國家數位基礎建設-迎接量子運管時代

中興大學副教授－譚偉恩

國家數位基礎建設——迎接量子運算時代

◆ 中興大學副教授 — 譚偉恩

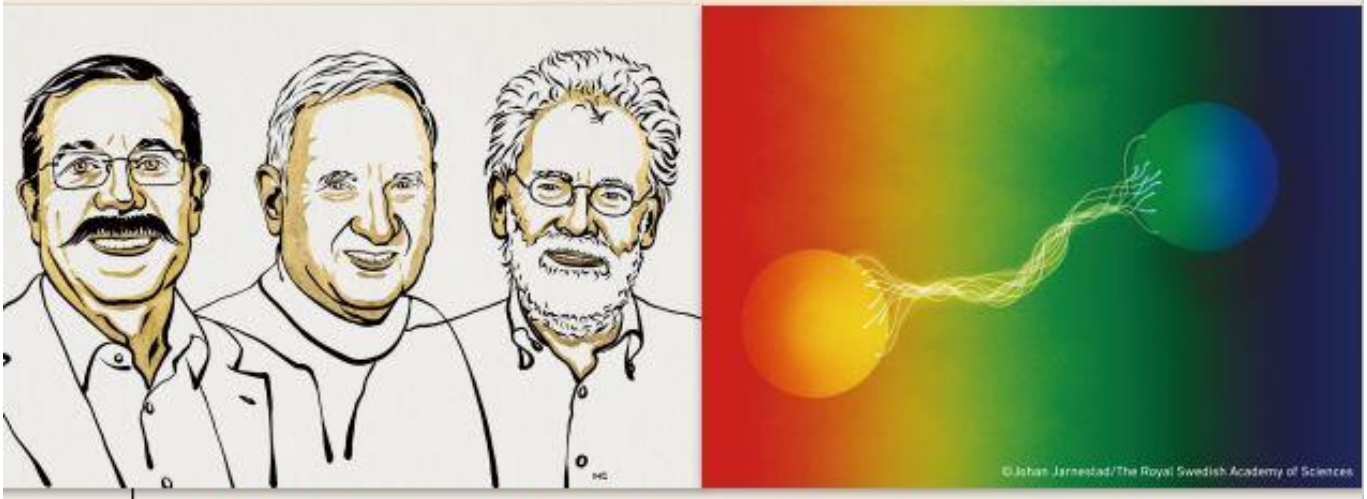
（Photo Credit: IBM Research, https://flic.kr/p/SrvZqe）

數位建設為我國「前瞻基礎建設計畫」的重點項目之一，[1] 思維上不再將基礎建設的定義侷限於硬體公共設施，而是將網路安全、資訊安全、數位文創等軟性設施列入國家基礎建設之範疇。

後疫情時代的數位發展

政府於「前瞻基礎建設 2.0」的推動計畫中，編列「數位建設」950 億元的特別預算，旨在發展後疫情時代的數位國家，並聚焦在雲端應用系統、第五代行動通訊技術（5G）、人工智慧（AI）及物聯網（IoT）等技術之升級和普及化。從安全研究（security studies）的角度觀之，上述的國家發展策略有助於臺灣整體競爭力的提升，但國民個人隱私與公私部門的資訊安全亦將面臨更高之風險。

[1] 國家發展委員會，《前瞻基礎建設計畫》，https://www.ndc.gov.tw/cp.aspx?n=608FE9340FE6990D。



2022 年諾貝爾物理學獎揭曉，由 3 位發現量子糾纏真實存在的科學家共同獲獎。量子糾纏效應可用於發展量子電腦，其超強運算能力，能夠在短時間內破解任何密碼，屆時 CI 的網路安全系統可能都不堪一擊。（Photo Credit: Nobel Prize Outreach, illustrated by Niklas Elmehed, https://nobelprize.qbank.se/mb/?h=a01ac2c0632b321a715b4cd9ff2438e6; The Royal Swedish Academy of Sciences, illustrated by Johan Jamestad, https://www.kva.se/en/news/the-nobel-prize-in-physics-2022）

