doi: 10.29843/JCCIS.202601_(50).0003

台灣民眾對網路攻擊的風險感知與政策態度

施琮仁

摘要

網路攻擊已成為各國共同面臨的國家安全挑戰，網路恐怖主義的核心目標在於透過灌輸恐懼與脆弱感，削弱民眾的韌性，動搖其對政府防禦能力的信心。這類攻擊所引發的不安，不僅威脅國家安全，也侵蝕民眾的數位福祉，危及公眾公平、安心地近用網路服務的權益。瞭解民眾對此議題的認知與風險意識，以及其對政策與民主價值的影響，因而成為亟需探討的課題。本研究從風險感知的觀點出發，結合媒介效果與決策理論，探討網路攻擊事件是否會削弱民眾對政府的信任，並影響其對強硬政策的支持。

根據 TWNIC 2024 年調查（N=2,147），多數民眾對具體攻擊事件並不熟悉，僅約四成相信政府有能力有效應對。然而，民眾普遍不認同政府應以監控電話、電子郵件或社群媒體等手段維護資安，也不支持對發動攻擊的國家採取報復措施，顯示人們不願為安全而犧牲隱私等基本人權與民主價值。研究亦發現，政治信任是影響政府應對信心與強硬政策支持的關鍵因素，而政策知識能增強民眾對政府應對能力的信任。政府若能透過健全法規與資訊透明，展現積極作為，將有助於提升公眾信任，並促進整體社會的數位福祉與韌性。

⊙ **關鍵字：基礎設施、網路攻擊、網路安全、應對信心、強硬政策支持、數位福祉**

⊙ **本文作者施琮仁為國立政治大學國際傳播英語碩士學位學程教授。**

⊙ **聯絡方式：**Email：tjshih@nccu.edu.tw；**通訊處：**116302 臺北市文山區指南路二段64號 國立政治大學傳播學院。

⊙ **收稿日期：**2025/04/10　**接受日期：**2025/12/17

Public Perception of Cyberattacks and Policy Attitudes in Taiwan

Tsung-Jen Shih

Abstract

Cyberattacks have become a pressing national security challenge worldwide. The core objective of cyberterrorism is to instill fear and vulnerability, thereby weakening public resilience and undermining citizens' confidence in the government's ability to protect them from future attacks. Such threats not only endanger national security but also erode citizens' digital well-being, jeopardizing their right to fair, secure, and reliable access to online services. Understanding how the public perceives and evaluates cyber threats, and how these perceptions shape their policy preferences and democratic values, has thus become an urgent research agenda.

Drawing on the perspectives of risk perception, media effects, and decision-making theories, this study examines the mechanisms through which cyberattack incidents may undermine trust in government and shape public support for hardline policies. Based on the 2024 TWNIC national survey (N = 2,147), results show that most citizens are unfamiliar with specific cyberattack incidents, and only about 40% believe the government is capable of handling future attacks. While citizens call for stronger responses, they largely oppose government surveillance or retaliatory measures, reflecting a reluctance to sacrifice human rights and democratic values in the name of cybersecurity. Political trust emerges as the strongest predictor of both confidence in government response and support for hardline policies. Strengthening cybersecurity legislation and improving government transparency may therefore enhance public trust, resilience, and overall digital well-being.

⊙ Keywords: Infrastructure, Cyberattacks, Cybersecurity, Confidence, Support for Hardline Policies, Digital Wellbeing

⊙ The author, Tsung-Jen Shih is a Professor of the International Master's Program in International Communication Studies at National Chengchi University

⊙ Corresponding author: Tsung-Jen Shih, email: tjshih@nccu.edu.tw; address: No.64, Sec.2, Zhinan Rd., Wenshan Dist., Taipei City 116302, Taiwan (R.O.C.)

⊙ Received: 2025/04/10 Accepted: 2025/12/17

壹、研究緣起

2016 年美國總統大選期間俄羅斯所進行的網路攻擊，突顯了網路作戰在國家國家安全中扮演了日益重要的角色，也引起了各國政府對於網路軍事操作（cyber operations）的重視。在亞洲，日本防衛省旗下的防衛研究所於 2022 年發布了新版的《中國安全保障報告》。該報告透露，中國在一年內針對台灣發起了超過 14 億次的網路攻擊，並通過偽裝手法向台灣傳播有害信息。報告特別指出，中國利用非軍事方式所進行的認知作戰，對台灣構成了「重大挑戰」（林翠儀，2022）。

這類的網路攻擊已被定義為「國家級駭客威脅」，一方面是因為攻擊的層面遍及社會各個層面，包含通訊傳播、交通、國防供應鏈等。例如，馬偕醫院與彰化基督教醫院接連於 2025 年初受到網路攻擊，導致出現院外掛號系統失靈及電腦病例無法開啟之情事（曾以寧，2025）。另一方面，近來的國家安全研究報告也指出，許多網路駭客其實都直接受國家指揮、背後亦有國家資源的支持，使其行動更具備組織性與策略性（羅正漢，2025）。因此，確保整體國家或個別民眾的網路安全，是當前刻不容緩的任務。

事實上，數位安全（包括網路威脅與個資濫用）已被經濟合作暨發展組織（OECD）列為評估「國民數位福祉（digital wellbeing）」的十一項重要指標之一，是造成數位風險、降低數位機會的關鍵因素（OECD, 2019）。數位福祉指的是人們在數位環境中，能夠以健康且平衡的方式使用各種數位設備與網路服務；亦即在享受數位科技所帶來的便利與效益的同時，也能避免其可能造成的負面影響與風險（Vanden Abeele, 2021）。

面對日益頻繁的網路攻擊及其對數位福祉的影響，學界已開始關注此一主題，相關實證研究也逐漸累積。然而，相關研究在早期多聚焦於個人層級的威脅，例如身份盜用、帳號遭竊、個資外洩等，或是金融詐騙（Montañez, Golob, & Xu, 2020；Van Schaik, Jansen, Onibokun, Camp, & Kusev, 2018；Van Schaik et al., 2017），直到近年才逐漸將視角擴展至外部勢力意圖顛覆政權或破壞民主的攻擊行為，部分民主國家的政府也開始陸續發布相關報告（Jaikaran, 2025）。實際上，網路攻擊的類型多樣，涵蓋從竊取資訊、散布假訊息到癱瘓系統等不同層面，若未加區分而一概而論，可能導致

研究結果偏誤。其中，「破壞性網路攻擊」（degradative cyber-attacks）特指那些目的在於削弱或摧毀重要設施之網絡、運作或功能的行動，對社會與國家安全的潛在衝擊尤為重大。然而，目前針對此類攻擊的公眾感知與風險認知研究仍相當有限。本研究因而聚焦於破壞性網路攻擊，期望補足現有文獻在此面向的不足，並深化對民眾實際感受與認知反應的理解。

雖然網路攻擊不像戰爭或恐怖攻擊一般，會直接破壞環境、設施或造成傷亡；然而，網路攻擊會藉由癱瘓一個國家的基本運作，使人民的生活受到不便或人身重要資料受到威脅，讓社會進入一個較為緊急的狀態。過去研究顯示，在國家整體面對威脅時，政府會因為需要處理危害而制定對人身自由較為限縮的政策，而人民為了將低風險，對於這類限縮自由的政策亦有較高的接受度。例如，美國在 2001 年 911 恐怖攻擊之後不久便頒布「愛國法案」（The USA Patriot Act），賦予美國政府很大的權限得以監控人民的通訊與財務交易活動，而人們對此政策亦展現高度的配合（Goitein, 2021）。類似狀況也發生在新冠肺炎疫情期間，許多國家為了防疫而採取宵禁、限制行動或追蹤足跡等強化政府監控之措施（Snider, Shandler, Zandani, & Canetti, 2021）。

這類民主緊縮政策或許在緊急情況下確有需求，但擴張政府權力、限制人民自由以因應危機的手段，亦可能讓人們懷疑民主制度的效率與作用，特別是對於那些原本就對民主、選舉或政治人物抱持懷疑態度的民眾，他們因此更有理由認為民主體制運作不良（Kotze, 2022）。研究已經指出，接觸網路攻擊會讓民眾產生較為強硬、好戰的政治態度；加劇暴力衝突，以及偏好會犧牲個人自由的嚴格法律（Kreps & Schneider, 2019），甚至腐蝕對民主的信念。因此，瞭解網路攻擊的在人民眼中的嚴重性，以及對民主價值可能產生的影響，讓人們在遭受未來新型態網路攻擊時，能有應對或復原能力（Dacorogna & Kratz, 2023），實為必要且急迫的課題。

值得注意的是，雖然部分研究已逐漸揭示網路攻擊對民眾心理感知的影響，但相關發現多源自實驗設計。有學者對此提出質疑，認為在高度控制的實驗情境中所得結果，未必能充分推論至真實世界（Shandler & Gomez, 2023）。因此，他們主張應以實際發生的網路攻擊事件為依據，探討民眾的真實感受。本研究採用調查法，針對兩起發生於台灣之真實網路攻擊事件詢問民眾的熟悉度，不僅具備較高的外在效度，也回應了上述學者的呼籲。

整體而言，本研究主要的目的在探討網路攻擊事件是否真能瓦解民眾對政府的信心，以及對於強硬政策的支持，並特別關注政治信任與網路媒體參與的調節作用。政治信任是影響民眾對政府及政策態度重要的預測變項，研究顯示，越信任政府的民眾，越願意配合政府所提供的疫情行為指引，做出行為改變（Oksanen et al., 2020; Robinson et al., 2021），也較為傾向支持限縮公民自由的政策（Vasilopoulos, McAvay, Brouard, & Foucault, 2023）。但另一方面，政治信任與政策態度之間的關係，也可能受到其他因素的影響。例如，通常政治信任越高的民眾，越能接受政府犧牲個人自由以因應外部威脅，然而當外部威脅引發較強烈的恐懼感時，反而是政治信任較低的民眾對該類政策展現較高的支持（Vasilopoulos et al, 2023）可見政治信任的作用可能會因為不同的危害情境而有差異。

本研究亦側重網路媒體使用的原因，是因為網路平台在危機事件中通常是民眾主要的訊息來源，且和人們的風險感知、預防行為皆有緊密關係（Zeballos Rivas et al., 2021）。然而，在網路攻擊的情境中，網路媒體一方面作為提升風險意識的吹哨者，另一方面也是造成風險的來源之一，其角色值得更深入探討。

為了理解前述變項間複雜的關係，本研究結合幾個和媒體效果與風險感知相關的心理理論，特別是建構層級理論、歸因理論與評估傾向理論，一方面可以彌補過去研究偏重現象描述、缺乏理論連結的不足（Shandler & Gomez, 2023）；另一方面也能更清楚描繪民眾在面對破壞性網路攻擊時的心理歷程—從距離感到歸因再到情緒反應，深化政策制定者或風險溝通者對於民眾風險感知與態度形成過程的理解。

貳、文獻探討

一、風險意識與風險感知

雖然在有些研究中，風險意識與風險感知經常被視為類似概念且交替使用 (例如，Bradford 等人，2012)，但本研究將兩者加以區分，認為兩個概念在本質上有所不同。風險意識指的是人們對威脅事件所有基本的認識，包含擁有的資訊與知識 (Gibson, 2003)；風險感知則是對自身受到威脅事件影響與否的綜合判斷 (Slovic &

