OECD 與歐盟資安政策的策略發展與政策挑戰

科政中心 科研資料組
游婘茹

中文摘要

OECD 和歐盟在「政策制定循環」(含問題確認階段、政策形成與安排階段、決策階段、執行階段和評估階段)中的政策形成與安排階段發展資安策略。經過 20 年，資安策略的焦點已被調整從保護個人與機構組織，轉變為保護整體社會經濟。本研究分析 OECD 和歐盟如何設計發展新資安策略，包含：所遵循的基本原則，用以支持資安政策決策的統計證據，資安策略的跨單位協調合作機制，並探討目前正在解決的政策挑戰。本研究運用質性資料分析方法，調查 OECD 主要國家(包含：荷蘭、英國、德國、法國、芬蘭、澳大利亞、加拿大、美國與日本)新資安策略的主要目標，負責規劃的單位，與執行資安策略的單位。

再者，本研究發現 OECD 和歐盟面對的政策挑戰包括：組織的權利責任和成員國主權間平衡的不易，結構複雜的分工合作與管轄權，以及多元的國內與國際利害關係人間的溝通協調。儘管發展資安策略中面臨了政策方面挑戰，OECD、歐盟及其成員國皆認同對抗資安犯罪並增強資安能力，及國際相關組織共同合作的重要性。

The development of cybersecurity strategies and its policy challenges in the OECD and the European Union

Abstract

The OECD and European Union designed their cybersecurity strategies at the early stage of the policy-making cycle—the stage of policy formulation. In the 20 years since the OECD nations and the European Union first proposed their initial cybersecurity strategies, their focus of the cybersecurity strategies has been shifting from protecting individuals and companies online to strengthening the competencies of a nation and economy in the digital world. This research report investigated how new cybersecurity strategies have laid out in the OECD and the EU (i.e., principles, coordination mechanism, and statistical evidence for policy decision-making) and what policy challenges they are dealing with. The Qualitative Analysis Method is used, investigating the main goals of new cybersecurity strategies, the priorities of governments, and the units that take charge of the implementation of new cybersecurity strategies within the 9 OECD nations (incl. Australia, Canada, Finland, France, Germany, Netherlands, Great Britain, America, and Japan). Major policy challenges were identified as the delicate balance between member countries' sovereignty, the organizations' authority (i.e., the OECD and the EU), and responsibilities, the complex set of cybersecurity policy cooperation, and the coordination and communication with diverse stakeholders at national and international levels. The research findings suggested that in order to mitigate cyber risks, the OECD, the EU, and their member countries invariably strengthen their cybersecurity capabilities with specialized agencies by following new cyber security strategies, even though intractable challenges have to be solved.

一、 前言

自 2011 年起，資安政策已成為歐洲安全與合作組織(OECD)與歐盟執行委員會(European Commission)的重點政策。在政策制定循環(policy making cycle)中分為五個階段：(1) 問題確定(Issue Identification)；(2) 政策形成(Policy Formulation)；(3) 決策(Decision Making)；(4) 執行(Implementation)；(5) 評估(Evaluation)；而政策策略是在規劃階段中被發展而成。從新資安策略與過去策略間不同的規劃可看出，OECD 和歐盟決策者對資安問題所關注的焦點與新資安策略的發展範圍，已從過去的保護個人與機構組織，轉變為保護整體社會經濟。而讓資安策略有所調整和改變的原因是網路的角色對社會與經濟的重要性不斷提高，舉例而言，在過去的時代，網路對個人和機構組織是提供資訊的有用平台，國家執行資安政策主要是為預防和管理網路失誤對個人與機構所造成的損失，但是，在現代化的社會裡，網路對整體經濟舉足輕重時，所造成的失誤後果將會影響整個社會經濟。

本研究報告重點在於探討 OECD 主要國家(包含：澳大利亞、加拿大、芬蘭、法國、德國、荷蘭、英國、美國和日本)與歐盟在政策執行階段之前，發展出哪些新資安策略，規劃新資安策略的考量面向，例如：決策者考量的統計證據、政策規劃所依循的概念和原則。另外，再進一步分析，於執行階段中，OECD 主要國家新資安策略的執行目標等，以及歐盟各機構間的協調合作機制。最後，探討 OECD 和歐盟在執行資安策略中需解決的政策挑戰。