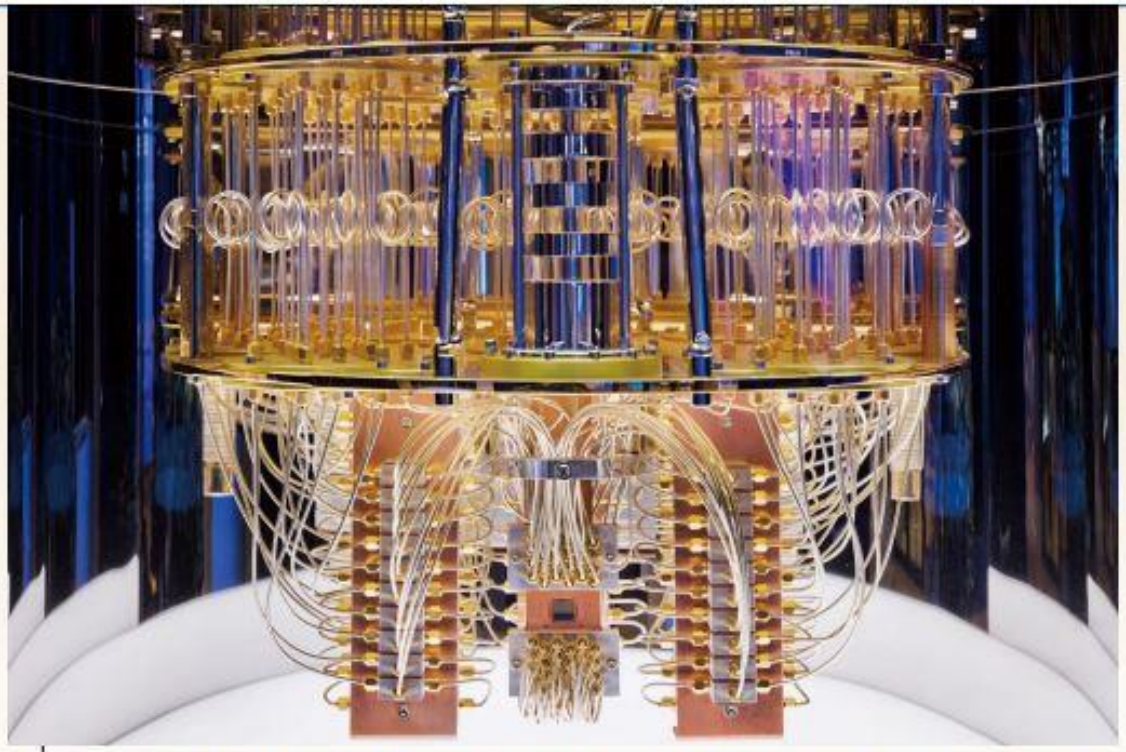
量子運算科技的美麗與哀愁

量子運算（quantum computing）使用的是量子位元（quantum bits / qubits），基於量子可能同時存在狀態 0 與 1，故可用一個線性組合來表示量子位元的疊加現象（superposition），理解上不妨想像一個量子位元的狀態可以是 90% 的機率為 1 與 10% 的機率為 0，兩種狀態同時存在。[2] 量子運算不僅可以對確定的值進行演算，也能同時對所有可能的疊加狀態進行演算，所以比傳統電腦的二進位計算方式有效率。

正因為如此，量子運算對於目前許多加密技術造成威脅，並對所有藉由加密技術而獲得保障之非公開資訊帶來很大的風險。舉例來說，非對稱式加密（asymmetric encryption）是透過兩個金鑰（公鑰與私鑰）進行加／解密，RSA 演算法即是屬於一種非對稱式加密。我國的自然人憑證便是透過 RSA 演算法來維護國人的個資，但在 2013 年前後，有量子運算與密碼學的研究者以 220 萬個 1024 位元加密的自然人憑證系統（新版使用 2048 位元）進行破密試驗，找出 103 個密碼是使用相同的質數（prime numbers）。

這個例子雖然已是過去式，且自然人系統的資安水平也大幅提升，但誠如美國國家標準暨技術研究院（National Institute of Standards and Technology, NIST）指出，量子運算會對現行常用的加密方式造成衝擊，因此重要的國家資料或檔案都需要開始準備一個新的密碼系統，來因應量子運算科技普遍化後的時代。