Peters, 2006)。兩個概念不見得會有相關性，例如，民眾可能知覺氣候變遷正在發生，但不認為自身會受到影響，此即為具有風險意識，風險感知卻低的案例。Cisternas, Cifuentes, Bronfman, & Repetto（2024）的研究也發現，風險意識、風險感知對於自然災害防備意圖各自有不同的關係，因此認為此二概念不應被混為一談。延續此邏輯，本研究將風險意識定義為網路攻擊事件的熟悉度。

風險意識與風險感知的關係，可以從建構層次理論（Construal Level Theory）的概念來理解，該理論認為，人們對風險事件的反應，取決於其對該事件的心理想像。心理距離感較接近的事件，人們會以較為具體的方式理解，而在記憶中保留較多的細節。相較之下，對於心理距離較遙遠的風險，人們通常會以較抽象的方式來建構之，因此在記憶中只會保留較為主要、高層次的概念（Trope & Liberman, 2010）。

基於前述論點，人類對於具體的事件較能產生直觀感受（意即低建構層次），因而較容易採取行動，但對於抽象、未來的事件則需花費較多的心理建構的過程來理解，故認知和行為的連結較為薄弱。因此，相較於具象思考，抽象思考會讓民眾低估風險事件發生的機率（Lermer, Streicher, Sachs, Raue, & Frey, 2016; Wakslak, Trope, Liberman, & Alony, 2006）。例如，若人們有受到氣候變遷影響的具體經驗，或是認為氣候變遷會造成立即的危害，則較可能相信氣候變遷的存在、採取因應行為（Chu & Yang, 2020），以及氣候政策（Chu, 2022）。

過去研究亦發現，若人們對於風險事件感到懼怕，由於情緒是對於威脅事件的直接感受，屬於低建構層次的理解，故較可能支持對風險的應對政策或手段；相反地，若人們對風險事件感到懷疑，則較難產生因應行為或配合相關政策，因為懷疑屬於高層次的理解。

在網路攻擊的情境下，若民眾能察覺到網路攻擊的具體事件（亦即風險意識高），則容易產生較高的風險感知。因此，本研究提出以下假設：

H1：民眾對網路攻擊的事件熟悉度和風險感知有正面關係。

熟悉網路攻擊事件與公眾對政府與政策的態度有著複雜的關係。一方面，事件熟悉度會降低公眾對政府應對能力的信心；另一方面，卻可能促使人們支持更為強硬的政策，例如加強監控與報復。這兩種看似矛盾的態度，或許能從公眾在面對網路威脅時所產生的心理與政治反應來解釋。

然而在論述之前，有必要先定義本研究所採用的依變項。「政府信心」指的是人們對政府、領導人或國家安全部門是否具備預防與減輕未來網路攻擊、並維持國家正常運作能力的主觀評價（Shandler & Gomez, 2023）。而「強硬政策」則意指政府為了降低風險與回應威脅，而採取具強制性、懲罰性或安全優先取向的措施，包括擴張監控、加強社會控制，或對外部威脅採取報復性行動等（Huddy, Feldman, Taber, & Lahav, 2005）。

當公眾越是了解網路攻擊事件，他們對政府應對危機的能力就越沒有信心。因為當一個成功的網路攻擊（例如大規模資料外洩或關鍵基礎設施受損）被廣泛報導時，民眾會將此視為政府的失敗。他們期望政府能夠保護國家和個人，但攻擊的發生卻顯示出防禦的漏洞。這種認知落差會削弱公眾對政府的信任，讓他們覺得政府缺乏足夠的專業知識或資源來抵禦未來的威脅，進而對政府的應對能力產生疑慮。Shander 與 Gomez（2022）的研究發現支持了這樣的論述，其結果指出，知悉網路攻擊事件的民眾，對於政府較不具備信心。

儘管公眾對政府的信心可能降低，但對網路攻擊的熟悉感卻會增加他們對強硬政策的支持，例如實施更嚴格的監控和採取報復行動。當個人資料或公共服務因網路攻擊而受到威脅時，人們會產生強烈的焦慮與不安，並希望政府能採取果斷措施來恢復安全感。為了換取更多的安全，公眾可能會願意犧牲部分個人隱私，支持政府進行更廣泛的監控，因為他們認為這是預防未來攻擊的必要手段。此外，對於某些具體且後果嚴重的網路攻擊，公眾可能會產生強烈的憤怒與復仇情緒，進而要求政府採取報復性行動。這種情緒化的反應，往往會促使公眾支持那些能夠展現政府力量與決心的強硬政策，無論這些政策是否為最理性的選擇。關於風險意識與限縮自由政策的關係，在健康傳播領域，有研究發現若民眾意識到喝酒與癌症之間的關聯性，便覺有可能支持相關的禁酒政策（Bates 等人，2018）。Snider 等人（2021）亦發現，有接觸網路攻擊資訊的民眾，較有可能支持網路安全相關政策，即便有些政策可能會犧牲既有之公民權利。

因此，本研究提出以下研究假設。

H2：民眾對網路攻擊的事件熟悉度與（a）政府應對信心有負面關係及（b）強硬政策支持度有正面關係。

二、風險感知、政府信心與政策態度

風險感知指的是一般大眾對風險的直覺或主觀判斷（Kung & Chen, 2012）。風險感知的概念認為，一般民眾可能會依據與專家不同的邏輯來判斷風險，例如依賴較多的個人經驗、情緒、媒體報導或文化價值觀，而非僅依賴風險事件發生的機率（Slovic, Fischhoff, & Lichtenstein, 1976；Slovic & Peters, 2006；Wildavsky & Dake, 1990）。風險研究學者認為，人們感知風險的方式至關重要，因為它不僅影響應對行為，還會影響對特定科技、政策和規範的接受程度 (Siegrist & Árvai, 2020)。特別是許多健康行為相關理論，都假定風險感知是促發降低風險行為的重要前置因素（Brewer, Weinstein, Cuite, & Herrington, 2004）。值得注意的是，風險感知的作用，可能因情境、議題而有差異，也可能會和不同的依變項有不同的關係。和一般健康或科學領域之研究不同，本研究所關注的是民眾對政府未來應對網路攻擊的信心，以及是否願意為了保障國家安全而妥協既有之民主價值（不論是在國內政策治理上或國際關係上）。

在網路攻擊的情境下，風險感知和政府應對信心的關係，可以從歸因理論（Attribution Theory）的角度加以解釋。該理論認為，人們會試圖將事件的成因歸結於特定的行為者或情境（Weiner, 1985），而相較於傳統的軍事攻擊或恐怖攻擊，網路攻擊的發起者常常匿名且難以追蹤（De Bruijn & Janssen, 2017），導致民眾難以明確地將責任指向具體的行為者（如某個國家、組織或個人）。在缺乏明確歸因對象的情況下，民眾傾向於將責任轉嫁至他們認為最有能力且最有義務提供保護的角色（亦即政府）。這種傾向源自於社會對政府的角色期待：政府被視為保護人民的重要防線，應能防禦各種形式的威脅，包括高度複雜的數位攻擊。因此，當攻擊成功時，無論真正的攻擊者身分是否明確，民眾都容易將事件解讀為政府的失職、準備不足或應變不力，進而削弱對政府的信任與信心（De Bruijn & Janssen, 2017）。

除了歸因機制外，情緒反應同樣能解釋為何風險感知的升高會削弱民眾對政府應對能力的信心。研究顯示，當民眾感受到高度風險時，常會伴隨焦慮與憤怒兩種主要情緒（Lerner & Keltner, 2001）。焦慮源於不確定性與缺乏控制感，會驅使人們尋求更多資訊與保障，若人們試圖找尋更多的防護資訊而不可得，便可能認為政府沒

有盡到應盡之責，而降低對有關單位的信心。另一方面，憤怒則與責任歸因密切相關（Quigley & Tedeschi, 1996）。當民眾因攻擊事件而感到憤怒，卻無法明確指認攻擊者時，他們更可能將責任投射到政府身上，認為政府在預防或應對上失職，導致信任感下降。Wagner （2014）以英國 2000 年初的財政危機為案例，發現民眾若是認為某個機構或個人應該為此危機負責，便可能有較高的憤怒感，而認為當時執政的工黨政府應該負責的民眾，則容易特別憤怒。

在強硬政策的支持方面，根據 Appraisal Tendency Framework（ATF），憤怒源自於人們對事件的「確定性」與「可控性」的認知評估，並帶有一種懲罰性的行動傾向（Lerner & Keltner, 2001）。在網路攻擊的脈絡下，憤怒會驅動民眾偏好更具強制性的政策，以達到報復與重新掌控局勢的目的，例如對加害者進行報復性行動，或透過擴大監控來預防與懲治潛在威脅。Canetti-Nisim, Ariely, & Halperin（2008）針對以色列的兩個少數族群進行研究，發現民眾若是認為此二族群對於社會有安全的威脅（亦即風險感知），則較可能支持較為排他性的政策。而 Davis 與 Silver（2004）以 911 恐怖攻擊為背景的研究也發現，風險感知愈高的民眾，愈願意在既有的公民自由權利上做出讓步。根據前述文獻，本研究提出以下研究假設。

H3：民眾對網路攻擊的風險感知與（a）政府應對信心有負面關係，但與（b）強硬政策支持度有正面關係。

除了檢視變項間的直接、間接關係，本研究亦探討兩組可能的交互作用關係，分別是政治信任與網路媒體參與的調節角色。此二變項分別代表了訊息處理模式中的兩條路徑—捷思式訊息處理與系統式訊息處理。捷思式的訊息處理靠著簡單準則的運作，讓人們得以快速、有效地做出決策，而系統式的訊息處理則是一種「全面且分析性的思維方式，在此過程中，人們會檢視並評估所有資訊的相關性與重要性，並將有用的資訊加以整合，以作出判斷」（Chaiken, Liberman, & Eagly, 1989, p. 212)。

而決定人們採取何種認知途徑的重要關鍵，在於能力與動機，若人們具有推論、分析資訊的能力，並具有資訊尋求的動機，便較有可能採取系統式訊息處理，反之則較可能依賴捷思（Petty & Cacioppo, 1986）。在網路攻擊的情境下，風險感知一方面提供了人們尋求更多資訊以解決問題的動機，另一方面卻也可能造成資訊迴避，促使民眾依賴認知捷徑，來幫助自己理解問題及找出解決方式，如風險訊息尋求與處理理

論所揭示（Yang & Kahlor, 2013）。因此，本研究結合訊息處理理論與風險訊息尋求與處理理論，檢視和風險感知可能產生交互作用的變項，在系統式訊息處理方面，本研究以網路資訊參與（包含資訊接收與表達）為代表，而在捷思式訊息處理方面，則著重政治信任的角色，以下兩小節將分別針對此二概念進行深入討論。