透過 OECD 與歐盟的經驗作法，本研究報告希望提供我國政策決策者在國家資安策略的規劃與決策、責任分工、協調合作、以及解決政策挑戰的參考。

二、 OECD 主要國家、歐盟國家的新資安策略

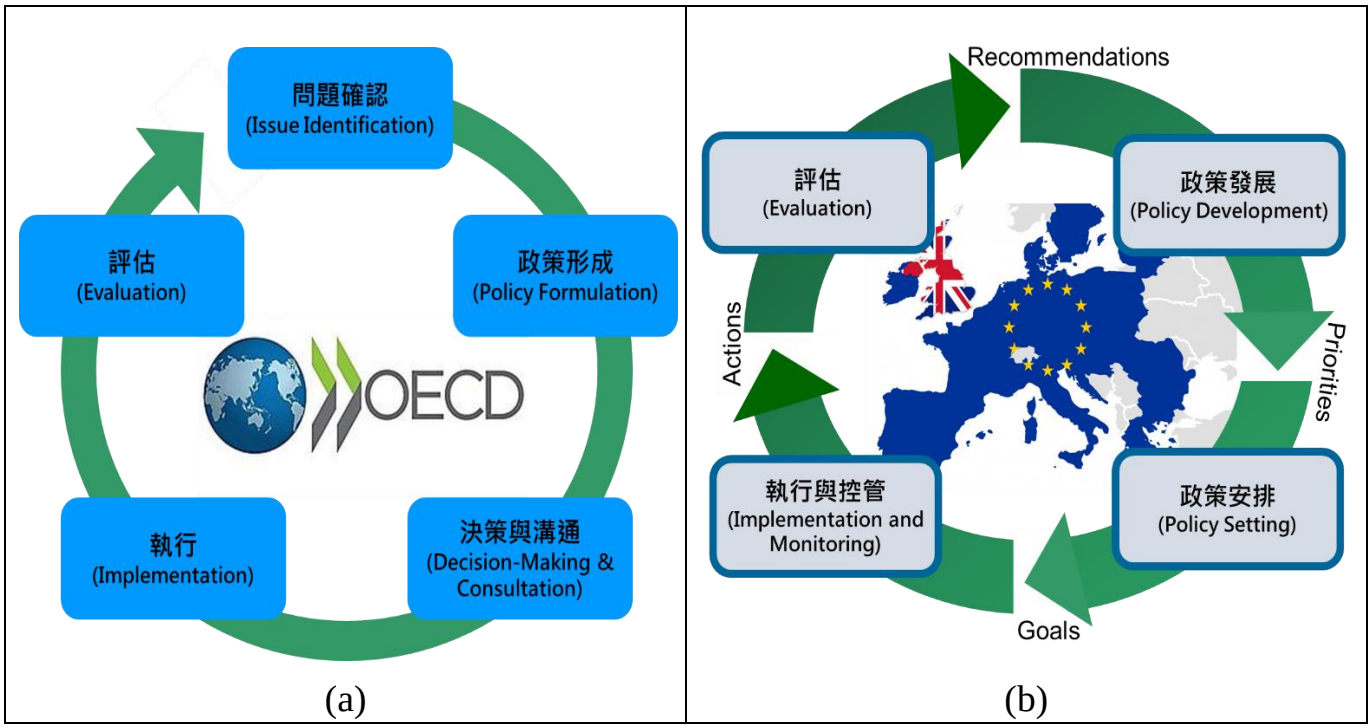
在 2000 年代早期，制定資安政策的目的為提高網路使用信任，讓網路環境的條件足以推動經濟繁榮和人民福祉，各國政府對於數位基礎設備的

建設著重在使用性和效率，而非安全性(US White House, 2009)。但在二十年後，世界各國政府皆面臨到不同的狀況：網路經濟成為推動國家成長的重要資源，也是在許多經濟領域中提供機會創新的平台；在這段期間，網路所存在的科技弱點(technical vulnerabilities)大致上無改變，但有改變的是，社會與經濟十分依賴於不安全的網路環境(OECD, 2012)。因此，解決資安危機成為各國政府的首要任務，因此需要發展策略性方案來保護社會整體。

(一) OECD 與歐盟政策策略發展

OECD 的政策制定循環基本上分為五個階段(如圖一所示)。在問題確認階段，國家的最高管理體系含議會(parliament)、國會(congress)、元首(monarch)或總統(president)共同參與問題分析與確定；在政策形成階段，政府部門(ministry)和內閣(cabinet)參與策略與政策工具的發展；在決策與討論階段，以聯邦政府管理為主，關鍵利害關係人共同達成協議；在執行階段，政府部會與機關運用律法和政策工具以達成政策目標；以及在評估階段，各政府機關進行效能管理、結果回報與審核。

另外，歐盟的政策週期是歐盟從 2010 年起處理重大危害事件所採用的方法；例如：處理網路犯罪，特別是線上交易與金融卡詐欺，網路兒童性侵害，和危害歐盟資訊系統的網路攻擊事件；此政策週期為期四年，分為四個階段(如圖一所示)。在政策發展階段，分析所面臨的問題對現階段和未來的歐盟會造成多少危害，提出優先順序；在政策安排階段，常務委員會(Standing Committee)審核優先順序，規劃出四年的策略性計畫，並列出政策週期內所要達成的策略性目標；在執行與管控階段，以營運行動計劃(Operational Action Plans)來執行已核准的策略性計畫與目標，由 National EMPACT Coordinators 進行計畫執行的管控，歐盟提供行政管理和法規方面的支持；在評估階段，每年進行委員會審查(commission review)和期中評估(interim assessment)，在評估階段裡所習得的成果，會是開始下一個政策週期的數據資料來源。



圖一：政策制定循環：(a)OECD；(b)歐盟

資料來源：Chapman, A., *et al.*(2016) & Council of European Union，本研究整理

綜上所述，在 OECD 和歐盟，一旦已存在的問題(如：網路犯罪)經過分析和確認後，政策制定者決定要處理該特定問題，並且設定政策目標與排序，接下來在政策形成階段，開始計畫和發展政策策略和政策工具來達成政策目標，以及確保未來的政策執行架構能夠被成功執行。

接續本研究報告將探討 OECD 和歐盟所規劃的新資安策略，以及規劃過程中的考量面向。

(二) OECD 主要國家的新資安策略

新資安策略的執行範圍含括了與經濟、社會、教育、法律、執法、科技、外交、軍事和情報相關的資訊安全。基本上是由州、區或中央政府的行政首長來支持整合性的資安策略。以下為 OECD 主要國家政府(包含：澳大利亞、加拿大、芬蘭、法國、德國、荷蘭、英國、美國和日本)在規劃新資安策略所遵守的四大概念：

1. 提升政府機關間在策略執行上的協調

當資安成為國家的重要安全問題時，政府有責任制定明確的資安政策目標與政策策略，但是在政策制定過程中無單一行政機關能對政策策略的規劃提出完整明確的建議，或是管轄範圍上能管治所有資安政策層面的事務，因此，跨機關與跨單位間的溝通協調極為重要。通常協調工作是由既存組織或新成立的單位來負責，其它相關的政府機關也會被交付此責任，以協助機關間的協調溝通，促進合作與結盟，實施新措施，或避免重複工作的發生。其中，在協調過程中已將多元組織(multi-agency)的協調方式轉換到跨組織(inter-agency)的協調方式，配合需要高效能且合理的領導管理，讓既存的政府組織能夠進行協調溝通和合作。而各國有不同的文化與政府領導型態，在協調上的安排也會有所不同。

2. 加強國營機關與私營機構的合作關係(public-private cooperation)