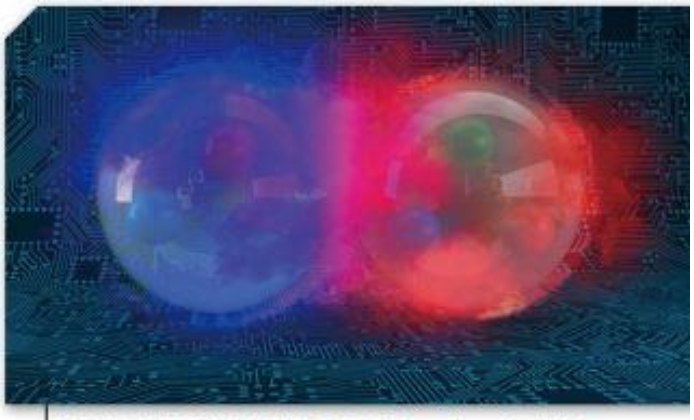
[2] 透過「量子疊加」及「量子糾纏」，量子運算科技創造出多種組合狀態，超越傳統電腦運算中非「0」即「1」的限制。



量子計算是利用量子力學的現象，例如疊加、干涉和纏結來做計算分析，能同時對所有可能的疊加狀態進行演算，所以比傳統電腦的二進位計算方式有效率；圖為 IBM 開發之 Q System One 內部系統，其為全球第一臺商業化的量子電腦。（Photo Credit: IBM Research, https://flic.kr/p/2jyFt2u）

積極治理是讓科技效益最大化的關鍵，並能緩解過程中的潛在風險。量子運算使用不同的物理原理（也就是量子力學）實現傳統電腦運算無法做到的資訊處理，例如模擬化學反應和物理過程，從而更快地進行新藥物與新材料的研發，還有提升 AI 的深度學習品質。然而，量子運算科技的應用也同時為資訊安全帶來風險，如果沒有相應的法規和治理措施（特別是風險預防），這麼尖端的科技有可能為一個國家帶來的損害多過於利益。

鑑此，迎接量子運算時代的國家數位基礎建設應具備兩點思考：一、技術面：軟體或硬體的強化，特別是用更強的加密機制來與量子運算抗衡。二、規範面：基於人類是理性選擇者，重視自我利益與效用最大化，政府的治理邏輯應該是先揭露量子科技在應用上的各種風險，甚至提供風險評估、風險分析、風險管理等三方面的資訊。



隸屬美國能源部的「橡樹嶺國家實驗室」（ORNL）為首次成功在量子電腦上模擬原子核的科學研究團隊，圖為氘氦質子（紅色）和中子（藍色）的束縛態。（Photo Credit: ORNL, Andy Sproles, https://flic.kr/p/KjE3QQ）

