建置兼具國家安全與個人隱私保護的資通訊情蒐與分析系統

胡毓忠教授
政治大學資訊科學系

吳啟文副主任
行政院資通安全辦公室

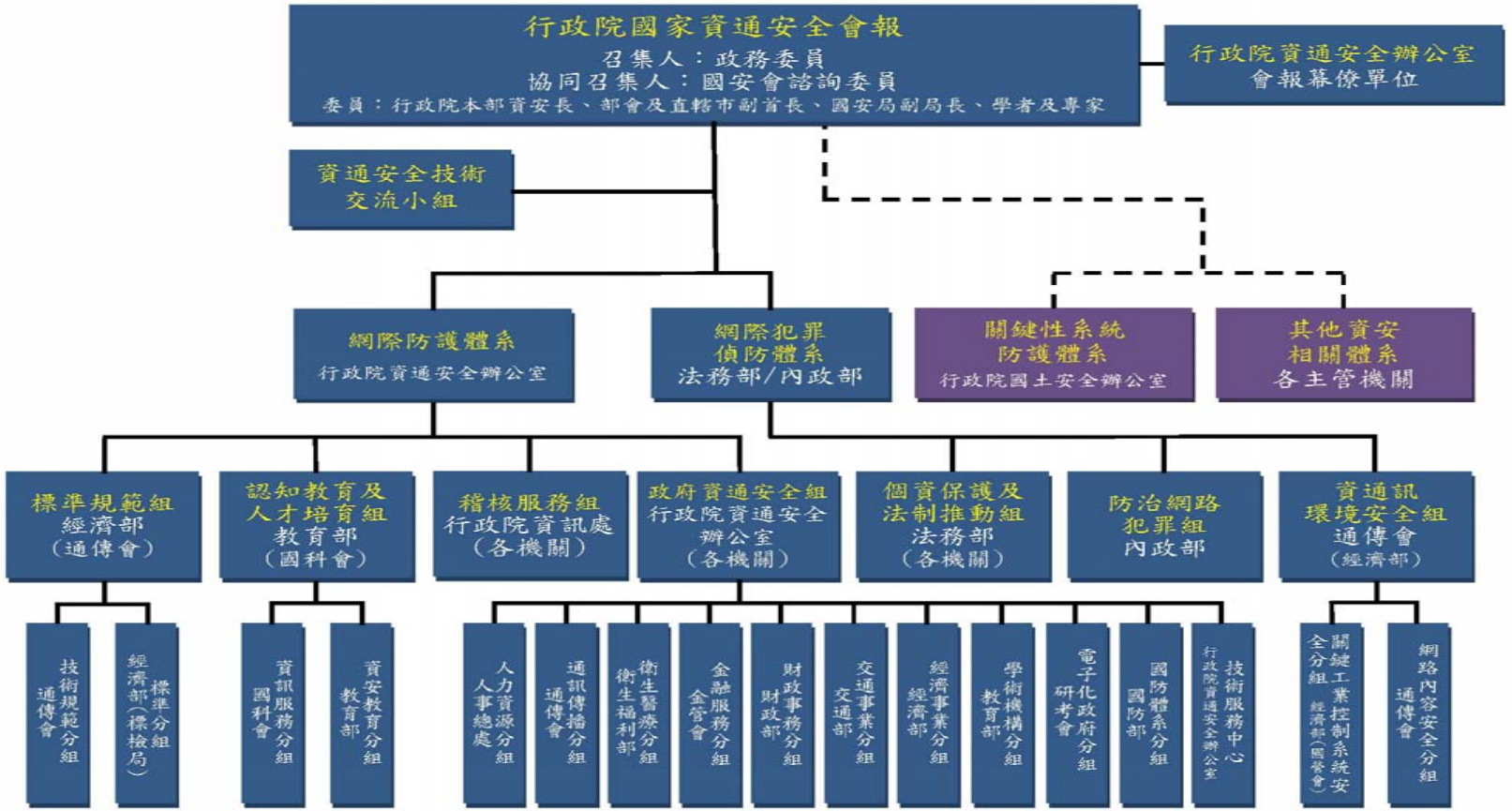
主要目錄

1. 導論
2. 研究動機
3. 研究目的與貢獻
4. 現有資通情蒐與分析系統
5. 新世代資通情蒐與分析系統
6. 如何兼具國家安全與隱私保護
7. 相關研究
8. 結論與未來研究
9. 參考文獻

導論

- 國家關鍵資訊基礎設施保護（Critical Information Infrastructure Protection , CIIP）主要目的為何？
- CII和其它國家關鍵基礎設施Critical Infrastructure , CI)的相關性為何？
- 國內主導國家關鍵資訊基礎設施保護(CIIP)工作的是行政院國家資通安全會報，資通安全辦公室是協助的幕僚單位。