各國政府決策者理解在網路領域中多數由私營機構包括企業公司、非營利組織與學術團體所建構和操作；為能順利執行資安策略，資安策略的規劃與國營機關和私營機構之間合作關係有密不可分的關係。然而，資安策略的諮詢討論方式與資訊交換方式，會因合作夥伴的不同，而有所差異。

3. 提高國際合作機會

雖然多數國家對公開如何建立國際合作關係之作法的意願不高，但是，仍有例外國家，例如：德國、英國、美國與澳大利亞，已公開發展資安政策的國際合作策略。舉例來說，英國已開始從 2011 年的倫敦網路會議(London Conference on Cyberspace)，藉由國際性交流對談，來提升國際標準的網路使用行為，例如：政府在管理網路空間，有必要遵守國內法和國際法，並必須要尊重個人隱私權利和保護智慧財產。另外，德國政府公開表示德國資安政策的目標之一是鞏固德國的資安政策規劃在歐盟國際資安政策(EU International

Cyberspace Policy)的範疇當中，持續與國際機構(如 United Nations, Council of Europe, OECD, NATO and OSCE)進行協調合作，以及遵守國際法[1]來發展國際與國家資訊安全問題的解決方案。

4. 重視基本價值

所有資安策略皆強調資安政策應重視基本價值，包含隱私、言論自由、以及資訊流通。其中部分資安策略提出應維持網路開放性，而非反對網路的開放來強化資訊安全。不同於一般網路開放是在提高商業機會用以發展網路經濟。

從以上 OECD 新資安策略所依循的四大概念中可發現，四大概念對 OECD 各國的新資安策略規劃的影響略有不同。以下將進一步說明 OECD 新資安策略中特別重視的部分。

1. 資安政策制定中的主權考量(sovereignty considerations)

主權意旨國家與國際的安全，情報，防護與軍事議題。新資安政策為保護整體社會經濟，並需要能整合政府一體化的作法。主權考量會出現在國家政策的三個層面：

(1) 策略層面：針對軍事方面的網路威脅，或其它國家發起的網路間諜活動，主權國家可決定是否對其它涉入國家產生主權認可(state recognition)。

(2) 機構層面：為制定資安政策，負責外交、情報和軍事的機關部門間需要跨部會的協調(Intergovernmental Coordination)，有時，跨組織(inter-agency)會被交付治理資安合作協調的責任。

(3) 執行層面：情報單位在瞭解資安環境狀況中扮演要角。

此外，主權考量也出現在國際政策：

(1) OECD 新資安策略以國際間溝通對話，來訂定網路領域的同意協定(rule of engagement)與網路互信建立措施(cyber confidence

[1] 德國資安政策所遵守的國際法主要為資安國際習慣法(Customary International Law of Cybersecurity)，請參考：http://esil-sedi.eu/?p=12815

building measures)。

(2) OECD 還強調有些國際機構，如北大西洋公約組織(North Atlantic Treaty Organization, NATO)和歐洲安全與合作組織(Organization for Security and Cooperation in Europe, OSCE)，也參與在國際資安政策過程中。

(3) OECD 指出在執行層面的溝通合作，成員國要注意機要情報資訊的交流。

2. 彈性政策

網路經濟是結合了數位科技，應用和產業市場的動態環境，經常以難以預測的方式來創造經濟效益的成長，另一方面，網路威脅也是存在於網路經濟環境裡的問題。OECD 策略中分別有為提高資安政策的彈性和執行速度，保護網路的公開性和資訊流通。另外，有部分策略在提高網路對經濟與社會的利益，以及支持網路經濟的動態環境。還有部分策略主要在支持政策制定循環，加速決策的形成，納入回饋機制，包含學習循環、有效率的執行新措施。並且，還有部分策略建議在網路經濟環經中採自我管理(self-regulation)，或使用法律在某些無法進行自我管理或自我管理無效的案件中。

3. 資安對經濟的重要性

當所有資安策略皆在創造社會經濟的發展與富裕時，即提升了資安對經濟效益的影響。國際中有些國家特別重視具高階資安能力將能提高國家經濟競爭力，認為提升資訊安全對國家經濟帶來重要的影響。有些策略鼓勵彈性政策來影響產業市場對資訊安全的需要。有些策略在提高產業市場對資安有較結構性的認識理解，例如：鼓勵在產品和服務上使用資安標誌，提高產業市場對資安的認知。有些國家制定資安政策的主要目標在建立強大的資安產業部門，包含：培育大量資安人才；並也提及可發展資安相關保險部門。有些策略的主要目標為確認高階科技的自主性和資訊安全的發展。

4. 多元利害關係人的溝通效益

許多 OECD 資安策略皆闡述，在政策循環中與非政府機關的利害關係人間的對話是能制定好資安政策與影響策略執行成效的關鍵。但是，許多國家政府對於該如何進行多元利害關係人的互動溝通僅公開少許資訊。因此，有部分資安策略提出應設立特定組織，讓這些利害關係人為政府提供諮詢服務。目前發現，在產、學研和民眾三類別利害關係人中，產業界利害關係人所提供的資訊對資安策略執行十分有助益；相較於產業界，學研界利害關係人提供的資訊較少，然而，民眾社會(civil society)利害關係人所提供的資訊最少。

(三) OECD 主要國家對新資安策略的推動方案

OECD 主要國家推動新資安策略的主要目標，即是在建立政府機關間高效能的協調機制和重要的領導管理。策略推動方案中已清楚分工各政府機關的權責與義務，並規劃新組織結構。從各國的組織安排中可見文化與政府管理型態的不同；例如：在英國，澳大利亞和日本，政策協調方面工作被歸屬由總理或內閣辦公室來負責。或者是有些國家在協調組織體中設立特定的資安協調單位；例如：法國國家資訊系統安全局(National Cybersecurity Agency of France, ANSSI)。在政策協調的執行層面，有些國家設立特定的公、私營協調組織；例如：荷蘭和德國各成立國家資安委員會(National Cyber Security Councils)，以提供政府在平衡資安、經濟與四大原則間的具體作法。接下來將說明 OECD 主要國家對執行資安策略上的管理和作法，包含：國家資安策略的主要目標，負責規劃的部會/或單位，與負責執行的部會/或單位。

