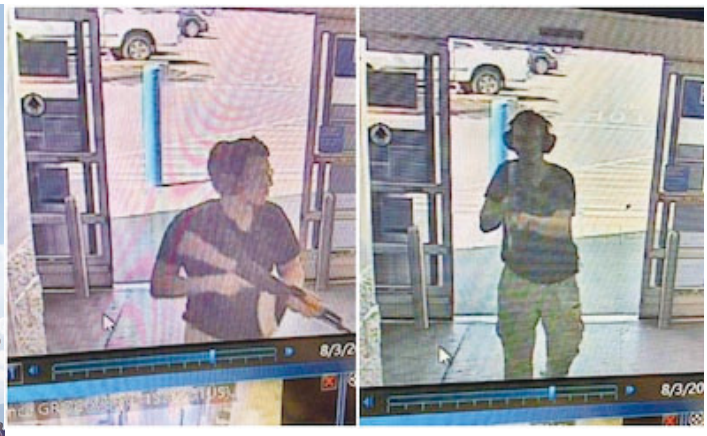
Both Democrats and Republicans are now much more likely to feel that violence for political ends is at least partially justified.



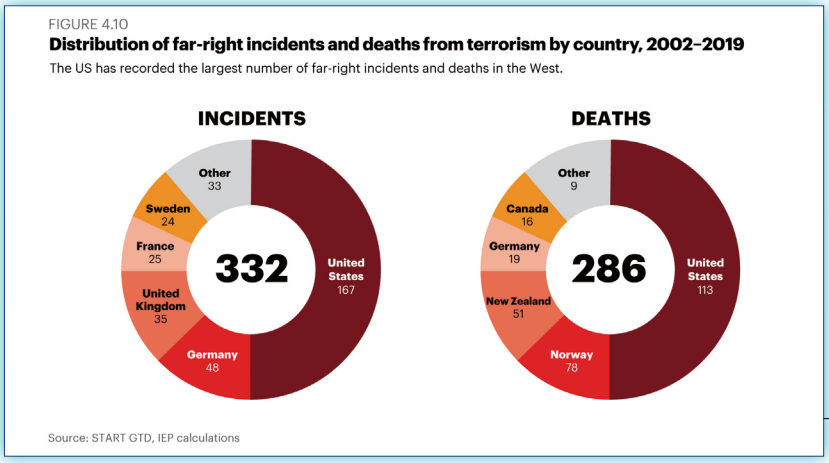
Source: YouGov, Voter Study Group, Nationscape

民調顯示，共和及民主 2 黨對於以政治為最終目的之暴力接受度整體提高。（Source: Institute for Economics & Peace, GLOBAL TERRORISM INDEX 2020, https://www.visionofhumanity.org/resources）

近年來激進分子增加並以強硬的暴力手段表達訴求，導致無辜民眾傷亡。圖為 2018 年匹茲堡猶太教堂槍擊案地點，槍手為白人至上主義，此事件造成 11 人罹難，6 人受傷。（Photo Credit: David Fulmer, https://www.flickr.com/photos/daveynin/45013855725）



2019 年 8 月發生在德州埃爾帕索 Walmart 賣場的槍擊案，美國司法部定調為本土恐怖攻擊。該案導致至少 20 人死亡，數十人受傷。（Photo Credit: Walmart Video Surveillance Camera, https://en.wikipedia.org/wiki/File:Patrick_Crusius_Video_Surveillance_Shooting.png; Deb Haaland, https://twitter.com/RepDebHaaland/status/1159227783513612291）



自 2002 至 2019 年，美國是西方國家中遭遇極右翼恐攻案件數及人民死亡數最高的國家，占比分別為 50% 及 40%。（Source: Institute for Economics & Peace, GLOBAL TERRORISM INDEX 2020, https://www.visionofhumanity.org/resources）

當黨政人物不排斥暴力，甚至縱容激進分子以暴力手段表達訴求或不滿時，恐攻事件將層出不窮。例如 2018 年 10 月賓州匹茲堡生命之樹猶太會堂槍擊案、2019 年 4 月加州聖地牙哥猶太會堂槍擊案、2019 年 8 月德州艾爾帕索賣場槍擊案、2020 年 10 月密西根州長惠特曼刺殺未遂案，以及 2021 年 1 月國會大廈暴動案等等。

根據「經濟與和平研究所」資料，自 2002 至 2019 年，美國是西方國家中遭遇極右翼恐攻案件數及人民死亡數最高的國家，占比分別為 50%（167/332）及 40%（113/286），在國會大廈暴動案後，更重創其國際形象，美國絕對是極右翼恐怖主義的最大受害國。