行政院國家資通安全會報組織架構圖

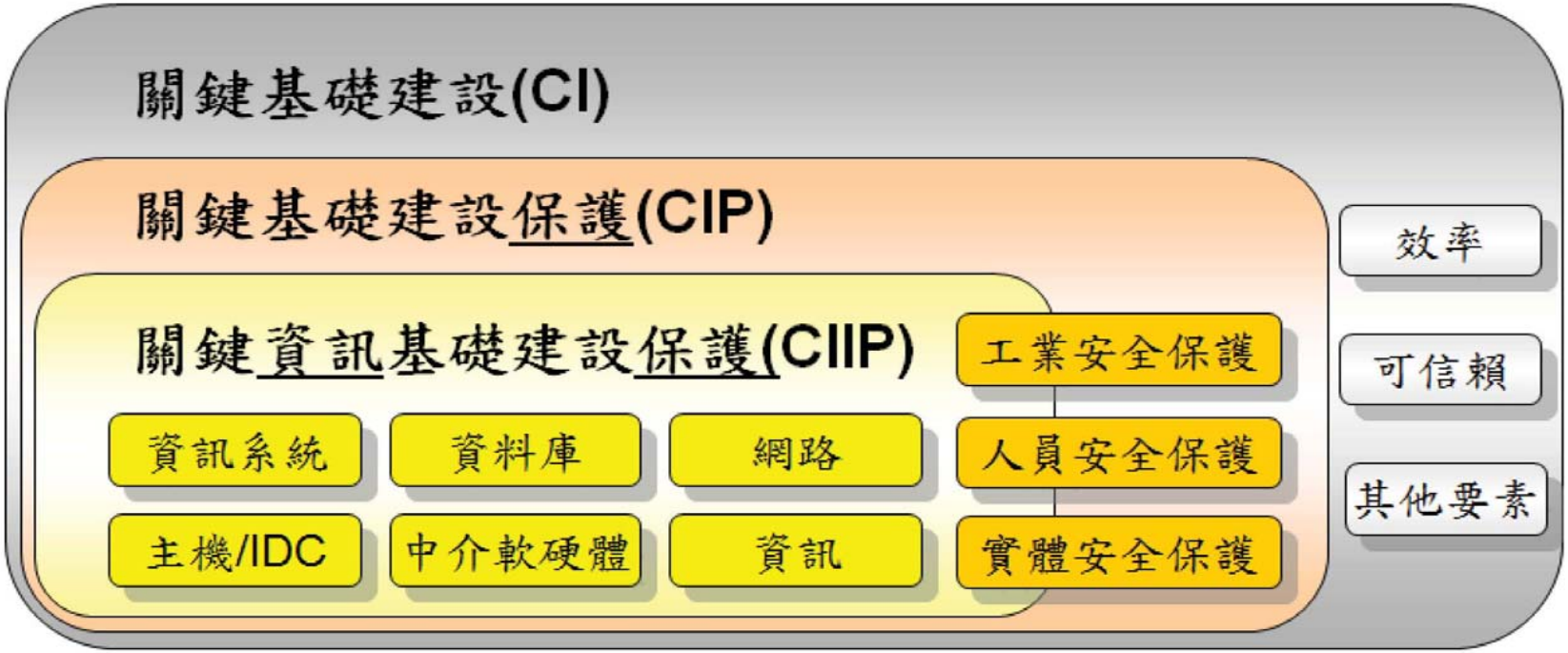


圖片來源：國家安全會報應變作業綱要（102年9月9日），行政院資通安全辦公室

國家關鍵資訊基礎設施防護(CIIP)主要目的

建置國家關鍵資訊基礎設施防護（Critical Information Infrastructure Protection, CIIP）架構主要目的是用來維繫並且支撐著其它重要八大關鍵基礎設施的保護(Critical Infrastructure Protection, CIP)，如水資源、能源、交通、中央政府、高科技園區、醫療、金融、資通訊與其它類別的保護。

關鍵基礎建設保護（CIP）之關係示意圖



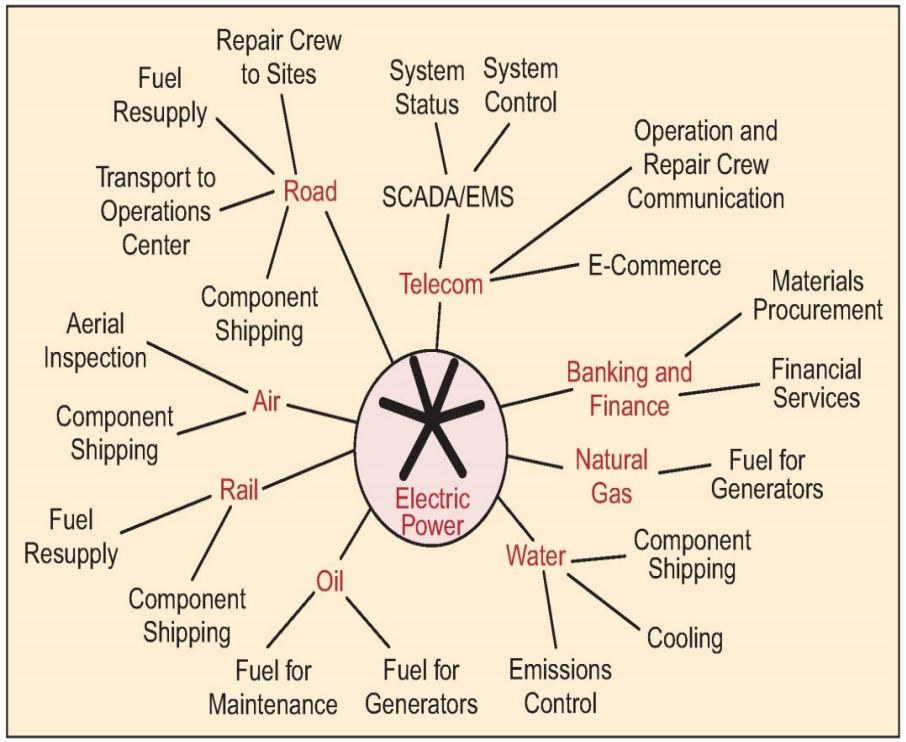
資料來源：行政院科技顧問組（科顧組），2011，《關鍵資訊基礎建設保護政策指引》，行政院國家資通安全會報

