

賄選疑義解析—以實務見解為例

新竹市政府政風處副處長/李志強

清流 MJIB

賄選疑義解析— 以實務見解為例

◆ 新竹市政府政風處副處長 — 李志強

九合一公職人員選舉將於 11 月 26 日舉辦，每逢選舉，賄選事件便層出不窮，眾人皆知候選人若支付現金買票即構成賄選，實務而言，何種情況會構成賄選？

常見疑義解析

一、賄選標準 30 元？

法務部曾於 90 年間函釋，以價值新臺幣（下同）30 元以下之單一宣傳物品作為檢察機關查察賄選之參考，以致長期以來候選人甚至是民眾多認為只要候選人致贈不超過 30 元的宣導品就不會構成賄選，但

法院判決則認為上述僅供參考，尚不得拘束法院對於個案之判決。

為維護選舉之公平性，雖應嚴禁候選人以不公平之金錢手段競選，但何謂不公平，則應於不違背國民之法律感情與認知下，就社會一般生活經驗而為判斷。即審酌行為人可能之主觀犯意外，亦應斟酌該



法務部於 2022 年 10 月 18 日公布 28 項妨害選舉類型，除走路工等 23 項傳統賄選型態，並新增「線上遊戲點數、第三方支付、手機行動支付、虛擬通貨等新興數位工具」、「約其放棄競選（搵團仔湯）」、「虛偽設籍（幽靈人口）」、「不實訊息（黑函、假訊息）」及「境外勢力資金滲透介入選舉」等 5 項犯罪類型。而沿用多年的發放 30 元以下「文宣品」不違法，但僅限於附著文宣之宣傳品，若非文宣品而贈送其他物品時，檢察官將會依法偵查。

禮金、禮品於客觀上是否可能影響選民之投票意願，同時參酌一般社會通念而為綜合考量。

二、何謂對價關係？

《公職人員選舉罷免法》之投票行賄罪，係指對於有投票權之人，行求期約、交付賄賂或其他不正利益，而約其不行使投票權或為一定之行使為構成要件。至對價關係，在於行賄者之一方，係認知其所行求、期約或交付之意思表示，乃為約使

有投票權人為投票權一定之行使或不行使；而在受賄者之一方，亦應認知行賄者對其所行求、期約或交付之意思表示，係為約使其為投票權一定之行使或不行使。

三、賄選對象僅限於有投票權人？

首先，《公職人員選舉罷免法》另定有對選舉區內之團體或機構賄選罪，旨在團體或機構之構成員間彼此互為影響而形塑一定之凝聚力，倘對該團體或機構賄選，足以影響或動搖其構成員之投票意向，而

達到實際影響投票之效果，其惡性不亞於對有投票權人直接行賄罪。

再者，行為人間接透過對團體或機構之行賄，其對象雖非構成員，且只要有使該構成員為一定投票權之行使或不行使為已足，不以該構成員確已行使或不行使其投票權為必要，但該賄選行為仍須具有交換選民投票權之對價關係，始足構成。

倘若行為人之捐助經評價尚未逾社會相當性之範圍，諸如參與民俗節慶、廟會活動，贈送禮金、禮品顯與社會禮儀相當者，即不能僅因捐助人或其助選人員有趁機請託其構成員投票支持之行為，遽認兩者間具有對價關係而予論罪。

四、在活動場合送禮並出現助選言論就會構成賄選？

於民主社會中，人民基於言論自由之保障，除公務員等具有特殊身分者應嚴守中立之立場外，任何人均得於競選期間，在各種公開或不公開之場合，發言支持某特定候選人。申言之，競選期間，在民間舉辦活動之場合中，候選人雖致贈相當價值之物品，且於活動中出現支持某特定候選人之助選言論，仍須釐清物品發放之來源及活動舉行之動機，是否確與選舉有直接密切之關聯，以及在場之人主觀上有無認識所收受財物係屬「賄賂」等情，故不能一律逕以投票行賄罪論處。



對價關係是指行賄者與受賄者均應認知行賄者對其所行求、期約或交付，係為約使其為投票權之行使或不行使。



法務部於 2022 年 10 月 18 日另公布 6 種不會構成賄選的行為態樣，包括「參與民俗節慶、廟會、婚喪喜慶，贈送禮金、禮品」、「為選舉造勢活動，提供參加民眾適度之茶水、簡便餐飲，不逾越社會常情者」、「為選舉造勢活動製作臨時性、簡便性之衣帽供助選人員作為辨識之用者」、「日常觀念認不具有相當價值之贈品，如門聯、桌曆、日曆、月曆等」、「單純動員群眾，以車輛載運往返競選活動會場」等常見選舉手法。（圖片來源：國家文化資產網，趙守彥攝，<https://nchdb.boch.gov.tw/assets/advanceSearch/folklore/20150123000003>）

