出國報告（出國類別：進修）

參加美國哈佛大學甘迺迪學院「台灣領袖計畫」進修報告

「網路安全: 政策與科技之交會」研習課程

(Cybersecurity: The Intersection of Policy and Technology)

服務機關：外交部公眾外交協調會
姓名職稱：林佾靜科長
派赴國家/地區：美國/波士頓
出國期間：**112**年**7**月**26**日至**8**月**9**日
報告日期：**112**年**11**月

目　　次

摘　要

職獲本部「哈佛-台灣領袖計畫」之遴選，於本(112)年 7 月 26 日至 8 月 9 日期間赴美國波士頓參加美國哈佛大學甘迺迪政府學院(JFK School of Government)新開設之「網路安全: 政策與科技之交會」(Cybersecurity: The Intersection of Policy and Technology)研習課程。該學院期以透過開設本項課程擴大網路安全政策及技術兩大領域專業人士之對話交流，引領政府部門及企業組織除持續提升資安防護能力外，亦須重新建立對「網路安全」分析架構及威脅型態，同時釐清行為者發動攻擊之目的及如何取得網路控制的機制；另資安防護必須從「事後補救」轉為「事前防禦」之思維，方能制定有效因應策略。

本研習課程邀集美國及歐盟等主管網路安全官員及產學專家，透過授課、專題討論及情境模擬等方式，引導各國參訓學員深入瞭解當前全球網路安全重要議題以及探討因應各類網路安全威脅之策略制定。參訓學員來自美國、歐盟、亞洲、拉丁美洲及非洲等國政府官員及企業中高階主管，透過密集意見交流、資訊分享及深度探討，可綜觀各國界定網路安全威脅型態及採取相關因應策略之異同，利於建立跨國資訊交流及政策討論之交流平台，亦有助於理念相近國家間雙向瞭解公私部門管控網路安全風險之相關作為。

一、 參訓目的

職獲本部「哈佛-台灣領袖計畫」之遴選，於本(112)年 7 月 30 日至 8 月 4 日赴美國波士頓參加美國哈佛大學甘迺迪政府學院(JFK School of Government)新設之「網路安全: 政策與科技之交會」(Cybersecurity: The Intersection of Policy and Technology)研習課程。課程主持人 James Waldo 教授為該校資訊工程及公共政策資深教授，期透過開設網路安全主題課程擴大政策及技術兩大領域專業人士之對話交流(註: 網路安全議題前分屬該校國際安全及電腦資訊工程，無獨立開設專題研習課程)。另本課程訓練強調政府部門及企業組織除持續提升資安防護能力外，須重新建立對「網路安全」認知及分析架構，因應不同之網路攻擊模式，必須同時探討行為者發動攻擊之目的及如何取得控制的機制；另資安防護必須從「事後補救」轉為「事前防禦」之思維，綜此方能制定有效因應策略。本研習課程邀集美國及歐盟主管網路安全官員及產學專家，透過授課、專題討論及情境模擬等方式，引導各國參訓學員深入瞭解當前全球網路安全重要議題以及探討因應各類網路安全威脅之策略。

參訓學員透過密集意見交流及深度探討，可綜觀各國界定網路安全威脅型態及採取相關因應策略之異同，以利建立日後資訊交流及政策討論之交流平台，亦有助於理念相近國家間雙向瞭解公私部門管控網路安全風險之相關作為

二、 參訓過程

(一) 學員組成

來自美國、歐洲、亞太、非洲及中南美國家政府官員、國際組織與企業高階主管等主責資安決策人士及技術專家等參與本項研習課程，涵蓋國防、外交、國家安全、資通訊科技、金融財政、公衛及航運等專業領域等計 60 餘人，

深具豐富實務經驗，十分熱中參與各項研討活動。其中半數來自美國國防部門及各級政府體系主管軍事及網路安全事務官員，關注網路攻擊對美國構成之軍事威脅；另有世界銀行(World Bank)、非洲及亞洲國家中央銀行及跨國商業銀行高層主管參訓，較為關注跨境數位金融之安全性與穩定性。