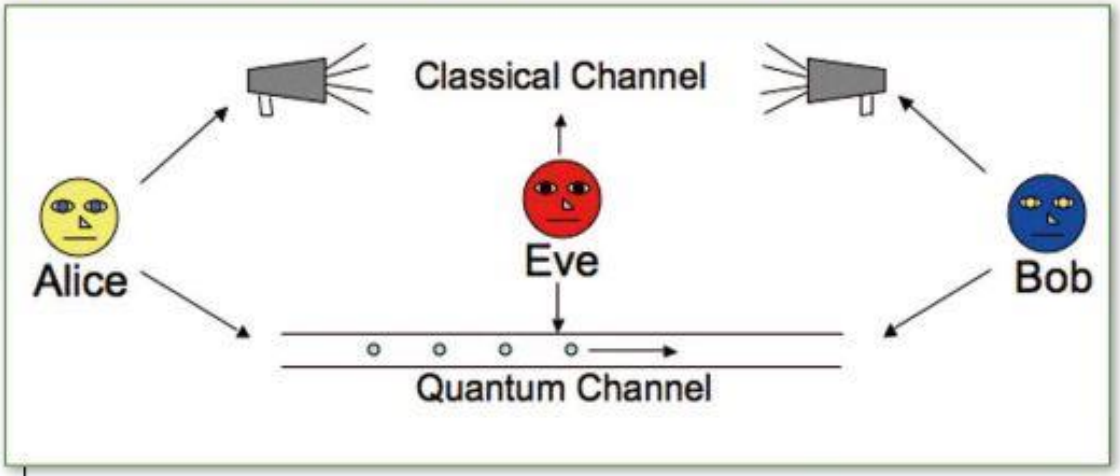
優化數位基礎建設應有的安全思維

新的加密模式在當前密碼學領域已成為熱點，目前用以取代傳統金鑰分發技術的模式主要有兩個：量子金鑰分配（Quantum Key Distribution, QKD）及後量子密碼學（Post-Quantum Cryptography, PQC）。

一、量子金鑰分配[3]

目前 QKD 已發展出若干協定及其衍生類型，但基本運作原理大致相同，即提供通訊雙方擁有一組可驗證彼此身分的傳統渠道（例如：公開的網路），以及一條可以傳送量子位元的渠道。QKD 協定開始時，通訊雙方先經由量子渠道傳送一連串的量子資訊，接著再經由傳統渠道比對資訊，藉以獲得所謂的共同金鑰。如果在協定運作與資訊傳送期間，未經核可的第三人竊得傳統渠道上的資訊或是對量子渠道中的資訊進行竊取，基於量子力學的資訊干擾理論及不可複製原理（no-cloning theorem），通訊雙方就會發現有第三人在進行資訊竊取的情況，[4] 甚至能夠計算被截獲訊息的數量。

美國大約在 2000 年前後開始建立國家級的 QKD 機制，是全球起步最早的國家，之後歐盟、日本、中國大陸等國開始跟進。然而，QKD 面臨的挑戰是，若使用光子作為量子位元的載體，在傳輸資訊時光子的能量會持續弱化，因此光子的有效傳輸距離大約只有 100 公里。要克服這個問題，有兩種方法；一是透過多陸面



量子金鑰分配是透過一組連接通訊雙方（Alice、Bob）、可驗證彼此身分的傳統渠道，以及一條可以傳送量子位元的渠道來進行比對運作，未經核可的第三人（Eve）若進行竊取，基於量子力學的資訊干擾理論及不可複製原理，通訊雙方會發現有第三人在進行資訊竊取的情況。（Source: Mart Haitjema, https://api.semanticscholar.org/CorpusID:18346434）

[3] 藉由單光子或糾纏的光子，在相隔一定距離的兩個地方建立共同密碼。本文先前提過，疊加態的特性讓量子呈現一種機率分布，技術上沒有辦法透過單一測量的結果將整個機率分布的情況演算出來，因此，如果能使用光子攜帶隨機的 0 跟 1 來作為金鑰，第三人就沒有辦法僅透過單一測量的方法來竊取密碼。

[4] Byoung Ham, "Unconditionally Secured Classical Cryptography Using Quantum Superposition and Unitary Transformation," *Scientific Report*, Vol. 10, No. 11687, https://www.nature.com/articles/s41598-020-68038-7.

臺灣清華大學前瞻量子科技研究中心團隊已運用清華大學與陽明交通大學的校園光纖網路，成功實測總長 3.44 公里的戶外光纖量子加密通訊；工業技術研究院亦將加入部署相關設備，預計在 2023 年前，形成三地、10 公里長的環狀量子網路。（圖片來源：國家科學及技術委員會，https://www.nstc.gov.tw/folksonomy/detail/44681061-7216-473d-a4d9-5104564e63ff?l=ch）

節點的「接續傳輸」來把距離拉長，二是借助衛星進行三角傳輸。[5] 臺灣目前關於 QKD 的技術與相關實驗始於 2019 年，傳輸距離尚在 100 公里以內。QKD 面對的另一個挑戰是，美國國家安全局（National Security Agency, NSA）及歐盟安全單位 ENISA（European Union Agency for Cybersecurity），均反對使用 QKD 作為加密機制。