五、提前賄選會構成犯罪？

司法實務認為，有關投票行賄或受賄罪之規定，旨在防止金錢介入選舉，以維護選舉之公平與純正。故候選人為求當選，於選務機關發布選舉公告前或其登記參選前，對於有投票權之人預為賄賂，請求於選舉時投票支持，已足敗壞選風。換言之，行賄時縱尚未登記參選，如其已著手賄選之犯行，日後並實際登記取得候選人資格者，即與該罪之構成要件該當，並不因其賄選在先，而影響犯罪之成立。

妨害選舉與非賄選行為態樣

因應日新月異的賄選手法，法務部新修訂「妨害選舉刑事案件例舉」，主要分成兩部分，第一部分是列舉 28 項原則上會構成妨害選舉的行為態樣，第二部分是列舉 6 項原則上不會構成賄選犯罪的行為態樣。

第一部分除囊括過去 23 項傳統賄選型態，另新增「線上遊戲點數、第三方支付、手機行動支付、虛擬通貨等新興數位工具」、「約其放棄競選（搓圓仔湯）」、



法務部解釋，6種不會構成賄選的行為態樣，均僅是彙整過去實務見解參考，若發生實際個案，例如：假借以車輛載運往返競選活動會場，實則為旅遊行程，屬迂迴逃避刑責，仍應由承辦檢察官視個別情狀審慎認定及依法偵辦。（圖片來源：載自三立新聞，<https://youtu.be/SJuYBXSZYs>）

「虛偽設籍（幽靈人口）」、「不實訊息（黑函、假訊息）」及「境外勢力資金滲透介入選舉」。

第二部分的非賄選行為，包括「以介紹候選人為內容之文宣品或以文宣附著於價值卅元以下之宣傳物品」，即發放卅元以下的「文宣品」不違法，但若是「贈品」，不論金額，檢察官仍會發動偵查，再依個案認定是否構成賄選。又如「參與民俗節慶、廟會、婚喪喜慶，贈送禮金、禮品」、「為選舉造勢活動，提供參加民眾適度之

茶水、簡便餐飲，不逾越社會常情者」、「為選舉造勢活動製作臨時性、簡便性之衣帽供助選人員作為辨識之用者」、「日常觀念認不具有相當價值之贈品，如門聯、桌曆、日曆、月曆等」、「單純動員群眾，以車輛載運往返競選活動會場」等常見選舉手法，亦不會構成賄選。

法務部解釋，以上行為態樣，均僅是彙整過去實務見解，若發生實際個案，仍應由承辦檢察官視個別情狀審慎認定及依法偵辦。

由俄烏戰爭 談CI安全防護

關鍵基礎設施防護研究室研究員—陳永全

清流

MJIB

由俄烏戰爭 談CI安全防護



◆ 關鍵基礎設施防護研究室研究員——陳永全

國家關鍵基礎設施在天然災害、資安威脅及恐怖攻擊以外，已面臨到更嚴峻的挑戰，那就是戰爭所引發的戰災。

CI 的最嚴峻考驗

俄烏戰爭從 2022 年 2 月 24 日開戰以來，似乎陷入了看似拉鋸但卻遍尋不著終點的局面，而隨著氣候逐漸步入寒冬，交戰情勢也更顯冷冽與膠著。

衛戍烏克蘭安全的軍隊，在俄羅斯不斷地攻擊下，竭盡所能，想方設法維持其境內國家關鍵基礎設施（Critical Infrastructure，下簡稱 CI）的安全，也為 CI 防護詮釋了在面臨天然災害、資安威脅及恐怖攻擊外，所遭遇到的更嚴峻考驗，那就是戰爭所引發的戰災。



烏克蘭國防部、武裝部隊網站、國家銀行遭受網路 DDoS 攻擊。
(Source: State Special Communications Service of Ukraine, <https://cip.gov.ua/en/news/shodo-kiberat-aki-na-saiti-viiskovikh-struktur-ta-derzhavnikh-bankiv>)