(二)　課程安排

1. 課程主旨:

(1) 本項課程為哈佛大學甘迺迪學院於本年首度開設「網路安全專題課程」，盼結合網路安全相關議題之公共政策及國際安全學者專家，透過授課、小組討論、專題報告及情境模擬等方式引導參訓人員從個人、企業、國家及全球範疇等不同分析層次探討對應之網路安全威脅，以及軟硬體資訊系統安全防護之創新策略；

(2) 課程內容設計著重全球網路攻擊(global cyber attacks)態樣分析、國家及企業資訊安全危機管理、資安防護技術創新以及地緣政治衝突與網路安全等議題。總結課程主題內容簡列如下: (各項課程主題詳附件〔課程表〕)

- 網路自由及國家安全優先順位之辨證:權衡個人隱私保護及維護公共利益兩者重要性；建立網路安全管制之全球治理體制；
- 網路安全與國際衝突之相關性: 探討網路「武器化」及引發核武及傳統戰爭之隱憂；
- 惡意網路攻擊行為者之動機及公私部門風險危機: 網路攻擊已具策略性目的及行為模式，政府及企業除需解決系統修護之技術問題外，亦將面對組織信任及存續危機；
- 資訊安全防護之趨勢發展: 檢視資安漏洞修護技術發展歷程；探討「零時差網攻」(zero-day attacks)對國家及全球安全造成之重大威脅；

- 人工智慧(AI)對網路安全之影響: 探討 AI 科技對於全球政治經濟關係之影響，是否將導致國家及資本主義權力更為集中，集團化最終取代自由市場。

2. 課程進行方式: 透過講師授課、分組討論、專題報告及模擬情境演練等方式，以多層次、多管道之交流互動，建立深度參與及團隊合作之多元交流模式。

3. 講授網路安全相關學者專家舉列如下:

(1) 歐盟網路安全政策: Despina Spanou (歐盟執委會數位政策高階官員)；

(2) 國際網路安全及地緣政治研究: Melissa Hathaway(曾於布希及歐巴馬政府時期擘劃美國政府網路安全政策)、Lucas Kello(英國牛津大學國際關係教授)、Herb Lin(史丹佛大學國際安全與合作中心及胡佛研究中心資深研究員)、David Stranger(紐約時報知名記者，專精美國國家安全、外交政策及白宮等政治報導及評論，並熟諳台灣議題)；

(3) 企業/大型組織資安防護政策: Brad Chen (Google 隱私權部門高階主管)、Michael Tran Duff (哈佛大學資訊長)、Ryan Ellis (西北大學溝通研究教授)；

(4) 網路安全防護技術創新: Jim Waldo、Susan Landau (塔夫茨大學(Tufts University)網路安全政策教授)、Edlyn Levine (美國前沿基金 (AFF)共同創辦人及首席科學官，前身為 MITRE Corporation)、Allan Friedman (美國商業部網路安全計畫官員)、Bruce Schneier (美國著名密碼學及資訊安全專家；美國 BT 公司創辦人)。

4. 分組討論及報告:

專題討論個案包括: (1) 臉書 (FB) 支付巨額款項解決用戶隱私權集體訴訟問題；(2)中國以民眾之名為隱蔽發動網路攻擊；(3) 零時差(zero-day)網路攻擊及修護模式，以全球網通大廠思科(Cisco)資安漏洞為例探討攻防兩造競逐關

係；(4) 不特定個人查獲廠商資安漏洞，其交付程序碼動機及行為模式 (無償交付廠商或第三方，或進行贖金交涉)；(5)加密技術限制下探討無密碼防護模式及 AI 測試模組之可行性。

5. 網路安全情境想定討論及模擬:

(1) 個案情境想定課堂討論: 2027 年 3 月，美國掌握中國政府預備發動惡意程式進行毀滅攻擊，以癱瘓美國關島、夏威夷及加州地區基地，獲報可能對台灣進行第一波攻擊行動，美方應如何評估及因應威脅及衝突危機?