三、政治信任的調節作用

政治信任是在公共事務領域研究中用來預測民眾態度的重要變項，通常也具有顯著的影響力。政治信任的定義有三種不同的途徑，第一是表現取徑（performance-based approach），著重的是民眾對政府能力的評估，例如政府對災難事件的處理，會影響民眾對政治機構的信心 （Hibbing & Theiss-Morse, 2001）。第二是過程取徑（process-based approach），強調影響政府施政表現的過程；第三則是廉潔取徑（probity-based approach），此觀點側重政府單位的清廉與透明程度，若政府出現貪污或醜聞等情事，政治信任便會下降（Chanley, Rudolph, & Rahn, 2000）。因此，政治信任可以說是人民對政府表現、施政過程以及廉能程度的評估（Lim & Moon, 2020）。

現有研究主要將政治信任視為一種認知捷徑（heuristics），幫助人們理解複雜的公共事務（Rudolph, 2017）。政治信任之所以對政治態度、政策支持或選舉行為有顯著的影響力，係因民眾通常不具備足夠的知識或動機來做出政治決策（Chen & Chaiken, 1999）。過去研究顯示，認知捷徑不僅會直接影響民眾的態度，也會影響人們如何解讀訊息，使得同樣的訊息產生不同的意義（Kahan, Braman, Slovic, Gastil, & Cohen, 2009)。因此，越來越多的研究開始關注認知捷徑的調節作用。例如 Lim 與 Moon（2020）發現公民倫理（意指對他人或公共利益抱持誠懇與尊重的態度）和支持課徵環境稅有正面的關係，而此正向關係對於政治信任較高的民眾又更為強烈。政治信任的調節作用也發生在集體的分析層次中，Kulin 與 Johansson Sevä（2021）的研究發現，對氣候變遷的關切（concern）與氣候政策支持度的關係，在高政治信任的國家中較為強烈。

政治信任的調節方向，可以透過價值犧牲理論（ideological sacrifice theory）來推導，該理論認為，政治信任作用的強弱，取決於人們需要在物質上或價值上付出多少

的犧牲，故也稱為成本假說（cost hypothesis）。舉例而言，在美國，相較於共和黨，民主黨較爲支持疫苗政策；因此，對民主黨支持者而言，政治信任並非重要的態度影響因素。相反地，共和黨員若要支持疫苗政策，便要犧牲自己一直以來所抱有的價值觀，此時政治信任便會扮演較大的角色（Lim & Moon, 2020）。在社會福利政策上，過去研究也發現類似的模式，因為民主黨員向來較為支持此類政策，故不論政治信任程度的高低，其態度偏差幅度不會太大；但對共和黨員來說則必須犧牲其意識形態，僅有政治信任高的共和黨員會傾向支持社會福利相關政策（Rudolph & Popp, 2009）。

因此，根據價值犧牲理論，對於網路攻擊具有較高風險感知的民眾，可能對政府如何應對有較高的期待，即便是限縮自由或報復性之政策，不論政治信任程度的高低，此關聯性皆會存在。另一方面，風險感知低者會認為強硬政策非屬必要，若要支持此類政策則必須犧牲其原本的價值信念（亦即網路攻擊對台灣而言並非嚴重威脅），此時便需要較高的政治信任來彌補。因此，風險感知和強硬政策支持度之間的關係，可能會因為政治信任而有不同。一篇關於 911 恐怖攻擊的研究顯示，一般而言，民眾的風險感知愈高，愈可能支持限縮自由的政策，但是這個關係會受到政治信任的調節。換言之，政治信任愈低的民眾，愈無法接受以自由換取安全（Davis & Silver, 2004）。

風險感知和對政府應對信心之間的關聯性，也可能會受到政治信任的調節。若民眾對網路攻擊感到高度威脅，對政府亦有一定程度的信任，則可能對政府的應對能力有較高的信心。反之，若感受到威脅，但政治信任卻低，則會對政府較不具信心。

雖然根據前述推導，政治信任的調節作用看似明顯，然而過去研究也發現，價值犧牲的現象會因議題而異，且主要會發生在民眾覺得重要、和自身相關的議題上，此論點稱為顯著性假說（Devine, 2024）。由於在台灣和網路攻擊相關的民意調查才剛開始累積，民眾意見取向未明，故本研究以研究問題的形式來探究政治信任的調節作用。

研究問題 1a：風險感知與政府應對信心的關係，是否會因為政治信任程度而不同？

研究問題 1b：風險感知與強硬政策支持的關係，是否會因為政治信任程度而不同？

四、網路媒體參與的調節作用

當談論到媒體使用與風險感知的關係時，風險的社會放大理論（SARF）是經常被引用的理論基礎。SARF 的發展主要是為了理解風險事件在社會情境中的動態關係，特別是事件嚴重性和社會關注之間的落差。換言之，為什麼有些專家認為不嚴重的風險會受到社會關注，而有些危害較大的風險反而沒有受到重視（例如車禍、吸菸等）？該理論認為，解釋認知落差的一個重要關鍵，是了解風險資訊的傳播過程。仔細來說，一個風險是否會受到重視，取決於其形成的過程中受到多少的傳遞與詮釋，而社會中存在著許多「放大站」（包涵媒體、風險管理機構、公民團體、個人網絡等），他們扮演著過濾資訊、包裝資訊，以及賦予風險事件意義的角色（Kasperson, Kasperson, Pidgeon, & Slovic, 2010）。

大多數引用風險的社會放大理論作為基礎的研究，皆將媒體使用視為影響風險感知或態度的因素。例如，Binder, Scheufele, Brossard, & Gunther（2011）研究美國民眾對國家生物和農業防禦設施戰略計畫（National Bio and Agro-Defense Facility）選址的風險與利益感知，結果指出，對公共事務新聞越關注的民眾，對此事件的風險感知也越高。在英國，Frewer, Miles, & Marsh（2002）運用長期的民意調查資料，發現了民眾風險感知程度的高低與基因改造食品的媒體報導量多寡，具有有一致的關係。作者們也發現，相較於人們熟悉的風險，新型的危害由於資訊有限，更容易通過風險擴大過程影響公眾的看法。

風險的社會放大理論在現今網路發達的環境中，更是直得重視。一方面是因為網路是民眾接受訊息的主要管道，特別是風險相關資訊（Brossard & Scheufele, 2013; Chung, 2011）。基於網路訊息容易擴散的特性，少數的傳播者便能引發民眾對某一風險議題的關注，繼而透過社群的互動與發酵產生更大的漣漪效應。研究顯示，反卡西尼探測器運動（卡西尼探測器的目標是深入了解土星的結構、大氣、環境以及其衛星的特徵）起初只有大約六個人，但之後卻對該計畫形成強大的政治壓力。該研究也指出，雖然網路上對於此探測計畫的討論超過六成都是正面的，但少數的反對者充分利用網路傳播的特點，讓此計劃成為爭議焦點，進而達到減少未來預算的目的（Rodrigue, 2001）。

如前所述，目前大部分援引風險的社會放大理論的研究，大多關注媒體使用和風險感知的關係，亦即探討公眾的媒體使用經驗是否會放大或縮小風險感知。然而，該理論除了關切風險感知形成的過程，也重視風險感知引發的後續效應，例如商品銷售下滑、經濟虧損、政策行動、組織結構變化或對機構信心的喪失等（Kasperson, Webler, Ram, & Sutton, 2022）。風險感知和後續效應的關係，也可能會受到媒體使用的影響，此交互作用關係在現有研究中較少受到關注，故本研究欲彌補此一研究缺口。

由於網路是現代人理解風險的主要訊息來源，故本研究側重網路媒體的角色。網路媒體使用對於風險感知的調節作用，可從以下四個面向來推理。第一，根據風險訊息尋求與處理理論，當人們感受到威脅，卻又不清楚有效的因應方式時，便會尋求資訊以降低不確定性（Trumbo, 2002；Yang, Aloe & Feeley, 2014）。資訊尋求行為與其後續影響，可能因資訊內容的不同而呈現差異。當人們接觸到有關網路攻擊威脅的資訊時，風險感知可能進一步強化，從而加深對政府應對能力的不信任。然而，若民眾獲取的是政府因應措施或防治政策相關的資訊，則風險感知對政府應對信心的負面影響可能隨之減弱。從相似的觀點來推論，當民眾具有一定程度的風險感知，在網路上又接觸到威脅資訊時，便較可能支持限縮自由或報復政策，這是因為在面對威脅時，人們傾向尋求即時、強硬的解決方案，即使這意味著犧牲部分自由。當人們獲得較多關於政府如何行動的資訊時，他們會更傾向於支持以民主方式應對威脅。這可能是因為政府的行動資訊，能讓民眾感到情況在掌控之中，並相信透過體制內的合作與溝通，能有效解決問題。

第二，網路平台訊息的一大特色，是使用者大多僅會接觸到和自己立場類似的資訊，亦即同溫層的概念（Cinelli, De Francisci Morales, Galeazzi, Quattrociocchi, & Starnini, 2021）。同溫層效應會影響民眾在面對風險時，對政府應對能力的信心。當人們所處的網路同溫層充斥著威脅資訊時，便會不斷強化其風險感知，使他們傾向認為情況比實際更糟，進而對政府的應對能力產生不信任感。相反地，如果同溫層主要傳播政府行動的具體資訊，則有助於建立透明與信任感，讓民眾相信政府有能力以民主、理性的方式解決問題，進而提升他們對政府應對威脅的信心。因此，網路同溫層如同一個資訊濾鏡，決定了民眾接收到的訊息類型，並直接塑造他們對政府的觀感與信心程度。

另一方面，對網路攻擊風險感知較高的民眾，往往更有動機去尋求能夠驗證其憂慮並支持防護行動的資訊，因為網際網路透過演算法篩選與同質社群，讓使用者更容易接觸到與自身態度一致的資訊。因此，高風險感知且大量使用網路的人，更可能接觸到態度強化的訊息，認為監控或報復是必要的，進而強化風險感知與支持強硬政策之間的正向關聯。相較之下，網路使用程度較低的民眾較少暴露於此類強化環境，因此風險感知對強硬政策支持的影響也相對較弱。

第三，網路媒體上的資訊可能引發不同的情緒反應，而不同的情緒可能會導致對事件不同的評估或行為意圖。在政府應對信心方面，民眾可能因風險感知而產生焦慮感，而焦慮又促進更多的資訊尋求 (Lazarus, 1991)，當人們搜尋到更多的威脅資訊時，可能放大對政府「無力應對」的疑慮，導致政府應對信心降低。相反地，如果網路使用主要讓人接觸到政府政策與作為，焦慮雖然存在，但可能被「政府正在積極行動」的訊息緩解，風險感知對政府信心所造成的負面作用，便可能降低。

另一方面，現今網路上和不實訊息或網路攻擊相關的討論，大多充滿情緒，當人們透過新聞、社群或論壇接觸到指責特定外部行為者（如敵對國家、駭客組織）的資訊，其憤怒感便可能強化，進而使民眾將責任歸因於「對方惡意挑釁」，而更傾向支持嚴厲政策，如監控與報復。研究顯示，在美國 911 恐怖攻擊之後，焦慮的民眾較不支持戰爭，但生氣的民眾則較為支持強硬的反制手段（Huddy et al., 2005）。