1. 澳大利亞

澳大利亞的 2017 年資安策略 (Australia’s Cyber Security Strategy: 2017 Update)，基本上為提高澳大利亞在全球中的經濟成長，並啟動政府解決國家資訊安全危機的方法，強調政府、產業和研究機構團體間的合作關係。在國家安全顧問(National Security Advisor)的管理

與指導下，總理內閣中的網路政策協調者(Cyber Policy Coordinator)和國家資訊長(National Chief Information Officer)主導資安政策的規劃和發展。在執行上，澳大利亞的電腦安全事件應變小組(Computer Emergency Response Team, CERT Australia)，已發表了 159 建議報告，並已處理 10,351 件危害商業發展的資安事件，其中 363 件對國家資訊系統造成較危急的影響；在未來，新資安策略將會擴展電腦安全事件應變小組的能力，能夠對國家重要建設公司在發展工業控制系統時，提供專業的資安建議。另外，2016 年澳洲國防白皮書(Australian Defence White Paper)中所宣布建立的資安監控中心(Cyber Security Operation Center, CSOC)，負責提供政府在資安環境裡所需要的相關資源與高階能力以協助策略執行。

2. 加拿大

加拿大公共安全部(Public Safety Canada)設計規劃資安策略，於 2018 年公布國家資安策略(National Cyber Security Strategy)，主要在保護國家在數位經濟裡的安全系統，提升創新且最適化的網路生態系統(cyber ecosystem)，建立最強健的聯邦階層以領導管理資安；從 Budget 2018 中投入高於 5 億加幣在約五年的資安策略執行過程中。加拿大公共安全部負責國家資安策略中的溝通協調，和執行方法之設計，並，負責推動公共對資訊安全的認知。加拿大公共安全部中設有電腦資安事件應變中心(Canadian Cyber Incident Response Centre)，管控網路威脅，提供防禦措施，和處理資安危機事件，特別是對重要網路基礎建設。還有其他政府部門參與資安策略的推動，包含加拿大工業部(Industry Canada)提出的國家數位經濟策略，以創造安全可信賴的網路市場；國庫委員會秘書處(Treasury Board Secretariat)負責政府方面的資安，情報與訊息加密；司法部(Department of Justice)負責資安相關法規；以及，加拿大外交與國際商貿處(Foreign Affairs and International Trade Canada)涉入國際資安議

題。還有，加拿大國防部(Department of National Defense)與加拿大陸軍(Canadian Forces)處理屬於國防領域的網際網絡，與各部門的訊息傳達，和軍事聯盟間的合作關係。

3. 芬蘭

芬蘭於 2013 公布資安策略(Finland's Cyber security strategy)，其主要目在保護整體芬蘭社會，能解決處理所有情境下的資安危害；人民、政府當局和產業能有效利用安全的數位環境，並藉由資安措施去提升國家與國際資安能力；到 2016 年，芬蘭能成為在國際上有充分能力解決資安威脅問題的先驅者。在 2011 年 3 月 8 日芬蘭總統決定要解決國家所面臨的資安問題，並設計國家資安策略後，由芬蘭國家研發基金(Finnish Innovation Fund Sitra)主席 Mr. Mikko Kosonen，所領導的跨單位工作小組(cross-sectional working group)規劃芬蘭的國家資安策略。由隸屬於國防部的安全委員會(Security Committee)，負責管理與執行資安策略的工作。

4. 法國

法國國家資安策略從 2015 年 10 月總理 Mr. Manuel Valls 宣布開始，目的為保護網路安全，保衛國家資訊安全，為法國商業的發展，提高數位安全和強化資安防禦。法國資安策略的執行工作主要由三個單位負責。國家資訊系統安全局(French Network and Information Security Agency, ANSSI)，與國防與國家安全秘書長(SGDSN)共同負責國家資安策略推動，國家資訊系統安全局是政府在推動國家資安策略的跨部門協調者，包含提供跨部門安全溝通的方式，政府系統偵測，處理 IT 危機事件，相關專業訓練，以及提供資訊系統認證以保護國家機密；以及，國防部(Ministry of the Armed Forces)負責在鞏固網絡安全，並將處理數位攻擊事件納入國家軍事行動當中。另外，內政部(Ministry of the Interior)負責主導網路犯罪的調查工作，以及管理處理網路犯罪事件的單位。

5. 德國

德國聯邦政府在 2016 年 11 月核准通過新資安策略。由於多數的數位攻擊事件來自中國和俄羅斯，因此德國新資安策略要求國家與私人機構共同合作以對抗資安威脅事件；德國聯邦政府將提供網路安全上的支持以鞏固德國的商業發展；並特別加強保護重要設施包含：能源和水資源系統、醫療系統、數位系統和運輸系統。由聯邦內政部(Bundesministerium des Innern, für Bau und Heimat)主導，加上與其他部門間的合作協調，特別是與外交部，國防部，經濟部，和司法部。德國資安策略中宣布成立國家網路中心(Nationale Cyber-Abwehrzentrum)，由聯邦資訊安全辦公室(BSI)負責管理國家網路中心，該中心匯集了聯邦資訊安全辦公室的網絡防禦資源，讓政府各機關間的協調合作和資訊安全事件的處理能達到最佳化；其它部門如聯邦憲法保護辦公室(BfV)等，可依任務內容與權限，在該中心內進行溝通協調。該中心會將資安危機事件的處理情況與結果直接對聯邦內政部報告。