布加洛是近年來被公認為最危險的反政府、反威權暴力團體，其服裝特徵為夏威夷襯衫和軍服，以武裝推翻政府及主張擁有槍權是其兩大基本信念。（Photo Credit: Becker1999, https://www.flickr.com/photos/becker271/50284558387）

驕傲男孩是一個支持法西斯主義的右翼組織，成員基本為男性，組織宗旨為無政府、反毒品、反戰爭、反移民、反種族主義等，因為川普在總統辯論會上的認證，將此視為川普對他們的認同與激勵。（Photo Credit: Anthony Crider, https://www.flickr.com/photos/acrider/50658866101）

美國極右翼恐怖組織簡介

國會大廈暴動案後，美國執法機關盡全力追緝涉案者，發現民兵團體、陰謀論運動等極右組織為排名第二的重大罪犯，僅次於總統川普。依據知名民權團體「南方貧窮法律中心」（Southern Poverty Law Center）資料顯示，現今全美各地民兵團體超過 180 個，他們雖各有各的理念，然共同特色都是反政府組織，尤其是反對聯邦政府的槍枝管制，雖不宣揚暴力，但經常全副武裝，甚至參與暴力示威，包括美國總統大選後的 MAGA（讓美國再次偉大）示威活動。現簡單介紹其中 3 大罪犯。

一、布加洛

於歐巴馬就任總統後成立，公認為最危險的新興反政府民兵團體，美國司法部形容其是個鬆散的個人連結團體，成員們大都懷有暴力反政府情緒。人權團體「反毀謗聯盟」（Anti-Defamation League）指出，布加洛本質上就是反政府、反威權及反警察，武裝推翻政府及堅決主張擁槍權是其兩大基本信念。自 2019 年起，參與過擁槍權、反疫情封鎖、黑人的命也是命等示威活動。部分成員甚至仿效伊斯蘭激進武裝分子「mujahideen」（意謂自由戰士），自稱為「boojahideen」，利用抗議從事反公權力之武裝活動。2020 年 7 月 3 名成員企圖引發暴力示威，在內華達州以恐怖主義罪被起訴；2020 年 12 月司法部發布新聞稿，指布加洛成員共謀提供巴勒斯坦恐怖組織「哈馬斯」（Hamas）物資，並已認罪。美國總統大選後，布加洛線上論壇平臺「自由之樹」（Tree of Liberty）

匿名者 Q 屬極右翼陰謀論網路運動，其認為美國政府內部存在一個反對川普的深層政府，以擁護川普為目標，他們散布假訊息吸引民眾認同。（Photo Credit: Elvert Barnes, https://www.flickr.com/photos/perspective/50693880817; Anthony Crider, https://www.flickr.com/photos/acrider/49416341132）

貼文，號召支持者於 1 月 17 日在國會大廈及全美 50 個州州議會集結並武裝抗議，企圖阻止拜登就任總統。

二、驕傲男孩

於 2016 年由加拿大裔英國右翼分子 Gavin Mclnnes 主導成立，成員以西方沙文主義為傲。驕傲男孩是反移民的白人男性極右團體，「南方貧窮法律中心」稱其是仇恨團體，過去即有街頭暴力對抗左翼的歷史，特別是「反法西斯主義運動」（antifa），2 名成員因在紐約毆打反法西斯運動人士於 2019 年被判有罪並入獄服刑。2020 年 9 月 29 日的首場總統電視辯論會上，主持人問到是否譴責到處製造動亂的白人至上主義時，針對拜登點名驕傲男孩，川普公然答稱：「驕傲男孩，後退待命」。川普的認證激勵，讓驕傲男孩無役不與，當然包括國會大廈暴動案。

三、匿名者 Q

屬極右翼陰謀論網路運動，沒有真正的領導人，2017 年 10 月首度在美國出現，其聲稱美國政府內部有一個「深層國家」（deep state），由民主黨的歐巴馬、希拉蕊等政治人物夥同比爾蓋茲等社會精英組成的撒旦集團來領導，密謀向川普展開鬥爭，川普則是救世主。該組織以刻意製造的謠言（disinformation）或假訊息（misinformation）來吸引信徒，不但已全面滲透進入美國民眾日常，更藉新冠疫情而蔓延全球，其信徒或支持者已涉及多起暴力事件。2019 年美國聯邦調查局將其列為「國內恐怖主義潛在威脅」，西點軍校