根據以上文獻，本研究提出以下研究問題。

研究問題 2a：風險感知與政府應對信心的關係，是否會因為網路媒體參與程度而不同？

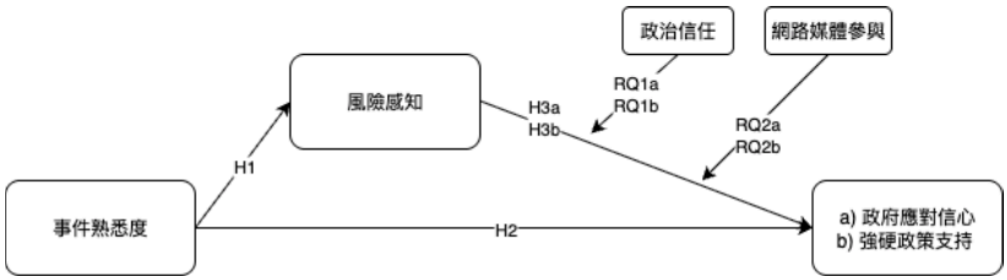
研究問題 2b：風險感知與強硬政策支持的關係，是否會因為網路媒體參與程度而不同？

研究問題 1 和 2 已探討政治信任及網路媒體參與在風險感知與兩個應變項（政府應對信心與強硬政策支持）之間的調節作用。基於此，本研究進一步關注整體中介歷程是否亦可能受到調節。換言之，事件熟悉度透過風險感知而對政府信心與政策支持所產生的間接效果，可能也會因政治信任、網路媒體參與程度的不同而有所變化。因此，本研究提出以下研究問題。

研究問題 3： 事件熟悉度透過風險感知對（a）政府應對信心與（b）強硬政策支持產生的間接效果，是否會因政治信任與網路媒體參與程度的不同而有差異？

整體而言，本研究的研究架構如圖一所示。

圖一：研究架構圖



參、研究方法

一、資料搜集

本研究使用的資料為具有全國代表性的電話調查樣本，由典通股份有限公司執行，調查對象為居住在全國地區年滿 18 歲以上的民眾。調查時間介於民國 113 年 6 月19 日至 113 年 6 月 29 日，共計十一天。

本調查使用雙底冊調查，同時針對市話與手機蒐集資料。市話方面運用電腦輔助電話訪談技術（CATI），從全國住宅電話資料庫中隨機抽樣，並生成後 3 碼，以確保涵蓋全臺所有家用電話，最終獲得 1,071 份樣本。在 95% 的信心水準下，誤差範圍約為 ±2.99%。手機方面則利用隨機數字撥號法（RDD），依據數位發展部所發布的「09AB 行動號碼分配情況」數據，先選取前 5 位門號，再隨機產生後 5 位數字，完成 1,076 份樣本，誤差同樣在 95% 信心區間內約 ±2.99%。本研究聚焦網路使用者，故分析樣本數為 1,949 人。

為使樣本符合台灣人口特徵，調查資料以「多變項反覆加權」（Raking）方式，

依據母體進行性別、年齡、教育程度及居住地區之權數調整，加權後之樣本結構與內政部 112 年 12 月發布之戶籍人口資料沒有顯著差異。然而，迴歸分析是否需要考量權值，現有文獻有諸多不同的討論，一般認為是否需要使用加權，應該取決於研究目的，例如是描述或推論統計？是否為了調整異質變異數（Heteroskedasticity）？是否為了內生抽樣（Endogenous sampling）而調整？或是是否要找出平均部分效果（Average partial effect），若並非前述目的，在迴歸分析中採用權值並非必要（Solon, Haider, &, Wooldridge, 2015）。此外，在迴歸分析中使用加權，會讓標準誤更難以評估，而使得結果難以解釋 (Gelman, 2007)。第三，Winship 與 Radbill（1994）指出，當權值主要和研究依變項相關時，才有納入的必要。例如 1960 年代美國聯邦準備理事會的消費者財務調查，在取樣時刻意抽取較多非常富裕的家庭，而消費行爲作為該調查的主要依變項，會受到取樣方式的影響。根據前述論點，本研究為一般隨機抽樣，也沒有對於變項之統計數值有特殊的調整需求，故在分析時未納入權值。

二、變項描述

本研究之依變項有二，其中強硬政策支持度測量的是民眾對於因應網路攻擊相關政策的態度，研究顯示，政府在面對網路攻擊時，有對內與對外兩種防治手段，對內主要是限制民眾的公民自由權利，例如對人民通訊、意見表達內容的監聽等 （Arsenault, Kreps, Snider, & Canetti, 2024）或隱私的侵犯（Swigger, 2013）；而對外則是對於潛在的攻擊方採取報復手段（Kreps & Schneider, 2019; Shandler, Gross, Backhaus, & Canetti, 2022）。因此，本研究以兩個問項，詢問民眾對網路攻擊防治政策的態度。在對內公民自由權的限制上，採用 Swigger（2013）研究中的問法，詢問受訪者是否同意：「為了防止網路攻擊行動，政府應該被允許監控電話通話、電子郵件及社群媒體對話。」在對外防治策略方面，則是改編自 Kreps 與 Schneider（2019）的題項，該研究詢問受訪者一系列的反制行動，從較為溫和的經濟、外交制裁，到較為強硬的武力攻擊。然而，在台灣，如何因應網路攻擊不論在民間或政府都還沒有充分的討論，遑論有具體的政策方向，若詢問受訪者太多想像情境，恐會有效度疑慮，而過多的題項也會加重受訪者的認知負擔，而降低回答的品質（Krosnick, 1999）。

因此，本研究詢問受訪者對於報復手段的整體態度，而非個別面向，實際問法如下：「針對那些對台灣進行網路攻擊的國家，政府應該採取報復或反擊手段。」回答選項為五點量表，從非常不同意（1）到非常同意（5）。本研究將兩個題項相加並取得平均數，形成強硬政策支持度量表，分數越高代表受訪者越支持較為強硬的因應政策（$M = 2.54$, $SD = 1.10$, $r = .27$, $p < .01$）。

本研究第二個依變項為對政府處理網路攻擊的信心，則參考 Shandler 與 Gomez（2023）之問項，該研究以四個題項詢問德國民眾對於政府未來防止網路攻擊的信心，包含整體網路攻擊、網路恐怖主義、針對基礎設施的網路攻擊，以及致命的恐怖攻擊。本研究亦綜合不同面向，以單一題項測量民眾對政府處理網路攻擊的信心。問卷中，受訪者回答是否相信「政府有能力應對各種類型的網路攻擊」，回答選項為五點量表，從完全不相信（1）到非常相信（5）（$M = 2.75$, $SD = 1.33$）。

本研究之自變項為事件熟悉度，為確保受訪者答題之有效性，本研究選擇兩起較為人知之網路攻擊事件，第一為美國聯邦眾議院議長裴洛西（Nancy Pelosi）於 2022 年 8 月訪台時，超商及鐵路局的螢幕看板都出現謾罵裴洛西的簡體字」；第二是最近幾年國內航空公司（包含長榮與華航）曾發生駭客在網路上不當曝光會員個資，藉以勒索航空公司的情況，本研究詢問受訪者對此二事件的熟悉程度，回答選項為五點量表，從完全不熟悉（1）到非常熟悉（5）。本研究將此二題項相加並取得平均數，形成量表，分數越高代表民眾對網路攻擊事件越熟悉、風險意識越高（$M = 2.31$, $SD = 1.21$, $r = .39$, $p < .01$）。

本研究之中介變項為風險感知，參考 Kostyuk 與 Wayne（2021）之問項，在問卷中詢問受訪者「未來一年，台灣政府或基礎設施（例如電網、電信）可能面臨境外網路攻擊」的可能性，回答選項為五點量表，從非常不可能（1）到非常可能（5）（$M = 4.22$, $SD = 0.99$）。

本研究檢視兩個調節變項，首先是網路資訊參與，在現今的媒體環境中，民眾不僅能此概念接收資訊，更能創作、回應與表達，故網路媒體使用可大致區分為資訊接收及意見表達兩個面向（Anderson, 2017; Namkoong et al., 2017; Yoo, Choi, & Park, 2016）。此外，由於網路是台灣民眾最主要的公共事務消息來源，根據 2023 年台灣傳播調查資料庫的調查，近三分之二的受訪者表示，會透過網路搜尋、瀏覽、點閱

或觀看和政治或公共事務有關的消息（TCS 電子報，2022[1]）。且為清楚呈現調節作用，本研究僅納入網路媒體。基於前述文獻，本研究於問卷中詢問受訪者「是否會關注網路上與政治或公眾事務相關的發文或留言」，回答選項為五點量表，接著詢問受訪者「有多常會在網路上（如：臉書、IG、Threads、部落格），公開發表或回應與政治或公共事務相關的貼文」回答選項為五點量表，1 代表從來沒有，5 代表總是。本研究將兩題問項相加並取平均數，形成網路資訊參與量表，分數越高代表網路資訊參與程度越高（$M = 2.00$, $SD = 0.67$, $r = .27$, $p < .01$）。

第二個調節變項為政治信任，本研究在問卷中詢問受訪者：「整體而言，不分中央或地方，請問您對於台灣政府單位的信任程度為？」回答選項為五點量表，從完全不信任（1）到非常信任（5）（$M = 3.14$, $SD = 1.28$）。

本研究亦控制了幾個會影響民眾態度的變項，包括民眾對相關政策的知識，參考 Pew Research Center（2023）的調查題項，本研究詢問受訪者：「根據您的瞭解，目前政府是否已有專門針對資訊和通訊安全而設立的法案？」回答選項為四點量表，1 代表絕對沒有，5 代表絕對有。由於台灣已設立「資通安全管理法」，故回答絕對有、可能有之受訪者被編碼為 1，代表正確答案，其餘選項則編碼為 0，代表回答錯誤（正確比例：53.4%）。此外，本研究亦納入年齡（$M = 47.61$, $SD = 15.73$）、性別（男性 = 53.7%）、教育程度（中位數 = 大學）等基本人口特徵，作為控制變項。

肆、研究結果

一、描述性分析

調查顯示，約四分之三（74.72%）的受訪者預期未來 12 個月內，台灣的政府部門或關鍵基礎設施（如電力系統或通訊網絡）可能遭遇來自境外的網路威脅。其中，33.1% 的人認為「有點可能」，49.8% 覺得「極有可能」。僅有不到一成（9.9%）的受訪者相信這種攻擊「不會發生」或「幾乎不可能」。

1. https://crctaiwan.dcat.nycu.edu.tw/ResultsShow_detail.asp?RS_ID=161

針對裴洛西訪台期間超商螢幕遭駭客入侵的事件，調查發現，近六成（59.8%）民眾對此知之甚少，其中 41.5% 完全不清楚，18.3% 略感陌生。另有約四成受訪者表示有些了解（28.3%）或相當熟悉（10.3%）。進一步詢問民眾是否了解近年國內航空公司（如長榮、華航）因駭客在網路上非法公開會員資料並勒索的事件，結果顯示，約七成（69.2%）民眾不甚知情，其中 49.2% 完全不知，20.1% 僅略知一二；而表示略為熟悉（24.5%）或十分清楚（5.2%）的人數相對較少。總體來看，本結果顯示，大多數民眾對網路攻擊事件缺乏認識。