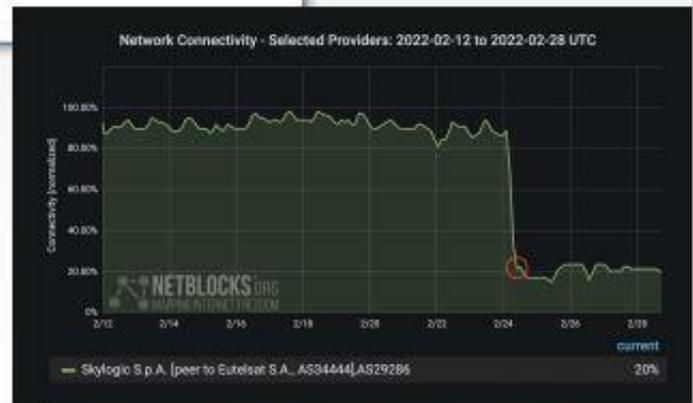
俄烏戰爭前夕—網路攻擊頻繁出現

俄烏戰爭開戰前一週，烏國即飽受疑似來自俄羅斯的駭客入侵，至少有 10 個以上與政府相關網站，包括國防部、外交部、文化部及 2 家國營銀行受到駭客攻擊；¹ 受攻擊網站都是被大量垃圾數據封包阻塞，使網站呈現癱瘓的狀態，研判是遭到大規模「分散式阻斷服務攻擊」(DDoS)。

DDoS 攻擊者運用多個盜用或掌控的來源持續不斷地攻擊目標，其意圖係讓烏克蘭民眾生活不便，造成其等恐慌，打擊民心士氣，進而製造社會的不安與動亂。

俄烏戰爭發起日—虛實攻擊併用

俄羅斯總統普丁於 2 月 24 日 5 時 50 分批准對烏克蘭發動「特種軍事行動」，



網路流量分析業者 NetBlocks 曾公開網路數據，顯示 2 月 24 日烏克蘭和歐洲大部分地區的網路連線中斷，後證實為隸屬美國電訊公司 Viasat、支援該區的 KA-SAT 衛星在戰爭中遭受駭客攻擊。(Source: NetBlocks twitter, <https://twitter.com/netblocks/status/1498365220107997191>)

烏國總統澤倫斯基旋即於 7 時發布緊急動員命令。在開始進行全國動員任務之際，多數烏府網站遭受駭客攻擊，網站失能癱瘓。據烏國數位轉型部表示，大規模 DDoS 除針對境內多家銀行外，亦發現駭客鎖定烏國防部的郵件伺服器，利用殭屍網路病毒 Dana Bot 進行攻擊。

¹ "Ukraine's defence ministry and two banks targeted in cyberattack", <https://www.euronews.com/my-europe/2022/02/15/ukraine-s-defence-ministry-and-two-banks-targeted-in-cyberattack>.



俄羅斯在 2 月 24 日當天進行超過 2 百次襲擊，摧毀癱瘓多處機場與導彈系統，其中包含全世界機身最長、承載重量最大的飛機 AN-225 Mriya。（Photo Credit: Kyiv City Council, <https://w.wiki/5pGe>）

在實體軍事攻擊上，據《法新社》報導，俄羅斯在 2 月 24 日當日進行超過 2 百次襲擊，俄國防部更於 2 月 24 日當晚宣稱，其已導致烏境內 11 處機場、3 個指揮所、1 處空軍基地、18 處 S-300 型地對空導彈系統和 1 處薩姆（SA-11）型導彈系統，全數摧毀癱瘓。

俄烏戰爭開戰後第一週—— 網站攻擊大爆發

俄烏戰爭開戰後的第一週內，相關網路攻擊事件更是不斷傳出，從政府機關、石油公司、軍事單位等，到電視臺、學術機構、協助烏克蘭難民的歐洲國家官員，也相繼成為駭客下手的目標。²另

有駭客入侵竄改烏政府網站，散發意圖動搖軍心士氣的不實訊息。例如，烏國特別通訊暨資訊保護局（State Service of Special Communications and Information Protection, SSSCIP）與安全局（Security Service of Ukraine, SSU）發現，駭客入侵烏國地方政府網站，宣稱「烏克蘭已經投降，俄羅斯和烏克蘭即將簽署和平協議的不實訊息與謠言」。烏克蘭議會也提出類似警告，指駭客入侵赫爾松公共廣播新聞臺，散布烏國投降的謠言。此外，烏國安全局也指控俄國軍事情報局（GRU），利用 Telegram 頻道不斷散發類似「烏克蘭政府即將投降及兩國即將簽署和平協議」等不實訊息。