CIIP提供CI所需之各種防護服務

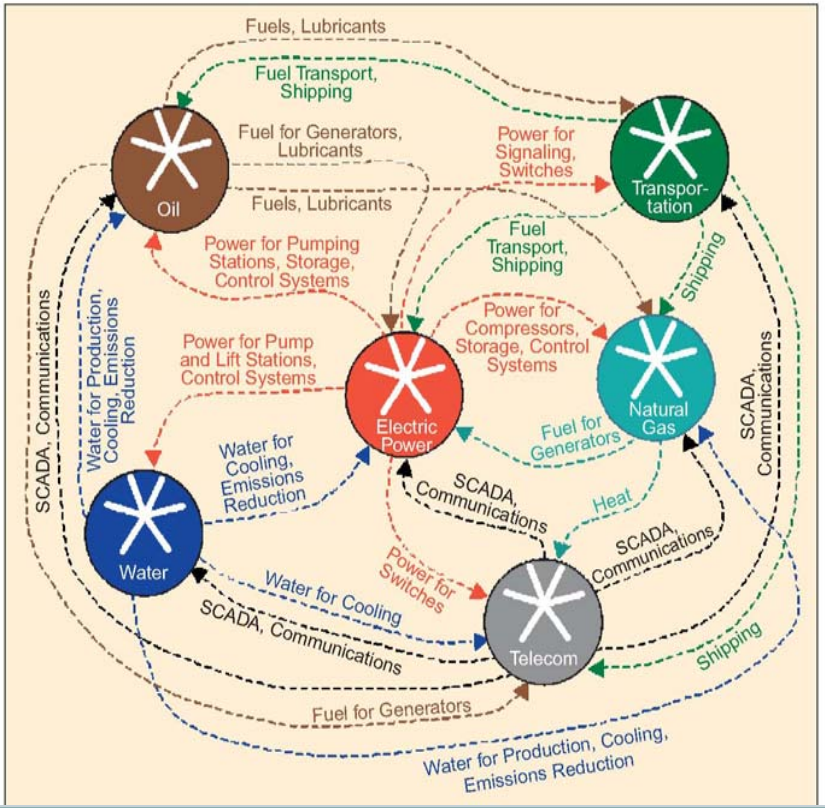
資料來源：行政院科技顧問組（科顧組），2011，《關鍵資訊基礎建設保護政策指引》，行政院國家資通安全會報

各種CI間相互關係示意圖

電力基礎架構與其它CI的關係



CI間相互關係的範例



Source: Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies. IEEE Control System Magazine .

研究動機

- 新資訊科技的發展、如雲端運算（Cloud Computing)與巨量資料(Big Data) ，將對資通情蒐與分析系統產生巨大的影響與改變。
- 新型態網路與電腦系統攻擊的演進，如零時差攻擊（Zero-Day Attack)與進階持續式威脅（Advanced Persistent Attack）將產生資訊系統防守與偵測的挑戰。
- 檢視現有資通情蒐與分析系統，思考如何運用上述新資訊科技來提升系統對於新型態攻擊的防守能力，更進一步確保CII的強韌度。
- 當落實國家安全目的所進行具個人識別碼資料蒐集與分析該如何考量隱私保護規範，以確保國家安全與國民隱私保護間的平衡。

研究目的與貢獻

1. 檢視現有國家關鍵資訊基礎設施防護的現況並分析其資訊安全保護網的架構與執行機制是否足以應付新型態的資訊攻擊。
2. 探討該如何考量新資訊科技，如雲端運算平台與巨量資料分析技術，落實國家未來資訊基礎設施防護。
3. 探討現有資通訊情蒐與分析系統在落實國家安全與犯罪防制與偵察時應同時考量個人資料使用與隱私保護兩項準則。

現有資通情蒐與分析系統

現有資通情蒐與分析系統

計有三種機制進行資通情蒐、分享、分析與回應：

1. 資通安全防護管理中心(Security Operation Center, SOC)
2. 電腦危機處理應變中心（Computer Emergency Response Team, CERT）
3. 資訊分享與分析中心(Information Sharing and Analysis Center, ISAC)