本調查亦探討了民眾對政府應對網路攻擊能力的看法，結果顯示，超過五成（56.3%）受訪者對此信心不足，其中 18.6% 完全不信任，37.7% 略感懷疑。另有四成民眾表示有些信心（30.1%）或極有信心（9.8%）。在政府是否應獲准監控電話、電子郵件及社群媒體的問題上，超過七成（72.4%）受訪者反對政府介入私人通訊，其中 44.5% 堅決反對，27.9% 傾向不贊成。但仍有約四分之一的人贊成監控，16% 表示認同，7.4% 非常支持。對於是否應針對發動網路攻擊的國家採取報復行動，48.6% 的民眾不贊成或強烈反對，44.2% 則支持或非常贊成，意見分歧幾乎持平。此外，調查發現，只有約半數人（53.2%）知道台灣已制定專門的資訊與通訊安全法案，約兩成（22.1%）認為不存在此類法律，還有 24.3% 的人坦言不清楚，顯示民眾對相關法規認知有限。

二、假設檢定

H1 假設事件熟悉度和風險感知有正面關係，為驗證此一假設，本研究採用 PROCESS 的模型 4 進行分析，此模型主要在檢驗中介效果。分析結果顯示，事件熟悉度（$b = .18$, $p < .01$）與風險感知具有正向關係，故 H1 獲得支持。在其他變項方面，年齡（$b = .01$, $p < .01$）、教育程度（$b = .11$, $p < .01$）、網路資訊參與（$b = .08$, $p < .05$）、政治信任（$b = .04$, $p < .05$）皆和風險感知呈現正向關聯。

H2a 假設事件熟悉度和政府應對信心有正向關係，結果顯示，事件熟悉度和政府應對信心有顯著之正向關係（$b = .05$, $p < .05$），故 H2a 獲得支持。在控制變項方面，男性（$b = -.08$）、教育程度較低者（$b = -.11$, $p < .01$）對政府處理能力的信任程度較

低。相較之下，政治信任和政府應對信心則呈現顯著正相關（$b = .54, p < .01$），此模型的解釋力達 32.15%。

在強硬政策支持度的分析中（H2b），事件熟悉度並非顯著之預測變項（$b = .00, p > .05$），因此 H2b 並未獲得支持。但年齡、性別、教育程度、網路資訊參與、政治信任和風險感知都和強硬政策支持有顯著的關聯性。年紀較大者（$b = .02, p < .01$）、男性（$b = .14, p < .01$）較為支持強硬政策，而教育程度則顯著降低對強硬政策的支持（$b = -.16, p < .01$）。此外，網路資訊參與程度較高（$b = .15, p < .01$）、政治信任程度較高者（$\beta = .16, p < .01$），也較為傾向支持強硬政策，此模型的解釋力為 17.74%。

H3a、H3b 分別假設風險感知和政府因應信心、強硬政策支持具有正面關係，結果顯示，風險感知越高，對政府的因應信心便越低（$b = -.06, p < .05$），和 H3a 的假定相反；另一方面，風險感知越高，對強硬政策的支持亦越高（$b = .11, p < .01$），符合 H3b 之假定。

關於事件熟悉度與對政府應對信心的間接效果分析，結果指出，該路徑之間接效果為負值且顯著（效果值 = -.01, 信賴區間 = -0.0213 ~ -0.0017），顯示事件熟悉度會透過風險感知和政府應對信心產生關聯性，亦即風險感知是顯著的中介變項。而事件熟悉度和強硬政策支持度間的間接效果則為顯著之正值（效果值 = .0192, 信賴區間 = .0099 ~ .0292），顯示民眾對網路攻擊事件的知悉程度會提升風險感知，並進一步增加對強硬政策的支持；易言之，風險感知亦為顯著之中介變項。

表一：「對政府應對信心」與「強硬政策支持度」的預測因素

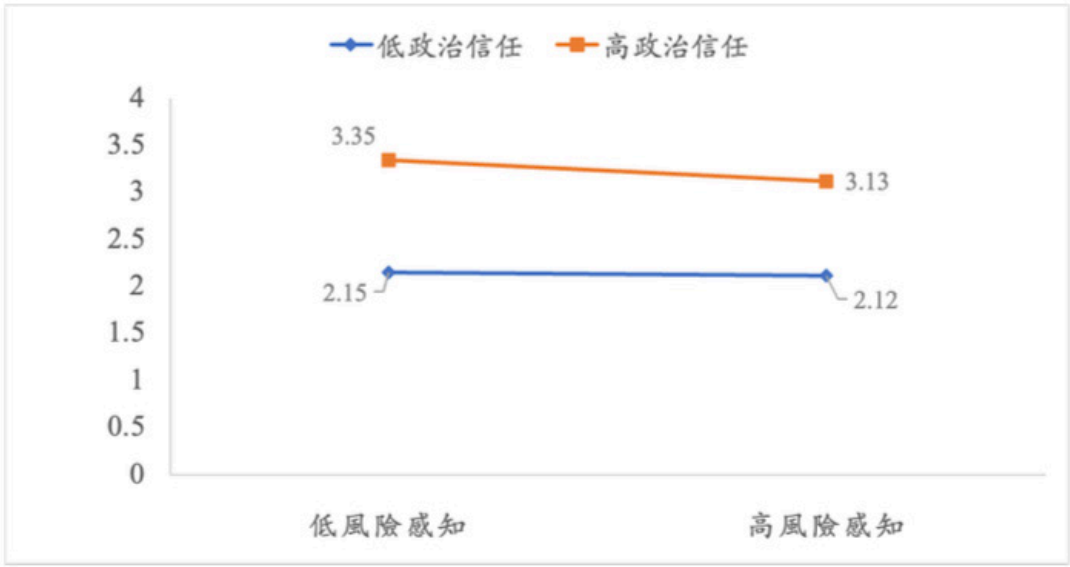
	DV= 風險感知	DV= 對政府應對信心	DV= 風險感知	DV= 強硬政策支持度
年齡	.01**	.00	.01**	.02**
性別（男=1）	.02	-.08	.03	.14**
教育程度	.11**	-.11**	.10**	-.16**
網路資訊參與	.08*	.02	.08*	.15**
政治信任	.04*	.54**	.04*	.16**
政策知識	.06	.21**	.06	.07
事件熟悉度	.18**	.05*	.18**	-.00
風險感知	--	-.06*	--	.11**
R^2	9.21%	32.15%	9.07%	17.74%
	效果值	信賴區間	效果值	信賴區間
間接效果	-.01*	-.0213~ -.0017	.0192*	.0099 ~.0292

$^{**}p < .01$, $^{*}p < .05$

註：表格中的係數為非標準化迴歸係數，結果來自 PROCESS 模型 4。

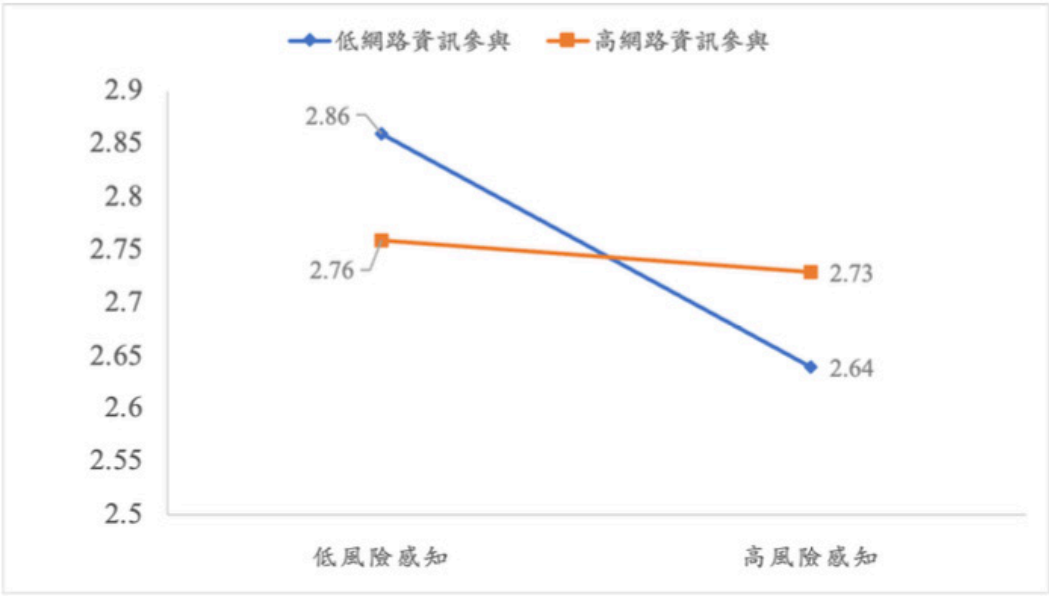
本研究涵蓋兩個調節變項，為了檢視此二調節變項的作用，作者採用了 PROCESS 的 SPSS 巨集，該巨集的模型 16 可以讓研究者檢驗中介變項與兩個調節變項是否對依變項有交互作用，結果如表二所示。根據表二第一欄的結果，政治信任與風險感知對政府處理網路攻擊的信任程度具有顯著的調節作用（b = -.04, p < .05）。本研究以自變項在單一調節變項的不同數值時所對應之依變項平均數作為基準，並以 84 百分點及 16 百分點來區分自變項與調節變項的高低數值，繪製出交互作用圖。如圖二所示，當政治信任較高時，民眾對政府的信任程度也較高，特別是在風險感知較低的情境下。然而，當風險感知提高時，即使是高政治信任者，他們對政府的信任程度也略微下降，平均降至 3.13，說明風險感知的增加在一定程度上削弱了政治信任對政府處理網路攻擊能力信心的正向關聯性。對於低政治信任者而言，情況則有所不同。無論風險感知的高低，此類民眾對政府的信心都較低，分別為 2.15 和 2.12，幾乎沒有變化。此結果顯示，對於低政治信任者來說，風險感知的變化並不會顯著改變他們對政府處理網路攻擊的信心。此模型整體的解釋力為 32.6%，表示此模型具有一定程度的解釋力。

圖二：政治信任和風險感知的交互作用關係（依變項：政府應對信心）



根據表二第一欄的結果，網路資訊參與和風險感知亦對政府處理網路攻擊的信心有顯著的交互作用。如圖三所示，對低網路資訊參與者而言，風險感知會降低民眾對政府處理能力的信心。相較之下，高網路資訊參與者即使在風險感知增加的情況下，對政府的信任仍相對穩定。當風險感知較低時，他們對政府處理網路攻擊能力的信任程度為 2.76，而當風險感知較高時，信任程度僅小幅下降至 2.73，未達統計顯著水準（請參見表三）。

圖三：網路資訊參與和風險感知的交互作用關係（依變項：政府應對信心）



在「強硬政策支持度」的依變項中，兩個調節中介分析的結果指出（表二第二欄），不論是政治信任或網路資訊參與都沒有顯著的交互作用關係。換句話說，事件熟悉度與風險感知和強硬政策支持度的關聯性，並沒有因為政治信任或網路資訊參與程度的高低而有區別，此模型的解釋力為 9.01%。

表二：政治信任、網路資訊參與的調節作用

	DV= 對政府處理網路攻擊的信心	DV= 強硬政策支持度
年齡	.00	.02**
性別（男=1）	-.08	.14**
教育程度	-.11**	-.16**
政治信任	.73**	.17*
網路資訊參與	-.37*	.06
政策知識	.21**	-.00
事件熟悉度	.05*	.01
風險感知	-.11	.08
風險感知 × 政治信任	-.04*	-.01
風險感知 × 網路資訊參與	.09*	.02
R^2	32.6%	9.01%