6. 荷蘭

荷蘭國家網路安全中心(National Cyber Security Centrum, NCSC)在 2018 年公布最新資安策略(National Cyber Security Agenda—A cyber secure Netherlands)，說明荷蘭政府致力於讓國家能夠基於資訊安全的方式以充分發展經濟與社會繁榮的機會，和保護國家資訊安全，並且與國際合作機構共同來保衛數位環境。由荷蘭公共安全與司法部(Ministry of Justice and Security, JenV)負責政府機關間的協調工作，並提升以網絡中心為主(network-centred)的合作方式。國家網路安全中心負責資安策略的執行工作，與通訊技術安全小組(GOVCERT.NL)進行合作，提供專業技術和建議以提升資安事件的危機管理能力；該中心負責處理網路威脅和危機分析。資通訊回應委員會(ICT Response Board)是屬於政府與民營機關的伙伴合作關

係，為決策者提供防範資安危機的建議。另外，國家網路安全委員會(National Cyber Security Council)的成員包括政府，企業公司與學研機構，共同提升國家資安發展和協助政黨在資安危機事件中進行決策。

7. 英國

英國在 2015 年所公布的 2016-2021 年資安策略，主要目的在啟動英國政府的計畫以確保國家與整體社會在網路環境裡的資訊安全，包含：處理網路犯罪，讓英國成為全球中最安全、可發展商業活動的網路區域；英國政府將改善與加強法律和執法單位對數位犯罪的制裁措施，以及，教育英國人民懂得在網路犯罪中自我保護安全等目標。於內閣辦公室(Cabinet Office)下設有網路安全辦公室(Office of Cyber Security, OCS)，負責提供政府跨部門的資安策略，並協調部門間的網路安全工作；除了提供策略方向外，該辦公室的任務還包括協助教育訓練，和私人機構或國際組織的合作關係，並與政府資訊科技總監辦公室(Office of the Government Chief Information Office, OGCIO)共同推動政府對內與外的資通訊科技發展。英國資安策略還成立網路安全營運中心(Cyber Security Operations Centre, CSOC)，該中心屬於多元機構的組織體，由英國政府通訊總部(Government Communications Headquarters)來管理，主要在處理危及商業與社會大眾的資安威脅事件。

8. 美國

美國在 2003 年公布最初的資安策略，到 2018 年，白宮發布最新的資安策略(National Cyber Strategy of the United States of America)，其中清楚闡明政府對資安策略執行的優先順序，首先，強化聯邦網絡、資訊系統和數據保護，制裁網路犯罪以保護美國整體國民；第二，推動數位經濟，與人才發展，以提高美國經濟繁榮；第三，推廣負責任的網路行為標準，並阻止不合理與非法的網路行為；第

四，建構公開且可信賴的網路環境，並提升美國在國際數位環境中的影響力。美國總統 Donald J. Trump 承諾保護國家的資訊安全，並明確表示 Trump administration 會做一切必要措施來保護美國的資訊安全(National Security Council, 2018)。由白宮的國家安全人員(National Security Staff)組成資安辦公室(Cybersecurity Office)，內有資安協調員(Cybersecurity coordinator)，負責跨部門間的溝通協調，與聯邦資訊長(Federal Chief information Officer)，以及國家經濟委員會(National Economic Council)共同合作。美國管理與預算局(Office of Management and Budget, OMB)為國家資安策略執行以提供適當的資源和經費計畫。

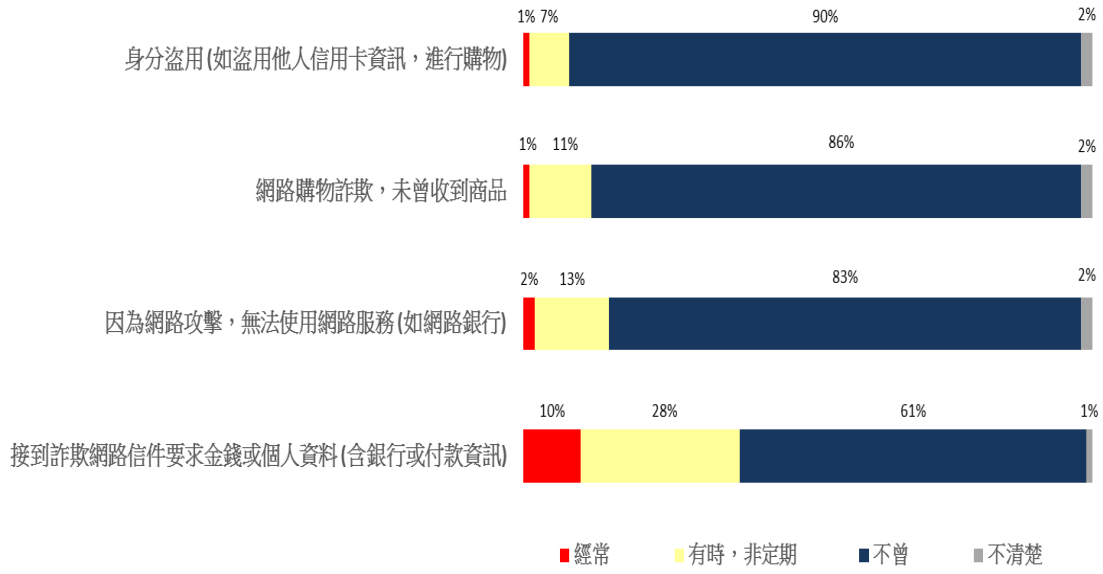
9. 日本

日本內閣於 2018 年 7 月決定通過 2018-2021 國家網路安全策略，該策略目的在為日本永續發展而推廣網路安全生態系統，建立網路安全的社會，並對國際合作社群在網路和平與穩定性方面有所貢獻。由隸屬於中央政府的日本資安事件整備與策略中心(National Center for Incident Readiness and Strategy for Cybersecurity, NISC)領導網絡安全策略的執行，該中心指導所有中央政府相關機關，以提升資安能力，進行跨機關的溝通協調工作，並且，負責提升產業、學研和政府間的合作關係。