現有資通情蒐與分析系統

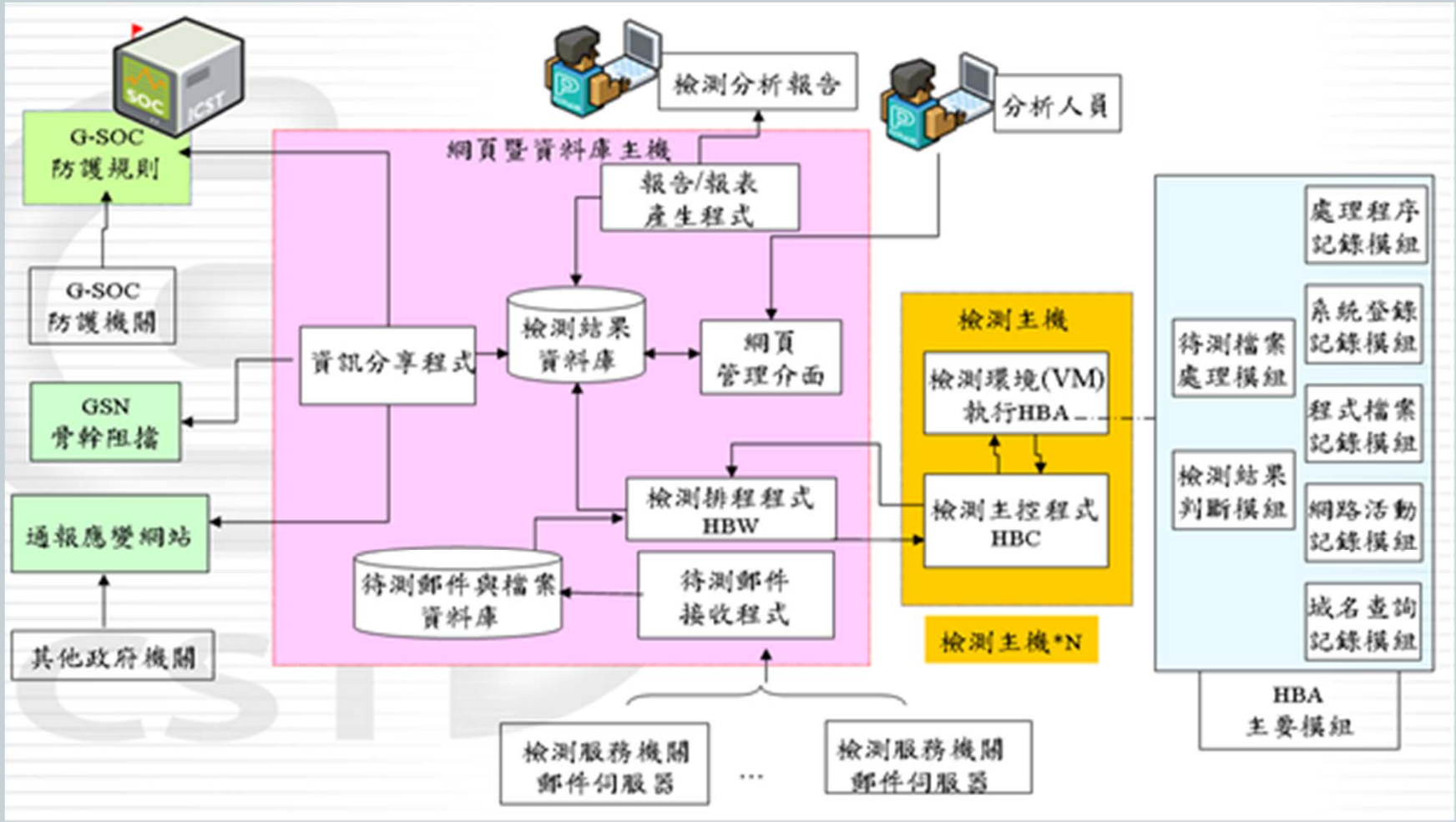
國內情資分享與通報應變機制一覽表			
類別	單位全名	簡稱	權責/主管機關
行政機構	行政院國家資通安全會報	NISCT	行政院
	國家資通安全會報技術服務中心	ICST	
	政府資安資訊分享與分析中心	G-ISAC	
	政府網路危機處理中心	GSN-CERT/CC	
	國家電腦事件處理中心	TWNCERT	
	國家資通安全應變中心	NCERT	
	國家通訊傳播委員會電腦危機處理中心	NCC-CERT	通傳會
	國營會資安資訊分享與分析中心	SEC-ISAC	經濟部
	經濟部電子商務資安通報服務中心	EC-CERT	
教育機構	台灣學術網路危機處理中心	TACERT	教育部
	教育學術資訊分享與分析中心	A-ISAC	
	教育部學術資訊安全監控中心	A-SOC	
法人機構	財團法人台灣網路資訊中心	TWNIC	交通部
	台灣電腦網路危機處理暨協調中心	TWCERT/CC	
	網路釣魚通報單一窗口	APNOW	