**$p < .01$, *$p < .05$

註：表格中的係數為非標準化迴歸係數。

根據表三，政治信任和網路資訊參與對風險感知與依變項（對政府處理網路攻擊的信任程度）之間的關係具有顯著的調節作用。當政治信任較低時，風險感知與政府信心的關聯不顯著（效果值 = -.0029，信賴區間為 -.0133 至 .0168）；但當政治信任較高時，風險感知與政府信任之間呈顯著負向關聯（效果值 = -.0208，信賴區間為 -.0356 至 -.0067），顯示在高政治信任情境下，風險感知對政府信任的負面關聯較強。在網路資訊參與的調節效果中，當網路資訊參與較低時，風險感知與政府處理能力的信心程度之間呈顯著負向關聯（效果值 = -.0142，信賴區間為 -.1668 至 -.0416）；然而，當網路資訊參與較高時，風險感知和政府處理能力的信心無關（效果值 = -.0098，信賴區間為 -.0758 至 .0562）。

最後，研究問題 3 探討事件熟悉度透過風險感知對（a）政府應對信心與（b）強硬政策支持產生的間接效果，是否會因政治信任與網路媒體參與程度的不同而有差異，亦即整體模型的調節中介效果。在政治信任方面，根據表三，調節效果的中介指數（Index）為負值（-.0090，信賴區間為 -.0159 至 -.0022），顯示事件熟悉度和政府處理網路攻擊信心的負向關係，會因為政治信任的提高而增強。在網路資訊參與方面，調節效果的中介指數（Index）為正值（.0184，信賴區間為 .0056 至 .0321），說明事件熟悉度和政府處理網路攻擊信心之間的負向關係，會隨著網路資訊參與的增加而減弱。

表三：政治信任、網路資訊參與與風險感知的交互作用關係

調節變項	效果值	信賴區間
低政治信任	-.0029	-.0133 ~ .0068
高政治信任	-.0208*	-.0356 ~ -.0067
Index	-.0090*	-.0159 ~ -.0022
低網路資訊參與	-.0142*	-.1668 ~ -.0416
高網路資訊參與	-.0098	-.0758 ~ .0562
Index	.0184*	.0056 ~ .0321

*p <.05

註：（1）表格中的係數為非標準化迴歸係數。（2）效果值指的是在不同調節變項數值中，風險感知和依變項（對政府應對網路攻擊的信心）的關係。（3）Index 為中介調節指數，正值表示該間接效果會因為調節變項而增強，負值則代表該間接效果因調節變項而減弱。

伍、討論

透過 TWNIC 的調查資料，本研究發現台灣民眾的風險意識和政府的應對信心有顯著的負面關係，亦即知悉具體網路攻擊事件的民眾，對政府未來是否有能力應對類似攻擊的信心較低。然而，事件熟悉度和強硬政策支持之間並不存在直接關係，而是透過風險感知的作用；換句話說，事件熟悉度強化風險感知，而風險感知又進一步將低對政府的應對信心與增加對強硬政策的支持，此結果和現有研究一致 （Snider 等人，2021）。而風險意識（亦即事件熟悉度）和風險感知在本研究中所展現出的不同作用，亦表示兩個概念雖然相關，但也有區分的必要。

本研究發現風險感知與政治信任對於政府應對信心具有交互作用關係，對於政治信任度高的民眾而言，風險感知與應對信心之間呈負相關；然而，對於政治信任度低的民眾來說，兩者之間則無顯著關聯。此發現符合「價值犧牲理論」的假定，如圖二所示，政治信任的效果在風險感知低時較為明顯，因為當民眾沒有感受到威脅時，必須仰賴政治信任的作用才能建立對政府應對能力的信心。

此發現也能從「期望」的觀點來解釋，高政治信任的民眾對政府有較高的期待，理應也對政府因應網路攻擊的能力較具信心；然而，當他們感到此危害的威脅，並發現政府尚未制定足夠的法令或政策來應對此一問題時，其信心便會將低。根據期望與落差效應（Expectation and Disconfirmation Effect），消費者對產品的滿意度取決於期望是否得到滿足；詳細來說，滿足是相對的概念，以期望為參照點，若產品或服務符合預期，則通常會產生滿意的態度，反之則讓民眾感到不滿 （Oliver, 1980）。

在本研究的情境下，政治信任度高的民眾期望政府能積極應對網路威脅，卻發現因應政策或法令尚未建立，這種期望落空導致信心的降低。換句話說，高政治信任的民眾並非對政府失去信任，而是對政府的準備程度感到不足。本研究發現僅有約半數民眾知悉台灣已有專門針對資訊和通訊安全而設立的法案獲得支持，且政策知識和政府應對信心有顯著的正面關係，即是支持此一推論之證據。

對於低政治信任者而言，風險感知的增加並不會顯著影響他們對政府處理網路攻擊的信心，原因可能是低政治信任者原本對政府的能力就已經抱持較為懷疑的態度及消極的看法，因此增加的風險感知並不會進一步降低他們的信心。另一種解釋是低政

治信任的民眾整體而言對政府能力較不具信心，因此不論自身風險感知的高低，都不認為政府能有效應對未來的網路攻擊。

此外，本研也究發現，當應變項為「支持強硬政策」時，政治信任和風險感知未呈現顯著的調節作用，此結果和 Davis 與 Silver（2004）不同。此差異可能主要來自研究議題性質的不同， 911 攻擊屬於規模巨大且具高度象徵意義的實體恐怖事件，加上極高的媒體曝光度，對民眾造成直接而強烈的情緒衝擊。在此類高情緒喚起的情境下，政治信任往往成為民眾快速判斷政府作為正當性與可接受性的心理依據。研究指出，當人們面對強烈威脅或焦慮時，可能會傾向依賴政治信任作為認知捷徑，以降低不確定感並尋求心理安全（Vasilopoulos et al., 2023）。因此，在實體恐怖攻擊的高情緒脈絡中，政治信任對風險感知與政策態度之間的調節作用更容易顯現。

相較之下，網路攻擊事件多屬抽象且間接體驗的威脅，其影響通常缺乏具體的災難場景或立即性的生命威脅，所引發的情緒激昂程度相對有限。加上網路攻擊的規模分散、後果不易被具象化，多數民眾僅透過媒體報導間接理解事件，使其風險感知偏向理性與認知層面，而非情緒性反應。在這樣低情緒喚起的情境下，民眾較少依賴政治信任作為判斷線索，導致政治信任在風險感知與政策支持間的調節效應不如實體恐怖攻擊情境明顯（Schlipphak, 2024）。

本研究也發現網路媒體參與有顯著的調節功能，對於低網路媒體參與者而言，較高的風險感知會削弱其對政府應對能力的信心。相比之下，高網路媒體參與者即便感知到較高風險，對政府的信任仍然維持相對穩定。此結果可能和網路媒體的正面功效有關，一篇 COVID-19 疫情期間的研究發現，社群媒體使用與政治信任的提升及採取防疫措施的自我效能感有正面關係，顯示經常使用社群媒體的民眾可能對政府建立起更具韌性的信任，即便感知到風險仍較不易動搖。相較之下，較少接觸網路的民眾可能缺乏這種信任強化的機制，使其對政府的信心更容易因感知到的威脅而減弱（Hassan et al., 2021）。

第二，如文獻探討中所言，經常使用網路媒體的民眾通常會接觸到多元的資訊來源，包括政府官方通訊、專家分析以及網路安全事件的即時更新，因此除了接觸到網路攻擊風險相關訊息之外，亦可能較為知悉政府的應對措施，從而增強對政府回應能力的信心。相較之下，較少使用網路媒體的民眾可能更依賴傳統媒體或個人社交網

絡，而這些來源可能無法提供同樣全面或即時的資訊，進而導致風險感知升高，並降低對政府應對能力的信心。

第三，文獻亦指出同溫層效應的重要性。相較之下，低度網路媒體參與者可能缺乏此類「社群支持」，其風險感知更容易單向轉化為對政府的不信任；反之，高度參與者在同溫層中可能透過追蹤官方帳號或專業意見領袖，獲得更多「政府有所作為」的訊息，從而減弱風險感知對政府信心的負面影響。

此外，本文有一些研究限制需要說明，以便對研究發現有適切的解讀。首先，本研究中有數個變項皆由單一問項測量（例如政治信任、網路媒體參與、政府應對信心等），其信度與效度可能不如由多個題項所組成量表。此結果肇因於本次調查關注眾多台灣重要的網路議題，使得每個概念所能分配到的題項較為有限。然而，TWNIC調查為台灣民眾網路行為與當前台灣社會最缺乏了解的網路現象提供最新的第一手資料，具有極高之政策意義。此外，在本研究中，主要的概念皆源自現有期刊文獻或國際重要調查，故其信度與效度應有基本的水準。

第二，網路攻擊涵蓋的範圍較大，可區分為致命的與非致命，前者包含造成受傷與死亡的網路攻擊，後者則意指產生財產或資料損失的網路攻擊（Gross, Canetti, & Vashdi, 2017；Snider et al., 2021）。但相關研究結果並不一致，有研究發現暴露於致命網路攻擊訊息的民眾，較可能支持警告型的政策（亦即在網路攻擊發生後適時通知民眾）；而接觸非致命網路攻擊訊息的民眾，則較可能支持監管型政策，亦指政府有介入保護人民或企業的責任（Snider et al., 2021）。另一方面，Gross 等人（2017）的研究卻發現，兩類不同的攻擊和民眾對政府的應對信心並無太多差異，特別是關於政府保護基礎設施的信心、保護個人資料的信心，以及保護公私立單位的信心。由於目前台灣較常出現的網路攻擊並非是造成傷亡的致命式攻擊，本研究聚焦於非致命、以基礎設施為對象的網路攻擊尚稱合理。

陸、結論

網路攻擊會導致基礎設施服務中斷、資料外洩以及民眾的焦慮與不安全感，不僅削弱個人與社會的數位福祉，也影響整體社會的穩定與信任。如何建構安全可靠的網

路環境，提升公眾對網路攻擊風險的認識與面對損害後的復原能力，已成為政府與相關單位亟需關注的重要課題。

運用台灣網路資訊中心（TWNIC）2024 年的調查資料，本研究發現台灣民眾雖然具有高度風險感知，但是對具體的網路攻擊事件並不熟悉，對於政府的應對能力也不具備太高的信心。更重要的是，網路攻擊讓民眾產生風險感知，進而降低對政府的應對信心，也支持較不符合民主概念的政策（例如限縮自由或報復性政策），可說網路恐怖主義已經發揮出其預設的效果。