(四) 歐盟的新資安策略

資通訊科技成已為各國經濟成長所依賴的重要資源，甚至許多企業公司的商業模式是建構在高效能的網路能力和資訊系統上。歐盟執行委員會在規劃新資安策略之前，對 27 個歐盟成員國人民進行(Special Eurobarometer 390: Cyber security)之研究調查，此研究調查結果提供歐盟執行委員會，進以瞭解歐盟國家人民對網路安全相關議題的認知和經驗之數據證明，該調查結果顯示，歐盟國家人民所遭遇各類網路犯罪和曾經成為各類網路犯罪受害者的比例；其中，超過 1/3 比例的歐盟人民反應曾接

到詐欺信件在要求錢財或個人資料包含銀行或付款資訊；有 15%的歐盟人民反應曾因為網路遭受攻擊，而無法使用網路；有 12%的歐盟人民曾經歷網路購物詐騙；以及，8%的歐盟人民曾遭遇網路身分盜用，詳細數據如圖二所示。



圖二：歐盟 27 成員國人民遭遇網路犯罪的比例

資料來源：European Commission，本研究整理

該研究結果也顯示歐盟人民對整體網路環境的信心程度。74%歐盟人民認同，在近幾年受到網路犯罪的威脅，成為受害者的比例不斷提高。89%歐盟人民對避免在網路上公開個人資料表示認同。另外，72%歐盟人民認為網站無法安全保存他們的個人資料。66%歐盟人民擔心政府機關無法保護人民的個人資料安全。

歐盟執行委員會運用統計證據來支持政策決策，不僅從中發現到網路犯罪的危害已影響歐盟地區的經濟發展，也讓資安成為歐盟各國政府極為重視的問題。在 2013 年歐盟執行委員所發布的資安策略中闡明，為提供全體歐盟人民具開放性和安全性的網路環境，歐盟資安策略是指導歐盟國家與國際發展資安政策的原則，詳細說明如下：

1. 資訊安全應保護人民基本權利，言論自由，與個人資料隱私權

資訊安全要能夠有效實行，必須依據歐洲聯盟基本權利憲章(Charter of Fundamental Rights of the European Union)：針對人民基本權利與自由之規定。同時強調，在沒有安全性網路的條件下，人民權利是無法得到保護。

2. 對全民開放網路連線

有限度或無法使用網路連線會不利於人民的生活條件。每一民眾都應能使用網路連線和有流通的網路資訊，因此必須保障網路的正當性和安全性，讓每一人民都能有安全性的網路連線。

3. 民主化和有效的多元利害關係人治理

數位化時代並不是由單一組織體來管控。有來自商業領域或非政府機關的多元利害關係人，共同參與網路資源的管理，規則與標準制定，以及網路在未來的發展。歐盟重申，全部利害關係人在網路管理模式中的重要性，並支持以多元利害人的治理方式。

4. 共同承擔資訊安全的責任

人類生活各方面對資通訊科技的高度需求造成了資安對人類生活的必要性。因此，不論是政府當局、私人機構或人民個體皆須有共同承擔資安責任的認知，以行動付出來保護和強化資訊安全。

基於以上四大原則，歐盟執行委員會提出五項新資訊安全重點策略；策略執行的目標為讓歐盟地區成為最安全的網路環境。

(一) 達成網路防禦

(二) 徹底降低網路犯罪

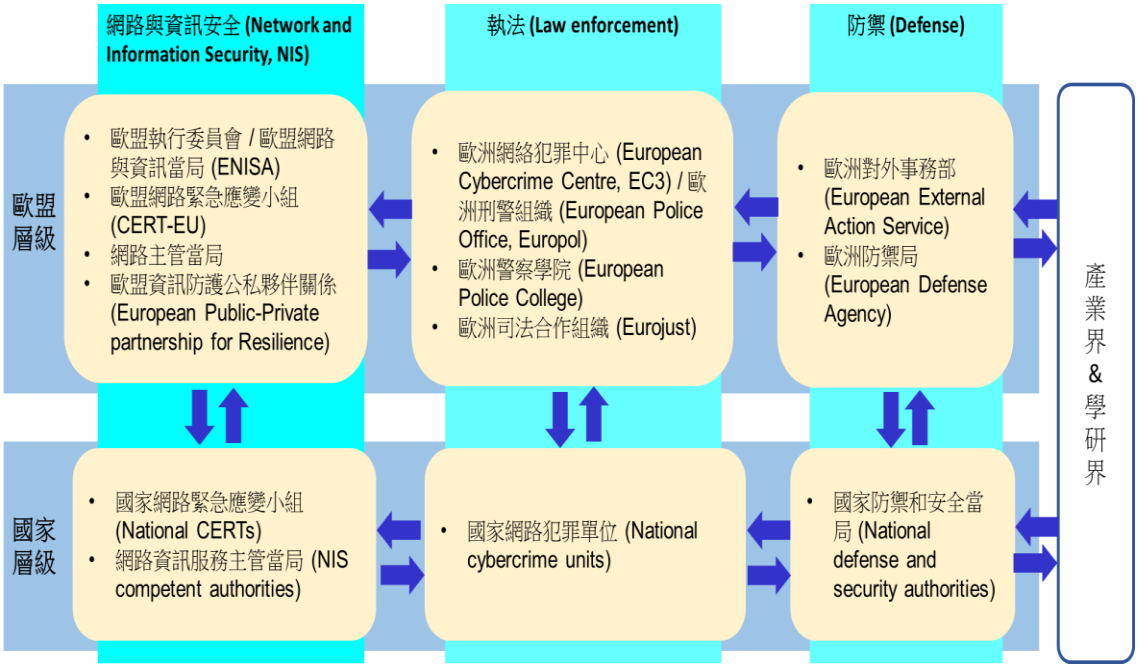
(三) 發展資訊安全政策、歐盟共同安全與國防政策(Common Security and Defence Policy)與資安能力