二、後量子密碼學

與 QKD 截然不同，PQC 的原理是針對量子運算的「劣勢」去構思加密策略，它的技術是利用代數結構的特性來抑制量子運算的效能優勢。美國的 NIST 已於 2016 年啟動 PQC 標準化流程，隨著近幾年在相關標準上的完備化，美國政府公部門、民間私部門，還有其他國家應該會漸漸開始使用 PQC 的加密模式來迎接量子時代。報導指出，最新的 PQC 標準將於 2024 年左右臻於完備，而目前在 PQC 的相關專利名單中，前十大專利申請者有 7 個是來自中國大陸，這非常值得臺灣重視。[6]

結語

我國的《量子科技研究及發展條例》在 2020 年通過立法院的一讀程序後，緩慢進展，而量子運算的相關科技已無懸念成為工業大國相互競爭或建立合作的新領域。美國於 2018 年推出《國家量子倡議法案》（National Quantum Initiative Act），現任總統拜登也在 2022 年 5 月發布行政命令，推動國內量子相關科研活動，並制定因應量子運算可能對美國網路安全造成衝擊的國安計畫；南韓亦於 2021 年、2022 年先後將元宇宙和量子運算納入國家的基礎建設項目，值得我國借鑑。

[5] 歐美國家對此的相關研究於 2012 年開始，詳見：Tobias Heindel, et al., "Quantum key distribution using quantum dot single-photon emitting diodes in the red and near infrared spectral range," *New Journal of Physics*, Vol. 14, https://iopscience.iop.org/article/10.1088/1367-2630/14/8/083001/meta.

[6] 臺灣其實有頂尖的 PQC 專家和研發人材，在參與美國 NIST 密碼標準化或數位簽章的技術升級上表現亮眼，政府應重視這些寶貴的人力資源，給予研發與專利申請上的後援，詳見：楊柏因，《量子電腦發展對密碼學或資安的影響》，台灣網路講堂，2021 年 8 月 4 日，https://www.twsig.tw/wp-content/uploads/2021/12/ 楊柏因 _ 量子電腦發展對密碼學或資安的影響 _20210804-nii.pdf。

本文摘自清流雙月刊中華民國112年11月 號P17-P21

從「林志穎火燒車」看緊急救援

大學助理教授-趙萃文

從「林志穎火燒車」看緊急救援

◆ 大學助理教授 — 趙萃文

藝人林志穎日前發生火燒車事件，幸好被民眾迅速救出，惟輿論上卻也引發依現行法律若熱心民眾、醫護警消等不幸造成被救護者傷亡，是否須負刑事責任之疑慮。

短短一分鐘，生死一瞬間

男星林志穎於 7 月 22 日開著白色特斯拉戴小兒子出遊，不知為何車輛偏移，直接撞上分隔島，電線桿幾乎把車頭切成一半，短短幾秒鐘後，特斯拉即成火球。幸好出事地點旁邊工地有群熱心民眾，他們立即衝上去試圖滅火並將林志穎與副駕駛座上兒子救出，人救出後特斯拉車頭旋即陷入火海。短短一分鐘，生死一瞬間。這些勇敢英雄們不顧自身安危救援，才及時挽救林志穎父子性命。[1]

嗣後有知名醫生於臉書發文指陳：「法律應該放寬對救助人時產生的刑罰，否則賠不起的要怎麼衝去救人」，此議題再度

[1] 《林志穎車禍畫面曝　熱心民眾湧上協助救人》，https://tw.news.yahoo.com/news/ 林志穎車禍畫面曝 - 熱心民眾湧上協助救人 -050712748.html。

藝人林志穎於 7 月駕駛特斯拉自撞汽機車分隔島，引發火燒車事故，幸好現場民眾見狀，連忙將其與孩子救出。（圖片來源：桃園市政府消防局）

依《緊急醫療救護法》規定，在臺灣熱心伸出援手者可不負民、刑事責任；惟按〈刑法〉緊急避難規定，正當防衛、緊急避難在行為過當的情況下，仍會構成犯罪。

引發熱議，能帶來多大程度之修正與撼動，值得後續觀察。

遇難不敢救，誰讓社會冷漠

我國〈刑法〉第 276 條規定：「因過失致人於死者，處 5 年以下有期徒刑、拘役或 50 萬元以下罰金。」過失定義依〈刑法〉第 14 條：「行為人雖非故意，但按其情節應注意，並能注意，而不注意者，為過失。」惟「應注意，能注意，而不注意者」之判斷標準，學說上雖然參考德國〈刑法〉引入客觀歸責理論取代傳統相當因果關係說，該理論仍嫌空泛，個案上是否構成過失仍有待法官、檢察官依其自由心證而做判斷。