民間業者	中華電信(股)有限公司	Hinet SOC	通傳會
	台灣碩網網路娛樂(股)有限公司	So-NET Taiwan	通傳會
	遠傳電信(股)有限公司	U-SOC	通傳會

資料來源：行政院科技顧問組（科顧組），2011，《關鍵資訊基礎建設保護政策指引》，行政院國家資通安全會報

現有資安情蒐與分析執行概況

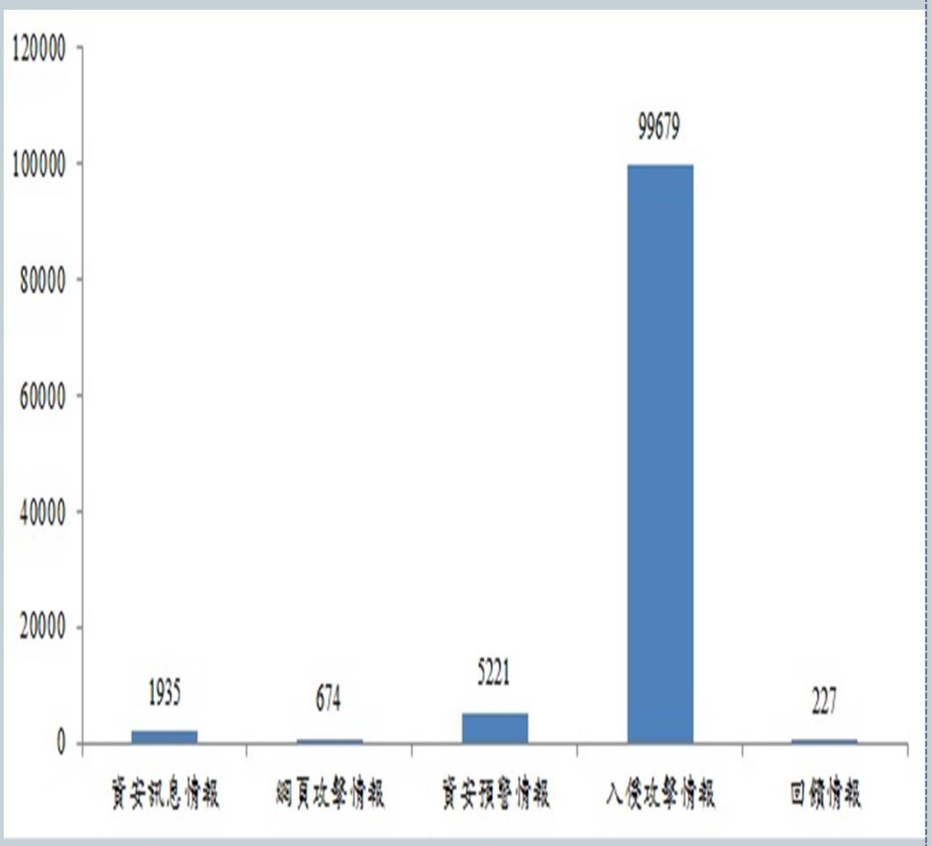
- 政府資訊分享與分析中心（G-ISAC）蒐集惡意網頁與釣魚網頁、社交工程郵件攻擊、網路攻擊與惡意程式、殭屍網路攻擊及垃圾郵件等各項資安事件來強化政府CII防護能力。
- 中央政府機關對於資通訊情蒐與分析是委外給資訊安全專業公司來進行，透過SOC 資安廠商可以提供網路監控服務的第一線監控。
- 目前正規劃第二線監控機制並且委由由行政院國家資通安全會報技術服務中心（技服中心）執行，請SOC資安廠商回傳資安事件相關資料，並進行資料關聯分析，以掌握資安威脅趨勢，並達成早期預警及資安聯防等目標。
- G-ISAC於101年加入了Amazon EC2與巨量資料分析模組MapReduce。