(四) 發展資安所需的工業化和科技性資源

(五) 為歐盟國家制定一致性的國際資安政策並促進歐盟核心價值

歐盟在資安策略中說明，策略執行的責任須由歐盟和各國政府共同分

工管理。因為策略中涉及了不同的法規架構，對歐盟而言，最大的挑戰在能夠清楚溝通協調各個不同機構單位的角色與責任。為處理此複雜的角色和責任分工問題，歐盟在資安策略中表示全然交給歐盟管理當局並非解決方式，各國家政府應是站在資安管理與網路犯罪防範的最佳位置，並與企業公司建立聯繫網絡，透過國家資安政策的推動與完備的法規架構，來處理網路威脅事件。同時，必須考量資安事件的風險，由於事件發生是在網路世界，對歐盟各國，最佳的資安處理方式需要有歐盟層級的介入。在歐盟資安策略中，歐盟執行委員會提出結合國家層級與歐盟層級的資安策略協調合作機制，如圖三所示。圖中，歐盟的資安策略協調合作機制呈現以全面性方式來處理網路犯罪，各項處理措施應要結合三大重要支柱包括：網路與資訊安全(Network and Information Security, NIS)，執法(Law enforcement)，和防禦(Defense)；各個支柱中有不同的法務單位參與運作與任務執行。接下來將進一步說明該機制中的協調合作方式。



圖三：歐盟資安策略協調合作機制

資料來源：European Commission，本研究整理

在國家層級方面，歐盟各國應建立能處理網路事件的能力條件。藉由國家網路與資訊安全(NIS)合作計畫的擬定，各國政府應規劃好各機構單位在資安策略，以及處理網路犯罪案件中的角色和責任；給予相關機構能跨不同網路犯罪領域的執行責任，提高私人機構參與的重要性，政府機關和跨單位應能有最佳合作與協調的方式。政府機關與私人機構間的資訊與技術能進行交流，為確保彼此對不同網路威脅事件，有最完整的理解，和最迅速的處理措施。

在歐盟層級方面，其中包含數各處理網路犯罪的相關機構單位。特別是各三大支柱中的歐盟網路與資訊當局(European Union Agency for Network and Information Security , ENISA)，歐洲刑警組織(European Police Office, Europol)和歐洲防禦局(European Defense Agency, EDA)，在歐盟各國中皆成立管理委員會(Management Boards)，做為歐盟層級的協調合作平台。歐盟網路與資訊當局，歐洲刑警組織，與歐洲防禦局三個組織間的協調合作工作特別針對趨勢分析，風險評估，訓練和實務經驗的分享；此三個組織，歐盟執行委員會，歐盟網路緊急應變小組(CERT-EU)與歐盟各國政府應共同支持資安技術與政策方面的專家團體發展。

另外，非正式的協調合作可經由結構化聯繫方式來執行；歐盟軍事參謀部(EU military staff)和歐洲防禦局的共同網路防護專案可被使用在防禦支柱中的協調合作。歐洲刑警組織(European Police Office, Europol)和歐洲網路犯罪中心(European Cybercrime Centre, EC3)的計畫委員會(Programme Board)整合歐洲司法合作組織 (Eurojust)，歐洲警察學院(European Police College, CEPOL)，歐盟各國，歐盟網路與資訊當局，和歐盟執行委員會，以提供機會來分享他們的專業知識與實務經驗，和確認歐洲網路犯罪中心的行動措施有顧及利害關係人的建議與要求。歐盟網路與資訊當局舉辦的活動安排，應能提高與歐洲刑警組織間的連結，和強化與產業界利害關係人的聯繫關係。

在歐盟的資安策略協調合作機制中最重要的部分是，歐盟執行委員會

在為網路與資訊安全(NIS)的立法提案，透過與各國網路資訊服務主管當局 (NIS competent authorities)的聯繫網絡建立合作架構，讓網路與資訊安全主管當局與執法當局可進行相關資訊的交流。

三、 OECD 組織、歐盟面臨的政策挑戰

(一) OECD 組織面臨的政策挑戰

OECD 組織在 1992 年的資訊系統保護標準綱要(Guideline for security of information systems)中宣布資安策略目的，即是在領導經濟與社會繁榮，以及對抗網路威脅；經過二十多年的政策發展，OECD 組織的資安政策似乎已發展到較成熟的水平。目前，OECD 組織的新資安策略不僅要達到相同目標，同時，還必須保持網路資訊的公開性，以提供科技發明和新資源開發的平台。因此，延伸而出的政策挑戰在於，各國政府處在不同層次的複雜情境，使得政策上的挑戰倍增，例如：政府需處理跨組織在決策過程中的協調工作。

另外，一複雜的政策挑戰是國家決策者需要一整體性方式，能一併考慮主權，經濟與社會因素，大範圍的政府體系，和私人機構間溝通協調，以加速團隊工作與行動。

(二) 歐盟面臨的政策挑戰

在歐盟，各國負責自己國家的資安能力發展，但是，各國間的資安成熟度(cyber maturity)差距相當大，導致歐盟在建立資安能力上面對極高的挑戰。接續將針對歐盟主要面臨的政策挑戰做進一步的分析和討論。

1. 歐盟的權利責任，與歐盟各國主權的平衡

造成歐盟權利與各國主權易失衡的因素在於，歐盟共同安全與國防政策(Common Security and Defense Policy, CSDP)讓歐盟能夠對國際安全和國防方面採取必要措施，而該政策隸屬於歐盟共同外交與安全政策(Common Foreign and Security Policy, CFSP)中的一部分，但是因為歐盟共同外交與安全政策中的權限限制，讓網路衝突事件和網路防禦不常與歐盟層級有直接接觸。並且有越來越多的歐盟成員國

訂立國家網路安全策略(National Cyber Security Strategy, NCSS)，管理自己國家的網路風險。另外，歐盟成員國傾向與北大西洋公約組織(NATO)合作以提升網路防禦能力。

歐盟為加強資安政策發展與策略執行，在 2013 年的網路安全策略(EU Cyber Security Strategy)以及 2015 年的歐盟會議就網路外交(Cyber Diplomacy)決議中已強調，與國際重要夥伴密切合作的必要性。在歐盟會議決議中，在資訊安全和網路治理兩個方面，國際合作有很大幫助，並與中國、印度、日本、南韓和美國展開對話溝通。歐盟理事會(Council of the European Union)倡導，歐盟國家在資安策略協調合作機制下應繼續對話溝通，並避免重複相同工作和活動。上述的溝通過程中，是由歐盟對外事務部(European External Action Service, EEAS)將資安相關議題介紹給進行談話的雙方國家或不同的組織機構。