本研究發現，不同於傳統的實體恐怖攻擊，網路攻擊並未出現所謂的「聚旗效應」（Rally-round-the-flag Effect），該現象指的是當國家遭遇外部威脅或重大危機時，民眾往往會因共同體意識的提升而暫時增加對政府或國家領袖的支持（Hetherington & Nelson, 2003）。然而，本研究在網路攻擊的情境下並未觀察到類似的效應。換言之，風險感知並未提升民眾對政府的信心，也未使民眾更傾向支持那些以國家安全為優先、卻可能侵蝕民主價值的強硬政策。這些發現顯示網路攻擊與傳統恐怖攻擊存在重要差異：恐怖攻擊通常具有明確的外部敵人與強烈的情緒衝擊，容易促發民眾的團結效應；相較之下，網路攻擊的發動者往往匿名且難以辨識，影響較為隱蔽與間接，民眾反而可能將責任歸咎於政府的準備不足。這樣的差異不僅突顯網路攻擊在政治心理層面的獨特性，也顯示值得進一步探究其對政府信心與政策態度的長期影響。

雖然風險感知和一些較為負面的後果有關（例如信心降低、支持強硬政策），但不代表政府應該隱瞞網路攻擊事件，本研究結果可以為台灣政府未來如何因應此類攻擊提供兩點建議。第一，建立更完善的法規制度，包含預防、事件監控與預警（Snider 等人，2021），讓政府具備對抗網路攻擊的能力。本研究發現，知悉台灣已有相關法規的民眾，對政府未來的因應能力較具信心；也發現政治信任較高的民眾，可能會因為認為現有法規不足以防範網路攻擊，而降低對政府的應對信心，都說明了建立因應制度並讓民眾知曉，是未來有益的施政方向。台灣現行的《資通安全管理法》主要著重於治理架構的建立，屬於原則性規範，且焦點多集中在公務機關。例如，公部門不得下載、安裝或使用可能危害國家資通安全的產品，並須設置資安專責人員，建立通報機制與相關罰則。然而，若對照歐盟的規範，台灣的法制架構仍有擴充空間。

以歐盟的《NIS 2 指令》為例，其法規適用範圍已超越政府部門，涵蓋能源、醫療保健、交通運輸及數位基礎設施等關鍵產業（羅正漢，2022）。在事件監控方面，歐盟透過高度協調的跨國資訊共享平台與歐洲網路危機聯絡組織（EU-CyCLONe），得以即時監測並迅速應對潛在威脅，台灣較缺乏類似跨部門、跨國的統一監控及快速協作機制，監控範圍及效率皆有待提升。在預警機制上，歐盟強調的不僅是事件通報，更包括標準化的資料揭露、弱點通報制度以及危機聯絡網絡的運作，以支援大規模資安事件的應變。而相較之下，台灣現行法制的預警仍主要著重於通報義務，尚未建立完善的威脅情報共享系統與跨產業協作機制。因此，無論是制定新的網路安全專法，或是對現有《資通安全管理法》進行更細緻的修訂與補充，都是強化國家整體資安防護能量的必要方向。

第二，建立法規制度後，需善用社群媒體與民眾溝通，並建立信心。本研究發現，社群媒體使用雖然會增加風險感知，以及讓民眾傾向支持較為強硬的政策，但同時也會減緩風險感知所造成的信心下滑。因此，政府應積極利用社群媒體平台，提供即時、準確且多元的資訊，包括網路安全事件的最新動態、政府應對措施、專家分析等，讓民眾知悉並感受到政府對於網路攻擊有具體作為，以提升信心。此外，在發生網路安全事件時，應及時向民眾提供準確的風險評估和應對措施，避免不必要的恐慌。此做法可以降低民眾的風險感知，預防後續對於政府應對信心的負面影響。

最後，在理論貢獻上，本研究整合建構層次理論、歸因理論與情緒評估傾向理論，提出一個從心理距離到情緒反應的多層次心理歷程模型。建構層次理論指出，心理距離會影響人們對事件的抽象或具體詮釋，然而它並未具體說明人們如何縮短這種距離。歸因理論正好補足此一不足，該理論指出，透過尋找明確的責任對象或因果來源，可以使抽象威脅具體化、心理距離被壓縮。而當責任歸因完成後，評估傾向理論進一步闡釋不同情緒（如焦慮與憤怒）如何根據事件的可控性與確定性，導向不同的態度與政策偏好。三者的整合使本研究能從「距離—歸因—政策態度」的動態過程，理解民眾面對破壞性網路攻擊時的心理機制，讓此領域的研究更具理論基礎。

參考文獻

林翠儀（2022 年 11 月 25 日）。日防衛省智庫報告：中國對台認知作戰 協助親中派候選人，取自 https://news.ltn.com.tw/news/world/breakingnews/4135437

曾以寧（2025 年 3 月 3 日）。彰基遭駭客攻擊 衛福部：資安專家進駐、將報案，取自 https://www.cna.com.tw/news/ahel/202503030111.aspx

羅正漢（2025 年 1 月 10 日）。【重新認識國家級駭客威脅】全民資安風險倍增！國家支持的網路間諜攻擊升級，取自 https://www.ithome.com.tw/news/166901

羅正漢（2025 年 5 月 22 日）。歐洲第二版資安指令 NIS 2 即將發布，更多重要中大型產業納入規範，取自 https://www.ithome.com.tw/news/151044

Anderson, A. A. (2017). *Effects of social media use on climate change opinion, knowledge, and behavior*. http://climatescience.oxfordre.com/view/10.1093/acrefore/9780190228620.001.0001/acrefore-9780190228620-e-369

Arsenault, A. C., Kreps, S. E., Snider, K. L., & Canetti, D. (2024). Cyber scares and prophylactic policies: Crossnational evidence on the effect of cyberattacks on public support for surveillance. *Journal of Peace Research, 61*(3), 413-428. https://doi.org/10.1177/00223433241233960

Bates, S., Holmes, J., Gavens, L., De Matos, E. G., Li, J., Ward, B., Hooper, L., Dixon, S., & Buykx, P. (2018). Awareness of alcohol as a risk factor for cancer is associated with public support for alcohol policies. *BMC public health, 18*, 1-11. https://doi.org/10.1186/s12889-018-5581-8

Binder, A. R., Scheufele, D. A., Brossard, D., & Gunther, A. C. (2011). Interpersonal amplification of risk? Citizen discussions and their impact on perceptions of risks and benefits of a biological research facility. *Risk Analysis: An International Journal, 31*(2), 324-334. https://doi.org/10.1111/j.1539-6924.2010.01516.x

Bradford, R. A., O'Sullivan, J. J., Van der Craats, I., Krywkow, J., Rotko, P., Aaltonen, J., Bonaiuto, M., De Dominicis, S., Waylen, K., & Schelfaut, K. (2012). Risk perception–issues for flood management in Europe. *Natural Hazards and Earth System Sciences,*

12(7), 2299-2309. https://doi.org/10.5194/nhess-12-2299-2012

Brewer, N. T., Weinstein, N. D., Cuite, C. L., & Herrington, J. E. (2004). Risk perceptions and their relation to risk behavior. *Annals of Behavioral Medicine, 27*(2), 125-130. https://doi.org/10.1207/s15324796abm2702_7

Brossard, D., & Scheufele, D. A. (2013). Science, new media, and the public. *Science, 339*(6115), 40-41. https://doi.org/10.1126/science.1232329

Canetti-Nisim, D., Ariely, G., & Halperin, E. (2008). Life, pocketbook, or culture: The role of perceived security threats in promoting exclusionist political attitudes toward minorities in Israel. *Political Research Quarterly, 61*(1), 90-103. https://doi.org/10.1177/1065912907307289

Chaiken, S., Liberman, A., & Eagly, A. (1989). Heuristic and systematic processing within and beyond the persuasion context. In J. S. Veleman & J. A. Bargh (Eds.), *Unintended Thought* (pp. 212-252). Guilford Press.

Chanley, V. A., Rudolph, T. J., & Rahn, W. M. (2000). The origins and consequences of public trust in government: A time series analysis. *Public Opinion Quarterly, 64*(3), 239-256. https://doi.org/10.1086/317987

Chen, S., & Chaiken, S. (1999). The heuristic-systematic model in its broader context. In *Dual-process Theories in Social Psychology*. (pp. 73-96). The Guilford Press.

Chu, H. (2022). Construing climate change: Psychological distance, individual difference, and construal level of climate change. *Environmental Communication, 16*(7), 883-899. https://doi.org/10.1080/17524032.2022.2061027

Chu, H., & Yang, J. Z. (2020). Risk or efficacy? How psychological distance influences climate change engagement. *Risk Analysis, 40*(4), 758-770.

Chung, I. J. (2011). Social amplification of risk in the Internet environment. *Risk Analysis: An International Journal, 31*(12), 1883-1896. https://doi.org/10.1111/risa.13446

Cinelli, M., De Francisci Morales, G., Galeazzi, A., Quattrociocchi, W., & Starnini, M. (2021). The echo chamber effect on social media. *Proceedings of the National Academy of Sciences, 118*(9), e2023301118. https://doi.org/10.1073/pnas.2023301118

Cisternas, P. C., Cifuentes, L. A., Bronfman, N. C., & Repetto, P. B. (2024). The influence of risk awareness and government trust on risk perception and preparedness for natural hazards. *Risk Analysis, 44*(2), 333-348. https://doi.org/10.1111/risa.14151

Dacorogna, M., & Kratz, M. (2023). Managing cyber risk, a science in the making. *Scandinavian Actuarial Journal, 2023*(10), 1000-1021. https://doi.org/10.2139/ssrn.4356389

Davis, D. W., & Silver, B. D. (2004). Civil liberties vs. security: Public opinion in the context of the terrorist attacks on America. *American Journal of Political Science, 48*(1), 28-46. https://doi.org/10.1111/j.0092-5853.2004.00054.x

De Bruijn, H., & Janssen, M. (2017). Building cybersecurity awareness: The need for evidence-based framing strategies. *Government Information Quarterly, 34*(1), 1-7.

Devine, D. (2024). Does political trust matter? A meta-analysis on the consequences of trust. *Political Behavior, 46*(4), https://doi.org/2241-2262. 10.1007/s11109-024-09916-y

Frewer, L. J., Miles, S., & Marsh, R. (2002). The media and genetically modified foods: evidence in support of social amplification of risk. *Risk Analysis: An International Journal, 22*(4), 701-711. https://doi.org/10.1111/0272-4332.00062

Gelman, A. (2007). Struggles with survey weighting and regression modeling. *Statistical Science, 22* (2), 153-164. DOI: 10.1214/088342306000000691

Gibson, S. D. (2003). The case for "risk awareness." *Security Journal, 16*, 55-64. https://doi.org/10.1057/palgrave.sj.8340140

Goitein, E. (2021.08.25). *Rolling back the post-9/11 surveillance state*. Brennan Center for Justice. https://www.brennancenter.org/our-work/analysis-opinion/rolling-back-post-911-surveillance-state

Gross, M. L., Canetti, D., & Vashdi, D. R. (2017). Cyberterrorism: its effects on psychological well-being, public confidence and political attitudes. *Journal of Cybersecurity, 3*(1), 49-58. https://doi.org/10.1093/cybsec/tyw018

Hassan, M. S., Al Halbusi, H., Najem, A., Razali, A., & Fattah, F. A. M. A. (2021). Risk

perception, self-efficacy, trust in government, and the moderating role of perceived social media content during the COVID-19 pandemic. *Changing Societies & Personalities. 5*(1), 9-35. 10.15826/csp.2021.5.1.120

Hetherington, M. J., & Nelson, M. (2003). Anatomy of a rally effect: George W. Bush and the war on terrorism. *PS: Political Science & Politics, 36*(1), 37-42. doi:10.1017/S1049096503001665

Hibbing, J. R., & Theiss-Morse, E. (2001). *What is it about government that Americans dislike?* Cambridge University Press.