政府部門電子文件自動檢測機制：HoneyBEAR

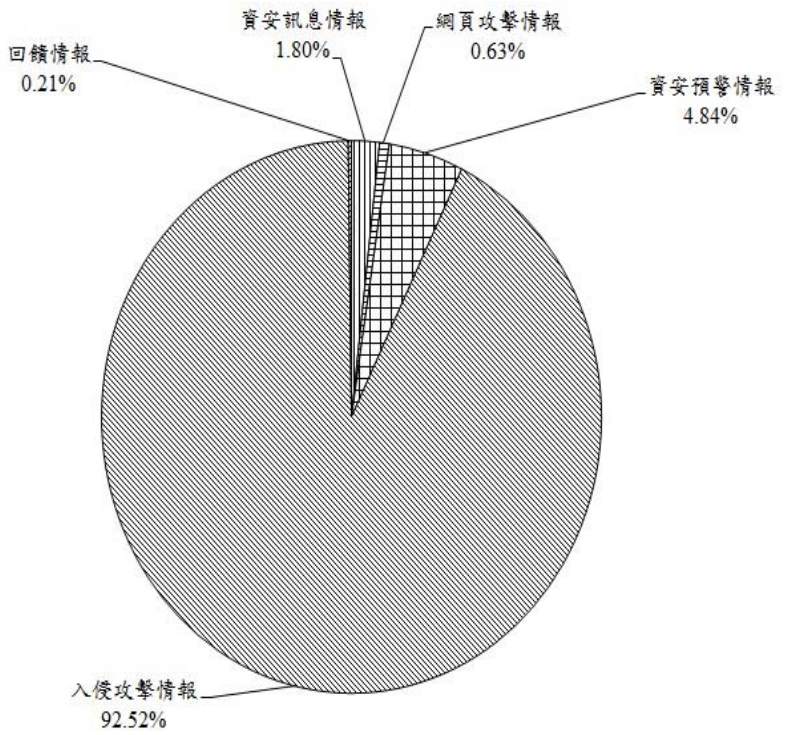


G-ISAC資安情報分享（101/06/01-102/04/30）

資安警訊事件數量分（共計107,736）

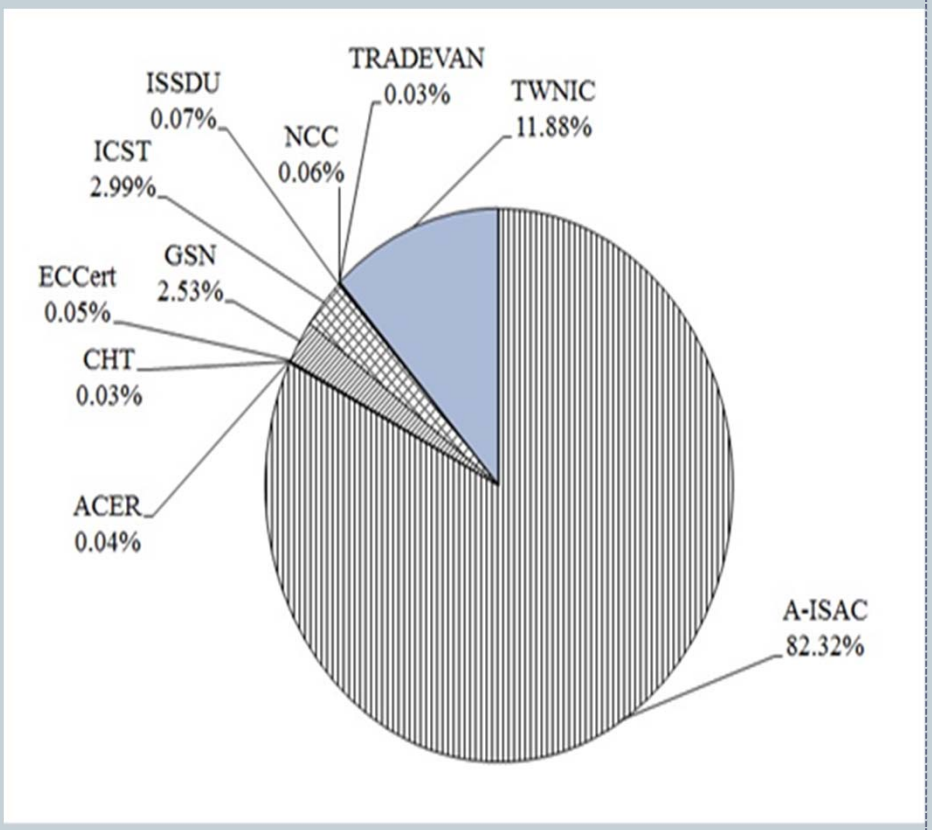


資安警訊事件百分比分布圖

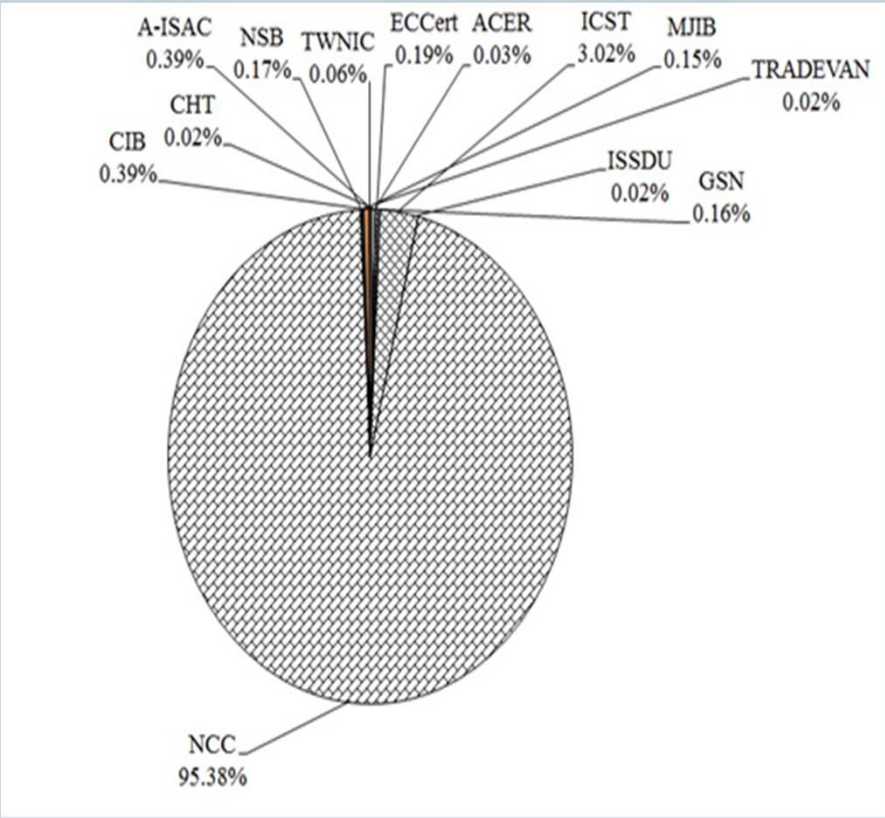


G-ISAC資安情報分享（101/06/01-102/04/30）

G-ISAC會員送出資安事件情報比率分布圖



G-ISAC會員接收資安事件情報比率分布圖



政府資安防護SWOT策略分析圖

優勢S(Strength)

- 設立行政院資安辦統合資安推動策略
- 部分機關已導入ISMS管理制度與SOC資安監控
- 政府機關、電信單位及教育機構之資安資訊分享與分析中心(Information Sharing and Analysis Center, ISAC)已進行資安資訊分享
- 訂定國家資通安全發展方案(102-105)規劃草案

弱勢W(Weaknesses)

- 政府機關雖通過資訊安全管理系統(Information Security Management System, ISMS)驗證，但仍需加強稽核深度
- 資安採購良莠不一，服務水準協議未全面納入要求
- 缺乏全國性情蒐威脅整合
- 通報應變落實仍有改善空間

機會O(Opportunities)

- MSSP業者提供政府機關服務
- 資安治理技術之推動與發展
- 個人資料保護法實施將可提升政府機關對資安與個人資料保護之重視
- 雲端運算之發展趨勢將有助於創新之資訊應用與發展

威脅T(Threats)