2. 歐盟機構中結構複雜的管轄權

因為過去歐盟三支柱對歐盟管轄權仍產生極大影響：第一支柱為歐洲各共同體(European Communities)，涉及經濟、社會、環境等政策；第二支柱為共同外交與安全政策(Common Foreign and Security Policy)，涉及外交、軍事等政策；第三支柱為刑事領域警察與司法合作(Police and Judicial Co-operation in Criminal Matters)，涉及共同合作打擊刑事犯罪。其中，因為有不同組織的參與合作而提高了管轄權的困難度。

然而，為讓合作過程能順暢進行，歐盟組織包含洲防禦局(EDA)、歐盟網路與資訊當局(ENISA)、歐洲刑警組織(Europol)和歐洲網路犯罪中心(EC3)和歐盟網路緊急應變小組(CERT-EU)已協議好對資安和防禦兩方面的合作方式。歐盟理事會也持續邀請歐盟國家、歐盟執行委員會與最高代表報告資安策略的執行狀況，以促進定期性合作。

3. 歐盟資安政策中的利害關係人類型與數量

在歐盟資安政策中有非常多元化的利害關係人參與其中。在歐盟國家層級，利害關係人可包含法務機關，情報機關，以及學術研究機構，因此，各個歐盟國家對各利害關係人在資安政策中的角色與任務需有不同的規劃安排，但也加重了以上第 2 點所敘述的複雜管轄權的困難度。

在國際層級，如歐盟會議就網路外交決議中強調與國際夥伴間的對話溝通是發展資安政策和資安能力的關鍵活動，因此，歐盟不斷與活耀在資安領域裡的機關單位有密切性合作，特別是聯合國(United Nations)、歐洲委員會(Council of Europe)、歐洲安全與合作組織(Organization for Security and Co-operation in Europe, OSCE)、經濟合作暨發展組織(OECD)、北大西洋公約組織(NATO)、非洲聯盟(African Union, AU)、美洲國家組織(Organization of American States, OAS)、東南亞國家協會(Association of Southeast Asian Nations, ASEAN)。

另外，資安相關產業也是關鍵利害關係人之一，因為產業界的科技發明和專業技能上的支持能減緩網路衝突的發生機率和可能造成的負面影響。為處理網路威脅事件，軍事，產業界和學研界間的合作對發展網路防禦科技十分重要，例如：北大西洋公約組織(NATO)和產業界間頻繁的合作活動，例如：資訊交流活動、教育訓練。最後，由產業公司所成立的歐盟電腦安全事件回應小組(CSIRT)，對資安策略的執行和資訊與專業知識方面的交流能有所貢獻。

目前所有參與在歐盟資安政策之利害關係人在其中皆扮演著重要角色，但在歐盟國家層級和國際層級上的角色任務可能有交疊，而造成工作重複和非一致性的作法。

4. 有限的數據可支持政策發展

政策執行能成功需有賴於高質量的數據證據的支持，但是，歐盟指

出至今在資安領域的數據資料質量不均，主要原因是在資安領域中仍有許多概念定義還尚未受到一致性的同意，另一原因是部分資訊內含軍事機密，而這些數據並非皆以科學方法收集而來，例如：無實驗設計或統計方法檢測。未來，歐盟機構和成員國將會加強有效數據的收集以支持歐盟的資安政策決策與策略執行。

最後，雖然歐盟在資安策略執行過程中也面臨了科技與法規相關問題，例如：現有法規架構應用在網路衝突中的不確定性；使用無人駕駛飛機在解決網路衝突事件時的法規不確定性，但由於本研究報告的目的，是在分析探討歐盟正面臨的政策挑戰，因此其他方面不在本研究報告中進行討論。

參考文獻

1. Chapman, A., McLellan, B., & Tezuka, T. (2016). Strengthening the energy policy making process and sustainability outcomes in the OECD through policy design. Administrative Sciences, 6(3), 9.
2. Council of the European Union (2015). The EU policy cycle to tackle organised and serious international crime. Retrieved on March 3, 2015, from https://publications.europa.eu/en/publication-detail/-/publication/9984824a-7509-448e-8ed8-ea7a54ff5ad6
3. European Commission (2012). Special Eurobarometer 390: Cyber Security Report. Retrieved on March 18, 2018 from https://data.europa.eu/euodp/data/dataset/S1058_77_2_EBS390
4. European Commission (2013). Joint communication to the European parliament, the council, the European economic and social committee and the committee of the regions. Cybersecurity strategy of the European Union: An open, safe, and secure cyberspace. Retrieved on February 7, 2013 from https://eur-lex.europa.eu/procedure/EN/202369
5. European Parliament (2017). Cybersecurity in the EU common security and defense policy: Challenges and risks for the EU. Retrieved on June 15, 2017 from https://www.enisa.europa.eu/news/enisa-news/cybersecurity-in-the-eu-common-security-and-defence-policy-csdp-challenges-and-risks-for-the-eurisks-for-the-eu
6. European Policy Centre (2017). European cybersecurity policy—Trends and prospects. Retrieved on June 8, 2017 from http://www.epc.eu/pub_details.php?cat_id=3&pub_id=7739
7. François Delerue (2018). ESIL Reflection: The Codification of the International Law Applicable to Cyber Operations: A Matter for the ILC? Retrieved on July 3, 2018 from http://esil-sedi.eu/?p=12815
8. OECD (2012). Cybersecurity policy making at a turning point: Analysing a new generation of national cybersecurity strategies for the internet economy. Retrieved on November 16, 2012 from https://www.oecd-ilibrary.org/science-and-technology/cybersecurity-policy-making-at-a-turning-point_5k8zq92vdgtl-en