(2) 個案情境想定模擬演練:

-模擬喬治亞州遭遇疑似網路攻擊事件，在各類情境想定中進行虛實訊息判定及建立各階段危機應變行動方案。全員分成兩組，各組均設立白宮、喬治亞州州長辦公室、喬治亞州電力危機應變團隊、國土安全部、情報單位、能源部及國防部等單位，並分處不同演練空間，限定僅能透過網路平台傳達訊息；

- 演練計畫由主控室發布情境訊息，由各組進行訊息來源查證、網路風險及機關職能評估，及時回報決策及執行模式及進行部門間協調溝通；藉此情境演練瞭解一國因應網攻危機涉及政府部門及職能，以及對國家安全影響之層面。

三、 觀察心得及建議

(一) 網路攻擊(cyberattack)已構成國家及全球安全之重大威脅，等同傳統軍事安全風險

1. 相較於千禧年時期對於「網路空間」(cyberspace)及「網路安全」(cybersecurity)之定義及議程，在高度數位化之人類活動場域，網路安全已跨越個人(person)及企業(business)層次，提升到國家(state)及全球範疇(global scope)，並從個人/企業資料防護及技術創新提升到國際安全層面，同時呈現傳統安全

(traditional security)及非傳統安全(non-traditional security)之威脅態樣，前者如癱瘓國家基礎建設、加劇戰爭及國際衝突情勢及引發核武危機，後者則如干擾全球經貿、金融、航運及緊急救援等體制穩定。

2. 國際社會憂慮網路空間受到「安全化」(securization)、「武器化」(weaponization)及「地緣政治化」(geo-politicization)之不當操弄情形，網路攻擊已具軍事及政治意涵及具體實踐，遂構成國家及全球安全之重大威脅。現今網路安全領域已從個資及商業機密遭竊、資安系統漏洞及網路詐欺，擴及國家體制運作及國防外交安全威脅，網路攻擊已跳脫個人或不特定團體之無差別惡意行為模式，逐漸發展成「國家化」之目標攻擊模式，目的在於遂行一國對外軍事、政治及外交目的，從而形塑出新的國家衝突及戰爭型態。

3. 近年歐盟及美國等國已視中國及俄羅斯兩國為主要網攻國家。參訓期間正值俄烏戰爭及中國持續升高台海緊張情勢，授課講師及各國學員均高度關切中、俄兩國採取網路攻擊之態樣及對國際安全之威脅，兩國已將網路行動(cyber operation)納入國防軍事體系，並視為和平時期之作戰策略，引起國際嚴正關切，如美國軍方刻高度戒備中國可能透過惡意程式(Malware)發動網攻以干擾及破壞美方軍事行動。國際安全社群主張美國、歐洲及北大西洋公約組織(NATO)等必須改變過往因應網攻威脅之被動態勢，轉而採取主動防禦策略(offensive strategy)，如俄烏戰爭中烏克蘭之網路安全防衛戰略即為成功策略。

4. 全球網路空間社群已有共識，認為網路空間已跳脫「自由無害場域」及「去管制化」(deregulation)的特性，日益支持一國政府及國際組織主動管制網路風險及建立全球網路安全治理機制，此係鑒於網路空間現已成為「不安全場域」，倘若政府與公民社會均無法建立有效管制網路威脅，最後將形成「惡意場域」；鑒此，針對惡意網路攻擊，國際體系必須以主動反擊達到嚇阻防禦目的。相

關課程檢視國際組織及各國因應全球網攻威脅所制定之策略及政策架構，如聯合國研議建立國家網路行為責任準則；美國本(2023)年制定「國家網路安全戰略」(National Cybersecurity Strategy)；另歐盟法制架構最為完備，重要法案及政策包括: (1)「歐盟網路安全法案」(The EU Cybersecurity Act)；(2)「歐盟網路韌性法案」(The EU Cyber Resilience Act)；(3) 「歐盟網路強化法案」(The EU Cyber Solidary Act)；(4) 「歐盟網路安全認證架構」(The EU Cybersecurity Certification Framework)；並設立歐盟網路安全執法單位及建構全球網路安全防禦體系，目的在於建立 27 個會員國因應網路安全威脅之共同政策及行動架構，強調相互能力建構及強化韌性之區域防護體系，也以此擴展為與其他國家合作之基礎架構。