- 組織型駭客試圖竊取公務機密之威脅仍未減緩
- 雲端運算與行動服務帶來新的資安威脅與挑戰
- 國際資訊戰與分散式阻斷攻擊事件頻傳
- 關鍵資訊基礎設施面臨威脅

新世代資通情蒐與分析系統

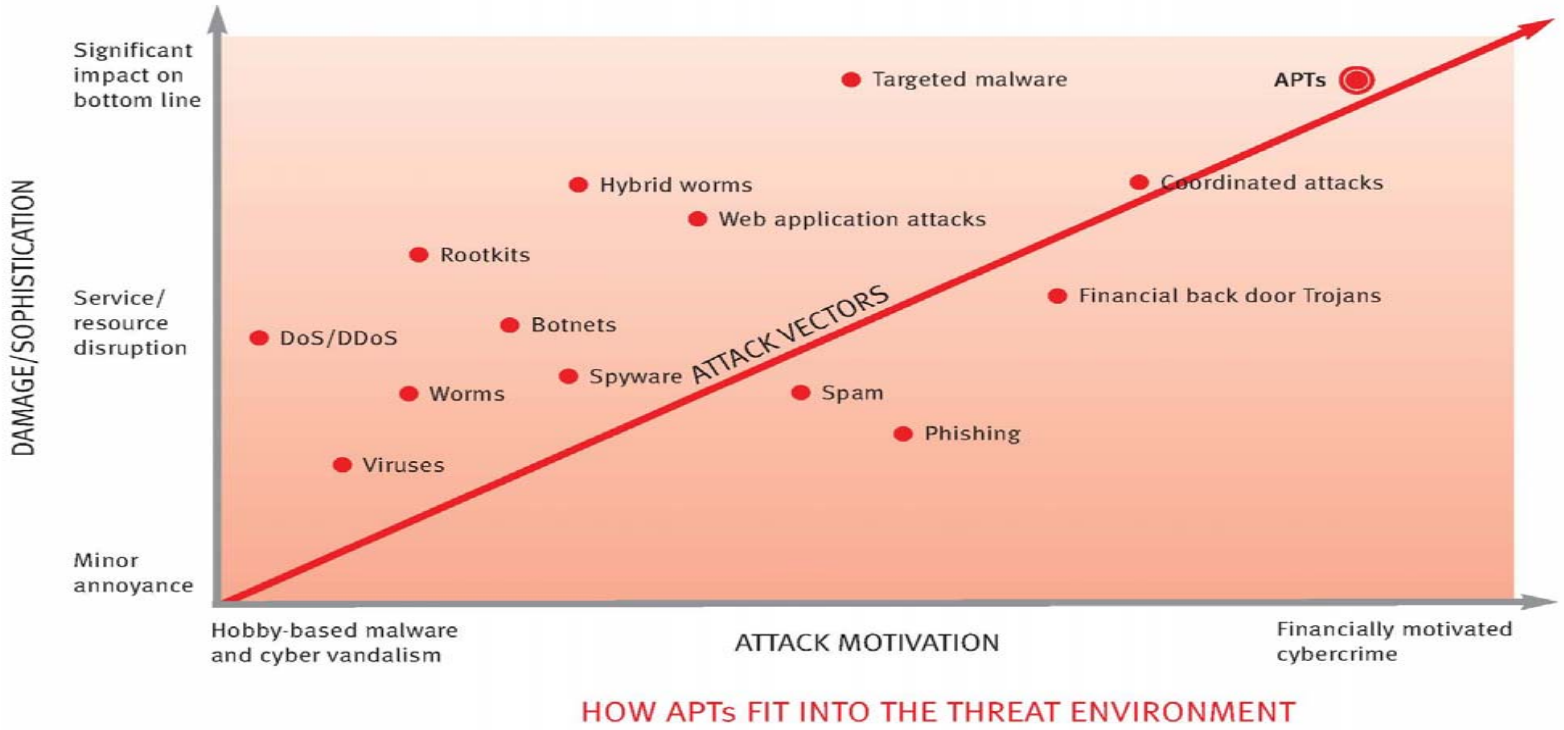
（不具）個人識別碼的資通情蒐、分享、與分析

- 資通訊資料的蒐集類別，大致上分成兩大類：具個人識別碼(Personally Identifiable Information, PII)、不具個人識別碼。
- (不具)個人識別碼的資通情蒐與分析可以透過防火牆(Firewall)與入侵偵測系統（Intrusion Detection System, IDS），以及各種網路設備中繼裝置如Switch, Router等。
- 入侵偵測系統（IDS)可以分成三個世代(Cardenas, et al., 2013)：

1. 第一世代IDS指的是最原始的系統架構
2. 第二世代IDS則是從多重資料源佈建感測器蒐集與篩選回來的示警系統(Security Information and Event Management, SIEM)
3. 第三代IDS則是以巨量資料（Big Data)分析技術為導向的智慧型SIEM系統。

Source: Cardenas, A. A, et al.. 2013. Big Data Analytics for Security Intelligence. Cloud Security Alliance.