雖有部分學者提出，依 102 年新修正之《緊急醫療救護法》（下稱〈救護法〉）第 14 條之 2 規定：「救護人員以外之人，為免除他人生命之急迫危險，使用緊急救護設備或施予急救措施者，適用《民法》、〈刑法〉緊急避難免責之規定。」用以強調在臺灣熱心伸出援手者可不負民、刑事責任；惟按〈刑法〉第 24 條緊急避難規定：「因避免自己或他人生命、身體、自由、財產之緊急危難而出於不得已之行為，不罰。但避難行為過當者，得減輕或免除其刑。」細研〈救護法〉上開條文，僅係重複規定，所謂特別法毋寧純屬具文，無實質助益；更且〈刑法〉第 23 條正當防衛、第 24 條緊急避難在行為過當之情況下，仍會構成犯罪，至多只是「得」減輕或免除

其刑而已。目前司法實務見解相對較為保守，在正當防衛、緊急避難造成相對人死亡之情況下，或為保障死者家屬之民事求償權，率皆判決防衛過當或緊急避難過當。

司法實務對好心救護者，仍稍嫌嚴苛

就上開〈救護法〉第 14 條之 2 在判決書查詢系統以死亡結果搜尋，僅尋得一則判決即臺東地方法院 105 年度訴字第 161 號刑事判決，判示指出：「然縱被害人當時確有無呼吸、心跳之情事，被告為被害人實施人工心肺復甦術前，仍應注意觀察被害人之呼吸、脈搏是否已達應實施人工心肺復甦術之程度，並以正確之方式，依序胸部按壓、暢通呼吸道及檢查與維持呼吸……惟被告明知自己未學過醫療相關人工心肺復甦術急救程序，未具備相關急救能力，足以觀察評估被害人之呼吸、脈搏是否已達應實施人工心肺復甦術之程度，及以正確方式實施人工心肺復甦術，理應儘速撥打急救專線，等待專業人士到場為被害人進行人工心肺復甦術，且依被告年齡智識、生活經驗及當時情形，亦無不能注意之情事，被告竟捨此不為，而係擅自以右手握拳集中往心臟處捶打之錯誤方式，持續約 1 分鐘，對被害人為錯誤之急救行為，足見其避難行為已有過當，應堪認定。」可見目前我國司法實務對正當防衛、緊急避難過當之判斷似仍嫌稍微苛刻。

實施人工心肺復甦術前，理應儘速撥打急救專線，並注意觀察患者之呼吸、脈搏是否已達應實施人工心肺復甦術之程度。

其刑而已。目前司法實務見解相對較為保守，在正當防衛、緊急避難造成相對人死亡之情況下，或為保障死者家屬之民事求償權，率皆判決防衛過當或緊急避難過當。

司法實務對好心救護者，仍稍嫌嚴苛

就上開〈救護法〉第 14 條之 2 在判決書查詢系統以死亡結果搜尋，僅尋得一則判決即臺東地方法院 105 年度訴字第 161 號刑事判決，判示指出：「然縱被害人當時確有無呼吸、心跳之情事，被告為被害人實施人工心肺復甦術前，仍應注意觀察被害人之呼吸、脈搏是否已達應實施人工心肺復甦術之程度，並以正確之方式，依序胸部按壓、暢通呼吸道及檢查與維持呼吸……惟被告明知自己未學過醫療相關人工心肺復甦術急救程序，未具備相關急救能力，足以觀察評估被害人之呼吸、脈搏是否已達應實施人工心肺復甦術之程度，及以正確方式實施人工心肺復甦術，理應儘速撥打急救專線，等待專業人士到場為被害人進行人工心肺復甦術，且依被告年齡智識、生活經驗及當時情形，亦無不能注意之情事，被告竟捨此不為，而係擅自以右手握拳集中往心臟處捶打之錯誤方式，持續約 1 分鐘，對被害人為錯誤之急救行為，足見其避難行為已有過當，應堪認定。」可見目前我國司法實務對正當防衛、緊急避難過當之判斷似仍嫌稍微苛刻。