² 《【資安週報】2022 年 3 月 1 日至 4 日》，<https://www.ithome.com.tw/news/149711>。

戰爭初始，腹地廣大的烏國民眾根本無從辨明訊息的真偽；俄軍突如其來的特別軍事行動，尤其是早有計畫地運用虛假訊息作為，除讓烏府措手不及外，更增添烏府在開戰初期緊急動員人力的難度。

俄烏戰爭開戰後迄今— 持續不斷的 CI 攻擊事件

茲針對俄烏戰爭期間之 CI 攻擊態樣與影響層面整理如下頁表 1。開戰後，俄羅斯

軍隊步步進逼，不間斷地奪控烏境內 CI，3 月即占領烏南札波羅熱（Zaporizhzhia）核電廠，該廠是歐洲最大核電廠，也是全球十大核電廠之一。由於俄烏雙方在核電廠周邊不停交火，更引發舉世擔心核災因此爆發之恐慌。

針對 CI 的網路攻擊，根據 SSSCIP 公布資料，俄羅斯攻擊目的，有 242 件涉及資訊蒐集，192 件是為了植入惡意程式；攻擊標的，有 179 起是鎖定該國與地方政府組織，104 起是針對安全與國防部門，另有 54 起鎖定能源產業。³



СЛУЖБА БЕЗПЕКИ УКРАЇНИ



俄國駭客入侵烏克蘭政府網站，佯稱烏克蘭已投降，兩國要簽署和平條約，烏克蘭安全局而後發布闢謠消息。
(Source: Security Service of Ukraine twitter, <https://twitter.com/ServiceSsu/status/1499418645537116160>)



從衛星空拍可見烏克蘭札波羅熱核電廠之俄烏交火對峙，引發舉世擔心核災爆發之恐慌。
(Photo Credit: Planet Labs, <https://www.planet.com/gallery/#/post/zaporizhzhia-nuclear-power-plant>)

³ 本統計數據截至 2022 年 6 月。《烏克蘭統計自開戰以來已遭到近 800 次網路攻擊》，<https://www.ithome.com.tw/news/151719>。另截至 2022 年 8 月底，烏克蘭電腦緊急回應組（CERT-UA）已檢測到 1,123 次網路攻擊。"Ukraine has recorded over 1,100 cyberattacks since the beginning of the year", <https://cybernews.com/cyber-war/ukraine-records-over-1100-cyberattacks>.

表 1 俄烏戰爭中受攻擊之 CI 設施

項次	CI 分類	被攻擊目標	衝擊影響
一	能源 關鍵基礎設施	1. 烏克蘭車諾比核電廠 2. 烏克蘭札波羅熱核電廠 3. 俄羅斯煉油廠 4. 烏克蘭哈爾科夫電廠 5. 烏克蘭卡霍夫卡電廠 6. 烏克蘭阿佐夫斯卡爾煉鋼廠	大規模停電
二	水資源 關鍵基礎設施	1. 盧甘斯克州 (Luhansk) 供水站 2. 北頓涅茨河水庫 3. 基輔水庫	大規模斷水
三	資通訊 關鍵基礎設施	1. 烏國與地方政府組織 2. 國安與國防部門 3. 銀行金融機構 4. 商業機構 5. 能源部門 6. 其他部門	大規模網路中斷
四	交通 關鍵基礎設施	1. 文尼察國際機場 (Vinnytsia) 2. 敖德薩機場 3. 斯韋托戈爾斯克橋樑 4. 馬立波港口 5. 克里米亞大橋	陸海空交通受阻
五	銀行與金融 關鍵基礎設施	1. 烏克蘭國營銀行 Privat bank 2. 烏克蘭儲蓄銀行 Oschad bank	金融交易 大規模中斷
六	緊急救援與醫院 關鍵基礎設施	1. 烏克蘭馬立波 (Mariupol) 醫院 2. 烏克蘭約 400 家醫療院所	緊急救援 服務中斷
七	中央政府與主要都會 關鍵基礎設施	1. 烏克蘭國防部網站 2. 烏克蘭外交部網站	訊息傳遞受阻
八	高科技 關鍵基礎設施	1. 烏克蘭基輔衛星服務站 2. 烏克蘭數位轉型部網站	重要通信傳播訊息 傳遞受阻