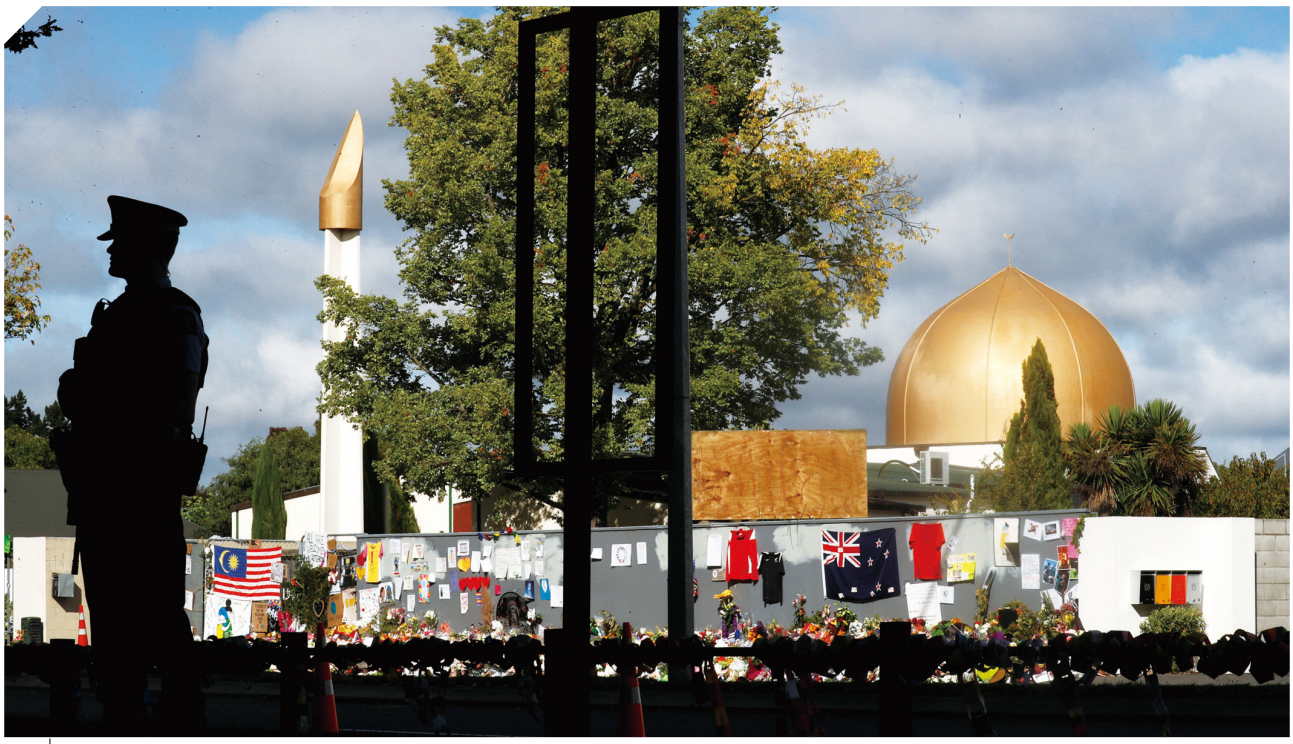
打擊恐怖主義中心亦形容其為「公共安全的全新挑戰」。在 2020 年 8 月白宮記者會中，當記者提到匿名者 Q 時，川普如是說：「我對這個運動不是很了解，只知道他們非常喜歡我，我很感激，而且他們還是愛這個國家的人民」。有了「愛國者」的加持，匿名者 Q 當然勇於衝鋒陷陣，攻占國會大廈。