Huddy, L., Feldman, S., Taber, C., & Lahav, G. (2005). Threat, anxiety, and support of antiterrorism policies. *American Journal of Political Science, 49*(3), 593-608. https://doi.org/10.1111/j.1540-5907.2005.00144.x

Jaikaran, C. (2025). *Cybersecurity: Selected Cyberattacks, 2012–2024*. Congressional Research Service. https://www.congress.gov/crs-product/R46974

Kahan, D. M., Braman, D., Slovic, P., Gastil, J., & Cohen, G. (2009). Cultural cognition of the risks and benefits of nanotechnology. *Nature Nanotechnology, 4*(2), 87-91. https://doi.org/10.1038/nnano.2008.341

Kasperson, J. X., Kasperson, R. E., Pidgeon, N., & Slovic, P. (2010). The social amplification of risk: Assessing fifteen years of research and theory. In P. Slovic (Ed.), *The feeling of risk* (pp. 317-344). Routledge.

Kasperson, R. E., Webler, T., Ram, B., & Sutton, J. (2022). The social amplification of risk framework: New perspectives. *Risk Analysis, 42*(7), 1367-1380. https://doi.org/10.1111/risa.13926

Kostyuk, N., & Wayne, C. (2021). The microfoundations of state cybersecurity: Cyber risk perceptions and the mass public. *Journal of Global Security Studies, 6*(2), ogz077. https://doi.org/10.1093/jogss/ogz077

Kreps, S., & Schneider, J. (2019). Escalation firebreaks in the cyber, conventional, and nuclear domains: moving beyond effects-based logics. *Journal of Cybersecurity, 5*(1), tyz007. https://doi.org/10.1093/cybsec/tyz007

Krosnick, J. A. (1999). Survey research. *Annual Review of Psychology, 50*(1), 537-567. https://doi.org/10.1146/annurev.psych.50.1.537

Kulin, J., & Johansson Sevä, I. (2021). Who do you trust? How trust in partial and impartial government institutions influences climate policy attitudes. *Climate Policy, 21*(1), 33-46. https://doi.org/10.1080/14693062.2020.1792822

Kung, Y. W., & Chen, S. H. (2012). Perception of earthquake risk in Taiwan: Effects of gender and past earthquake experience. *Risk Analysis: An International Journal, 32*(9), 1535-1546. https://doi.org/10.1111/j.1539-6924.2011.01760.x

Lazarus, R. S. (1991). *Emotion and adaptation*. Oxford University Press.

Lermer, E., Streicher, B., Sachs, R., Raue, M., & Frey, D. (2016). Thinking concretely increases the perceived likelihood of risks: The effect of construal level on risk estimation. *Risk Analysis, 36*(3), 623-637. https://doi.org/10.1111/risa.12445

Lerner, J. S., & Keltner, D. (2001). Fear, anger, and risk. *Journal of Personality and Social Psychology, 81*(1), 146-159. https://doi.org/10.1037/0022-3514.81.1.146

Lim, J. Y., & Moon, K. K. (2020). Examining the moderation effect of political trust on the linkage between civic morality and support for environmental taxation. *International Journal of Environmental Research and Public Health, 17*(12), 4476.https://doi.org/10.3390/ijerph17124476

Montañez, R., Golob, E., & Xu, S. (2020). Human cognition through the lens of social engineering cyberattacks. *Frontiers in Psychology, 11*, 1755. https://doi.org/10.3389/fpsyg.2020.01755

Namkoong, K., Shah, D. V., McLaughlin, B., Chih, M. Y., Moon, T. J., Hull, S., & Gustafson, D. H. (2017). Expression and Reception: An Analytic Method for Assessing Message Production and Consumption in CMC. *Commun Methods Meas, 11*(3), 153-172. https://doi.org/10.1080/19312458.2017.1313396

OECD (2019), How's Life in the digital age?: Opportunities and risks of the digital transformation for people's well-being, OECD Publishing, Paris.

Oksanen, A., Kaakinen, M., Latikka, R., Savolainen, I., Savela, N., & Koivula, A. (2020).

Regulation and trust: 3-month follow-up study on COVID-19 mortality in 25 European countries. *JMIR Public Health and Surveillance, 6*(2), e19218. 10.2196/19218

Oliver, R. L. (1980). A cognitive model of the antecedents and consequences of satisfaction decisions. *Journal of Marketing Research, 17*(4), 460-469. https://doi.org/10.1177/002224378001700405

Pew Research Center (2023). How Americans view data privacy. Retrieved from https://www.pewresearch.org/internet/2023/10/18/views-of-data-privacy-risks-personal-data-and-digital-privacy-laws/

Quigley, B. M., & Tedeschi, J. T. (1996). Mediating effects of blame attributions on feelings of anger. *Personality and Social Psychology Bulletin, 22*(12), 1280-1288. https://doi.org/10.1177/01461672962212008

Robinson, S. E., Ripberger, J. T., Gupta, K., Ross, J. A., Fox, A. S., Jenkins-Smith, H. C., & Silva, C. L. (2021). The relevance and operations of political trust in the COVID-19 pandemic. *Public Administration Review, 81*(6), 1110-1119. https://doi.org/10.1111/puar.13333

Rodrigue, C. M. (2001). Internet media in technological risk amplification: plutonium on board the Cassini-Huygens Spacecraft. *Risk: Health, Safety & Environment, 12*(3/4), 221-254.

Rudolph, T. J. (2017). Political trust as a heuristic. In S. Zmerli & T. van der Meer (Eds.), *Handbook on political trust* (pp. 197-211). Edward Elgar Publishing.

Rudolph, T. J., & Popp, E. (2009). Bridging the ideological divide: Trust and support for social security privatization. *Political Behavior, 31*, 331-351. https://doi.org/10.1007/s11109-008-9078-5

Schlipphak, B. (2021). Threat perceptions, blame attribution, and political trust. *Journal of Elections, Public Opinion and Parties, 34*(1), 59–78. https://doi.org/10.1080/17457289.2021.2001474

Shandler, R., & Gomez, M. A. (2023). The hidden threat of cyber-attacks–undermining public confidence in government. *Journal of Information Technology & Politics, 20*(4),

359-374. https://doi.org/10.1080/19331681.2022.2112796

Shandler, R., Gross, M. L., Backhaus, S., & Canetti, D. (2022). Cyber terrorism and public support for retaliation–a multi-country survey experiment. *British Journal of Political Science, 52*(2), 850-868. https://doi.org/10.1017/S0007123420000812

Siegrist, M., & Árvai, J. (2020). Risk perception: Reflections on 40 years of research. *Risk Analysis, 40*(S1), 2191-2206. https://doi.org/10.1111/risa.13599

Slovic, P., Fischhoff, B., & Lichtenstein, S. (1976). Cognitive processes and societal risk taking. In H. Jungermann & G. De Zeeuw (Eds.), *Decision making and change in human affairs. D. Reidel Publishing Company. Theory and Decision Library* (Vol. 16, pp. 7-36). Springer.

Slovic, P., & Peters, E. (2006). Risk perception and affect. *Current Directions in Psychological Science, 15*(6), 322-325. https://doi.org/10.1111/j.1467-8721.2006.00461.x

Snider, K. L. G., Shandler, R., Zandani, S., & Canetti, D. (2021). Cyberattacks, cyber threats, and attitudes toward cybersecurity policies. *Journal of Cybersecurity, 7*(1). https://doi.org/10.1093/cybsec/tyab019

Solon, G., Haider, S. J., & Wooldridge, J. M. (2015). What are we weighting for? *Journal of Human Resources, 50*(2), 301-316. https://doi.org/10.3368/jhr.50.2.301

Swigger, N. (2013). The online citizen: Is social media changing citizens' beliefs about democratic values? *Political Behavior, 35*(3), 589-603. https://doi.org/10.1007/s11109-012-9208-y

Trope, Y., & Liberman, N. (2010). Construal-level theory of psychological distance. *Psychological Review, 117*(2), 440.

Trumbo, C. W. (2002). Information processing and risk perception: An adaptation of the heuristic-systematic model. *Journal of Communication, 52*(2), 367-382. https://doi.org/10.1111/j.1460-2466.2002.tb02550.x

Van Schaik, P., Jansen, J., Onibokun, J., Camp, J., & Kusev, P. (2018). Security and privacy in online social networking: Risk perceptions and precautionary behaviour. *Computers*

in Human Behavior, 78, 283-297. https://doi.org/10.1016/j.chb.2017.10.007

Van Schaik, P., Jeske, D., Onibokun, J., Coventry, L., Jansen, J., & Kusev, P. (2017). Risk perceptions of cyber-security and precautionary behaviour. *Computers in Human Behavior, 75*, 547-559. https://doi.org/10.1016/j.chb.2017.05.038

Vanden Abeele, M. M. (2021). Digital wellbeing as a dynamic construct. *Communication Theory, 31*(4), 932-955. https://doi.org/10.1093/ct/qtaa024

Vasilopoulos, P., McAvay, H., Brouard, S., & Foucault, M. (2023). Emotions, governmental trust and support for the restriction of civil liberties during the covid-19 pandemic. *European Journal of Political Research, 62*(2), 422-442. https://doi.org/10.1111/1475-6765.12513

Wagner, M. (2014). Fear and anger in Great Britain: Blame assignment and emotional reactions to the financial crisis. *Political Behavior, 36*(3), 683-703. https://doi.org/10.1007/s11109-013-9241-5

Wakslak, C. J., Trope, Y., Liberman, N., & Alony, R. (2006). Seeing the forest when entry is unlikely: probability and the mental representation of events. *Journal of Experimental Psychology: General, 135*(4), 641. https://doi.org/10.2139/ssrn.946239

Wildavsky, A., & Dake, K. (1990). Theories of risk perception: Who fears what and why? *Daedalus, 119*(4), 41-60.

Winship, C., & Radbill, L. (1994). Sampling weights and regression analysis. *Sociological Methods & Research, 23*(2), 230-257. https://doi.org/10.4324/9780429284243-5

Yang, Z. J., Aloe, A. M., & Feeley, T. H. (2014). Risk information seeking and processing model: A meta-analysis. *Journal of Communication, 64*(1), 20-41. https://doi.org/10.1111/jcom.12071

Yoo, W., Choi, D.-H., & Park, K. (2016). The effects of SNS communication: How expressing and receiving information predict MERS-preventive behavioral intentions in South Korea. *Computers in Human Behavior, 62*, 34-43. https://doi.org/10.1016/j.chb.2016.03.058

Zeballos Rivas, D. R., Lopez Jaldin, M. L., Nina Canaviri, B., Portugal Escalante, L. F.,

Alanes Fernández, A. M., & Aguilar Ticona, J. P. (2021). Social media exposure, risk perception, preventive behaviors and attitudes during the COVID-19 epidemic in La Paz, Bolivia: A cross sectional study. *PLoS ONE, 16*(1), e0245859. https://doi.org/10.1371/journal.pone.0245859