(二) 台灣地緣政治戰略地位及全球半導體產業關鍵角色獲得廣泛重視

1. 課程期間，中國發動台海軍演及製造台海不安情勢引起廣泛討論，多位授課講師均提及中國對台之軍事威脅及網路攻擊態樣，可能成為攻擊其他國家之模式，更以台灣遭受中國攻擊為想定情境進行課堂討論個案(詳上文情境想定演練個案)，獲得學員熱烈討論並詢及台海情勢發展。渠等向職詢及我國政府如何因應中國軍事威脅及網路攻擊，顯現各方日益關注台灣位處第一島鏈及台灣半導體產業領先地位之戰略意涵。綜整參訓官員關切台灣議題如下:

(1) 中國軍事威脅對台灣半導體產業之風險評估;我國政府如何強化國內半導體產業安全防護；

(2) 「矽盾」一說是否確切? 台積電海外設廠佈署策略；

(3) 兩岸是否將於近期發生戰事? 是否高度依賴美方協防?

(4) 台灣是否具因應「網路戰」之軍事及資訊能力；

(5) 台灣民眾對於台海衝突情勢之看法等議題；

2. 針對上揭詢問，職已於課堂中及各式交流場合適機說明台灣半導體產業發展歷程及無法輕易被取代或仿製之特殊性；另也提供當前中國片面升高台海及區域緊張局勢之因素分析、我國因應中國軍事威脅採取之防衛戰略及台灣民意觀點，以及我國強化與民主陣營國家合作關係之重要安全意涵。

(三) 我國須制定參與全球網路安全建制之優先議題及策略

1. 綜上，授課講師及參訓學員已注及台灣深受中國軍事及網路攻擊威脅之情形，也充分瞭解台灣戰略位置及半導體產業之於全球安全及高科技產業之重要性。渠等十分關注我國在因應中國網攻之能力，因除涉及台海及區域安全，亦事關全球晶片供應穩定。職已適機說明我政府已將資訊安全視同國家安全之一環，台灣是中國境外網攻之熱點，隨中國加大對台軍事威脅，中國駭客組織更為頻密入侵企圖癱瘓台灣關鍵基礎設施。為因應中國網路攻擊威脅，我國政府持續強化國家資安指揮體系及應變韌性，如行政院成立數位發展部及資通安全署、國防部成立資通電軍、立法院也通過《資通安全管理法》等，另也協助企業及民眾資安防護之能力建構；另台灣與民主陣營國家緊密合作關係已對中國軍事冒進形成集體嚇阻力量。
2. 經查我國相關政府部門已制定國家資訊安全戰略，惟尚未建立公私部門協作因應機制及法制架構。尤以各國當前都十分關切「零時差網攻」之安全威脅，憂懼駭客無預警逕自攻擊尚未修補之資安漏洞，透過單方網路端入侵個人隱私、偷取商業機密及摧毀公共設施及全球產業鏈，亦能在分秒間癱瘓世界正常運作之毀滅行徑。面臨此等網攻威脅，許多國家政府現已採取事前預防之主動防禦策略，取代事後修補之被動應處，如美國將採取更具主動性之嚇阻戰略，宣示將竭盡國家力量打擊惡意威脅者，讓不負責任的國家行為付出代價，以確保美國國家安全；另亦積極建立公私部門之全球跨域聯防機制，如

歐盟等民主國家刻大規模建構因應跨境網路安全之法制及政策架構，並已明訂清晰之優先議題及行動方案；顯示未來國際社會將對於全球網路攻擊採行更為強勢因應作為，並建立新的國家責任典則。

3. 鑒於我國與民主陣營國家合作夥伴關係日益深化，為強化在網路安全合作關係，我國應儘速完備國內網路安全法制及國際合作架構，將有利發揮台灣專業優勢及與全球關鍵議題領域對接，以參與全球跨域聯防協作網絡及建立共同網路威脅防禦行動準則，進而強化我國資安防護能力及危機應變韌性。