極右翼恐怖主義特性

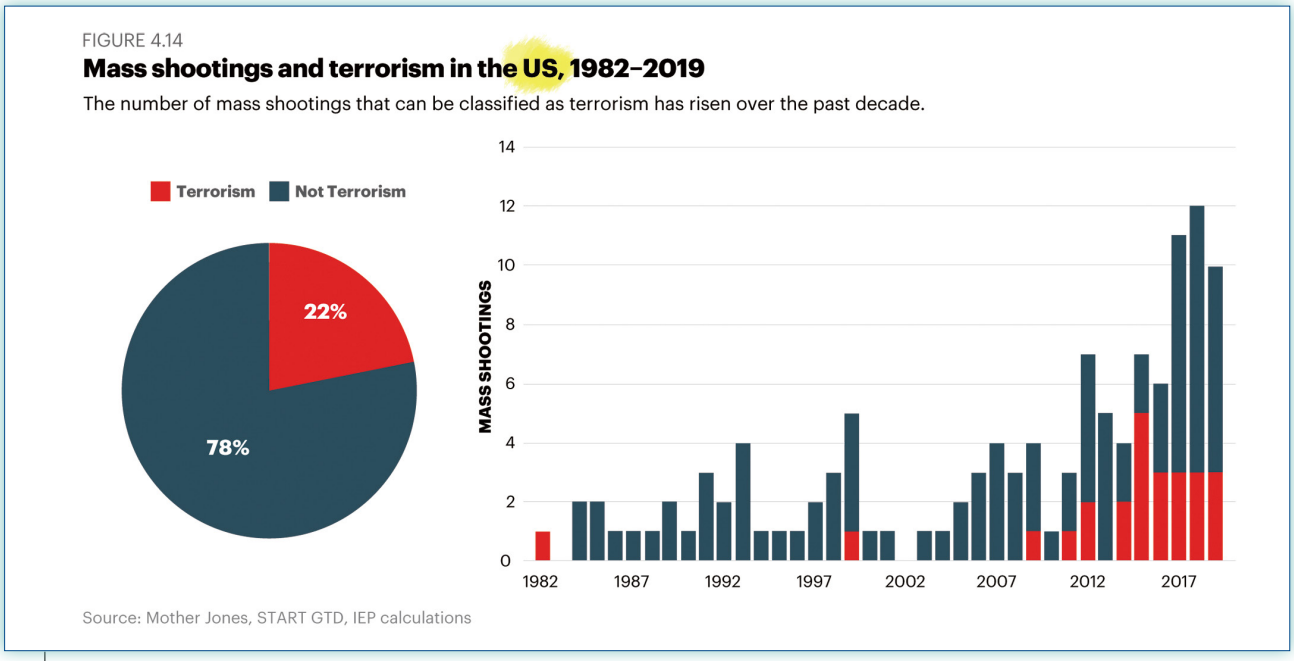
極右翼恐怖主義的崛起，已讓過去 5 年西方國家的極右翼恐攻案成長 250%，死亡人數增加 709%，極右翼恐怖主義已成為西方國家安全及民主價值的重大挑戰，其特性值得瞭解。僅依「經濟與和平研究所」2020 年 11 月發布之「2020 全球恐怖主義指數」統計資料，摘述於後：

一、致死率

西方國家過去 20 年，伊斯蘭恐攻案仍屬最致命，每案造成 4.49 人死亡，其次是極右的 0.86 人，極左則是 0.11 人。過去 5 年死亡人數超過 10 人的重大恐攻案共有 13 件，其中有 6 件屬極右恐攻案。1995 年 4 月美國奧克拉荷馬市聯邦大樓爆炸案死亡 168 人及受傷近 700 人，犯案者為極右團體主權公民運動者（Sovereign Citizen Movement）；2019 年 3 月在紐西蘭基督城的反穆斯林移民恐攻案更造成 51 人死亡。



在過去 20 年間的西方恐攻案件，伊斯蘭恐攻仍是造成最大的傷亡。圖為 2019 年發生的基督城清真寺槍擊案，當時造成 51 人死亡，引起全球嘩然。（圖片來源：路透社／達志影像）



2009 至 2019 年期間，恐攻槍擊案在大規模槍擊案之占比由 4.2% 成長到 30%，槍械成為恐怖分子重要的作案工具之一。（Source: Institute for Economics & Peace, GLOBAL TERRORISM INDEX 2020, https://www.visionofhumanity.org/resources）

二、作案者

大部分之極右翼恐攻案由孤狼所執行，孤狼並未加入任何恐怖組織或極右激進團體，但他可能曾與某極右分子接觸或受某極右恐攻案所激發。統計發現，6 成以上之右翼恐攻案由不附屬於團體的恐怖分子所為。例如 2002 至 2019 年期間，西方國家共發生 52 件造成死亡之極右翼恐攻案，其中只有 7 件由團體所為，而 2010 年以後，更是全由孤狼一人作案。

三、槍擊案

若將發生在公共場所、造成 4 人以上死亡及無確定受害對象之大規模槍擊案或瘋狂濫射案，歸類為恐攻案，則 2009 至 2019 年期間共發生 67 起槍擊恐攻案，恐攻槍擊案在大規模槍擊案之占比，由 4.2% 成長到 30%。過去極右恐怖分子以炸彈及爆裂物為主要作案工具，近年則愛用槍械，特別是高殺傷力作戰武器，例如紐西蘭基督城恐攻案恐怖分子即持用半自動霰彈槍及半自動步槍。

別讓民粹傷害民主

臺灣亦為民主國家，然近年來政黨對立面升高，民眾批判更加尖銳，為反對而反對，將民主變為民粹。觀看美國在政黨紛爭下，民粹凌駕民主後之慘況，臺灣人應戒之慎之，避免讓仇恨滲透進入你我日常，讓臺灣永遠成為居處全球動盪局勢中之最和平宜居的平行時空。