實施人工心肺復甦術前，理應儘速撥打急救專線，並注意觀察患者之呼吸、脈搏是否已達應實施人工心肺復甦術之程度。

別讓見死不救者，找到藉口

常言道：「臺灣最美麗的風景是人」，此言非虛。〈刑法〉過失犯之判斷，從法益衡量觀點，某一行為是否製造不受容許之風險，可從此一行為所提供之社會利益大小來判斷；凡帶有極大社會利益之行為，所容許之風險範圍自然更寬。故警消值勤、醫護救護或熱心民眾救援帶來之傷亡風險，**只要不是出於故意，皆應給予最大限度之寬容**。

當然，伸出援手救人者亦不能忽視醫療上應有之基本注意義務，由於現行〈刑法〉思潮並不禁止有利於行為人之類推適用，放大來看，或可直接類推《醫療法》第 82 條規定：「醫事人員執行醫療業務因過失致病人死傷，以違反醫療上必要之注意義務且逾越合理臨床專業裁量所致者為限，負刑事責任。」讓熱心助人之民眾只有在重大過失且輕率情況下，始負刑事責任，對善良助人者所涉法律爭議，若能朝有利方向推敲，當可創造美善和喜悅。果如是，方能寄望有人為實踐正義而努力不懈，熱心助人者才不致於心灰意冷，見死不救者也不會找到更堅強的藉口。

值得借鏡的「好撒馬利亞人條款」[2]

觀諸國外法例，德國社會較重視社會倫理，其立法者認為，與事故不相關之第三人，亦應課予災害發生一定之救助義務，

帶有極大社會利益之行為，所容許之風險範圍應更寬，警消值勤、醫護救護或熱心民眾救援帶來之傷亡風險，只要不是出於故意，皆應給予最大限度之寬容，熱心助人者才不致於心灰意冷。（圖片來源：花蓮縣政府 0918 震災資訊專區，https://0918.hl.gov.tw/News_Content.aspx?n=30969&s=103060）

[2] Good Samaritan law 源自於《聖經．路加福音》耶穌基督的寓言：一個猶太人被強盜打劫，受了重傷，躺在路邊，雖有不少人路過，但都不聞不問；唯有一位撒馬利亞人路過，不顧族群隔閡，動了慈心照應他，並自己出資讓猶太人到旅店休息，因此被稱為「好撒馬利亞人」條款。在美國和加拿大，此法是給自願救助傷患者免除責任的法律，在於使人做好事沒後顧之憂；而在其他國家亦要求公民有義務幫助遭遇困難的人，而德國更有法例規定，有能力但未提供協助是違法行為。https://zh.wikipedia.org/wiki/好撒馬利亞人法。

「好撒馬利亞人條款」命名源自《聖經》見義勇為的故事，設立目的在使人做好事沒後顧之憂。
（Created by Pelegrí Clavé, 1838）

故制定德國〈刑法〉第 323 c 條不為救助罪（「好撒馬利亞人條款」），明定：「於意外事故或公共危險、或危難發生時，如行為人之救助實屬必要，依當時情況又屬可期待，尤其對行為人自己並無顯著危險且不違反其他重大義務，卻**不救助者，處 1 年以下有期徒刑或罰金**。」本條為道德化之刑罰條款，強調行為人救助之期待可能性，以限制其處罰要件，且法定刑不高，雖德國實務上大多僅處以罰金刑，但仍具重大象徵意義。

綜上所述，我國人民雖古意而樂於助人，惟近來新聞上卻也時常可見凶殺、性侵等重大刑案，圍觀民眾見死不救或視若無睹之情況，有些世風日下；立法者在立法政策中，允宜反覆表達出對友誼、信任、同情心及正義感等道德情感之重視與發揚，才能讓國人有足夠情感動機去見義勇為。上述德國〈刑法〉第 323 c 條之不為救助罪，考慮可謂極其周延，或可供我國修法時之抉擇取捨。

本文摘自清流雙月刊中華民國112年11月 號P57-P61