資料來源：作者自行整理。

他山之石，可供借鏡

在戰事發動後，烏國並不像外界預期地被斷網斷訊，反而能號召網路戰士反制俄羅斯駭侵，且透過不間斷地對外傳送戰況，以及進行種種心戰喊話影音，讓俄方未能達到「速戰速決」的作戰目標。

這歸因於近 10 年來俄羅斯對烏克蘭的數次大規模網攻經歷，尤其是 2017 年的「NotPetya」勒索軟體事件，⁴其攻擊烏國境內私人企業與銀行等，造成數億美元的損失。烏國經此事件成為數位焦土後，烏府痛定思痛，傾盡全力地強化網路防禦能

力，透過中斷對俄能源依賴及在世界各地建立資料庫等方式，成功打造出強大韌性的網路安全系統。⁵

另戰爭一開始，烏國數以百計的中小型網路業者，主動冒著生命危險努力維持網路運作，尤其是當光纖電纜遭俄軍炮火破壞後，該國電信業者儘快搶修恢復通訊



美國國際開發署與 Space-X 合作，提供烏克蘭 5,000 個衛星接收終端設備，讓烏方在戰爭中得以維持通訊傳輸。(Source: Mykhailo Fedorov twitter, <https://twitter.com/FedorovMykhailo/status/1498392515262746630>)

的效率，頗令外界印象深刻，所以當俄軍入侵後，烏國網路始終保持暢通，這也讓澤倫斯基能透過視訊對全球喊話，進而得到驚人的外界馳援。加以美國 Space-X 大舉援烏衛星通訊，更是讓烏方得以維持通訊傳輸、發動網攻以及認知作戰攻防的重要利器。⁶ 因此，從烏國過去教訓直到發展出強大網路防禦等的相關經驗，實值得我方多加借鏡學習。

全災害風險管理概念

面臨戰爭的嚴峻考驗，須知 CI 防護之災害管理不應只有強調應變或是整備，災害管理政策要能成功推行，必須要完整地考量災害管理的四階段（預防減災、整備保護、應變、復原）全面作為，並互相配合，相輔相成。

換言之，即管理方式事實上與災害類型無關，而是對應各種災害都應該如此處理；且當管理災害方式能跳脫出僅侷限於純粹應變的思維，以災害管理四階段的角度思考—即全災害管理（All-Hazards approach）時，在人、實體及網絡面向上均妥善地加以管理，方可降低各項風險與各類型災害所帶來之危機。

⁴ "US charges Russian hackers blamed for Ukraine power outages and the NotPetya ransomware attack", <https://techcrunch.com/2020/10/19/justice-department-russian-hackers-notpetya-ukraine/>.

⁵ 《烏克蘭數位戰全靠他！31 歲科技部長花費 2 年強化網路韌性，俄國網軍難以善後》，<https://www.storm.mg/article/4258342>。

⁶ 《俄烏戰事中的網戰攻防、數位韌性與其對全球網路治理之衝擊》，<https://indsr.org.tw/respublicationcon?uid=12&resid=1875&pid=1629>。



災害管理四階段的全面作為（左）與安全防護的管理要領（右）。（資料來源：行政院國土安全政策會報，《國家關鍵基礎設施防護演習參考手冊》、《國家關鍵基礎設施安全防護指導綱要》，<https://ohs.ey.gov.tw/Page/6C4A1386ACBA6734>）

我網路安全情勢嚴峻，堪稱首見

8月3日美國眾議院議長裴洛西來臺訪問，中共運用網路攻擊我便利超商、臺鐵、高鐵車站看板，並顯示不雅涉及人身攻擊文字等；另加以入侵我公路總局、台電電網、內政部警政系統、高雄市環保局官網、外交部甚至是國防部網站等，⁷造成部分網站癱瘓、人心惶惶。此等全面遭入侵攻擊事件，堪稱臺灣首見，亦不輸俄

烏戰爭前夕之俄國駭客頻繁入侵烏國網站情節。

然以正面態度觀之，此次中共軍演與駭客攻擊，無疑係對我形成最佳的CI安全防護總體檢。另藉由觀察俄烏戰爭的過程，我政府與國人應深刻體認、從中學習，進而發揮災害管理思維，以主動積極態度及早部署與加強數位韌性，方能面對CI安全防護的最嚴峻挑戰。



⁷ 《臺灣 8 月初因裴洛西訪臺而遭到網路攻擊的事件總覽》，<https://www.ithome.com.tw/news/152491>。