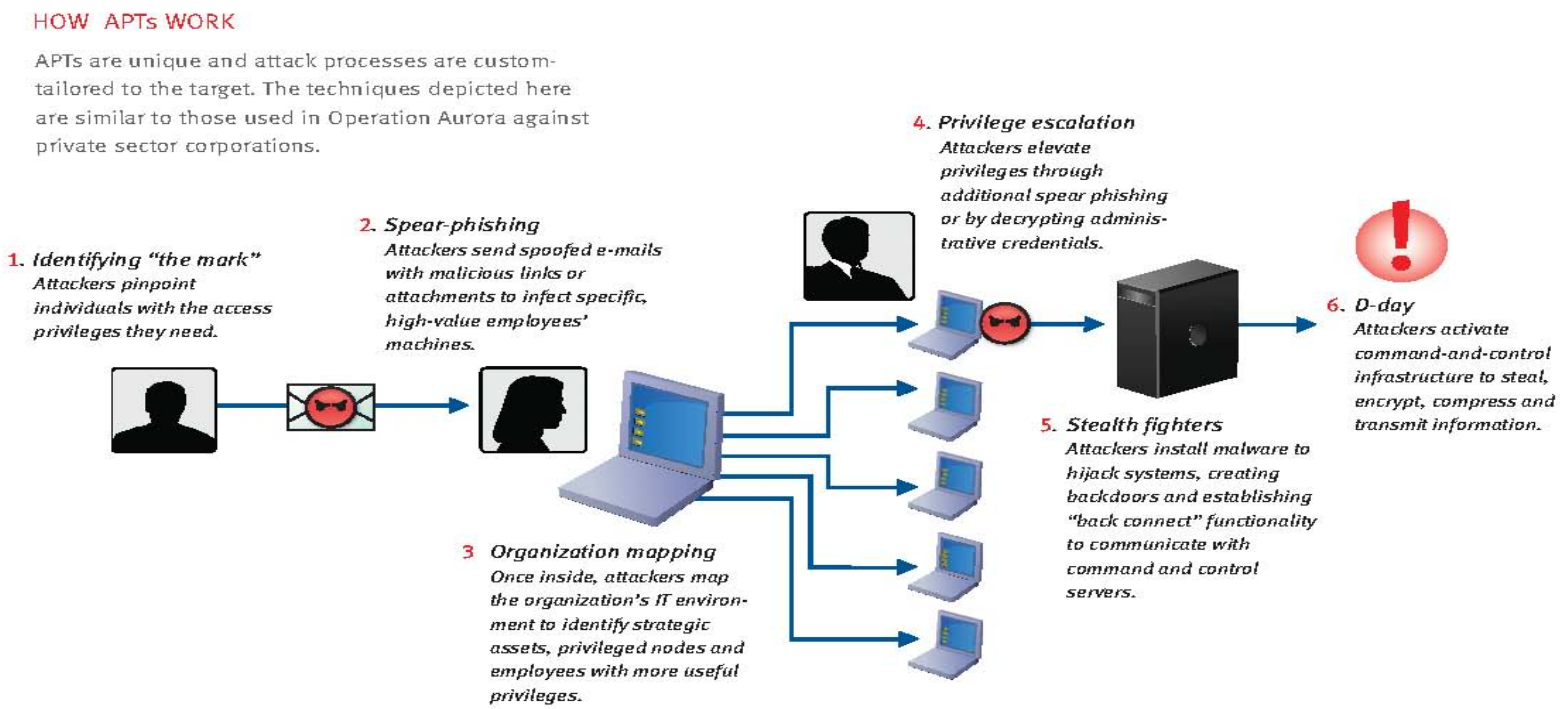
新世代資通情蒐與分析系統



HOW APTs FIT INTO THE THREAT ENVIRONMENT

Source: RSA Security Brief: Mobilizing Intelligent Security Operations for Advanced Persistent Threats. EMC , 2011.

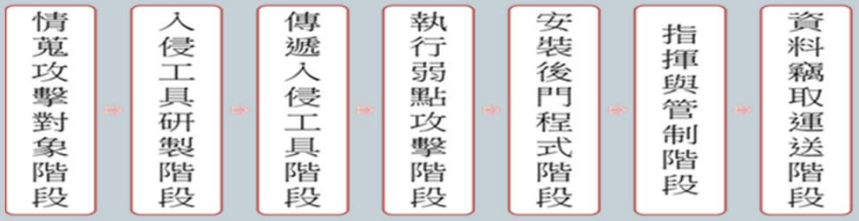
APTs攻擊的運作範例



Source: RSA Security Brief: Mobilizing Intelligent Security Operations for Advanced Persistent Threats. EMC, 2011.

網際網路狙殺鍊(Kill Chain Defense)架構

APT式攻擊的步驟流程



政府現有偵防工具與狙殺鍊比對

階段	A	B	C
情蒐攻擊對象 (Reconnaissance)	O	O	O
入侵工具研製 (Weaponization)	X	X	X
傳遞入侵工具 (Delivery)	X	O	O
執行弱點攻擊 (Exploitation)	O	O	O
安裝後門程式 (Installation)	X	O	X
指揮與管制 (Command and Control)	X	X	X
資料竊取運送 (Actions on Objectives)	X	X	X

A : G-SOC, B : G-ISAC, C : G-ISAC(HoneyBEAR)

資料來源：行政院國家資通安全會報技術服務中心（技服中心），2013，《國內資通訊情蒐分析架構的現況分析與優缺點》

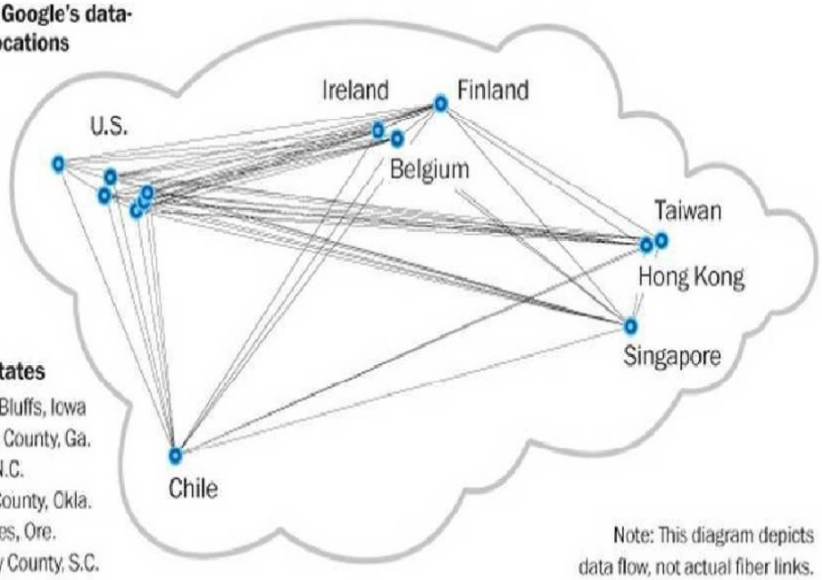
美國NSA 攔截私有企業網路的個人資料

4 Google's global infrastructure

Cloud companies, such as Google and Yahoo, store multiple copies of user data across geographically distributed data centers in order to improve reliability and performance.

Google and Yahoo generally connect their data centers over privately owned or leased fiber-optic cables, which do not share traffic with other Internet users and companies, to enable the fastest connections and keep information secure. Until recently, these internal data networks were not encrypted. Google announced in September, however, that it is moving quickly to encrypt those connections. Yahoo's data center links are not encrypted.

Some of Google's data-center locations



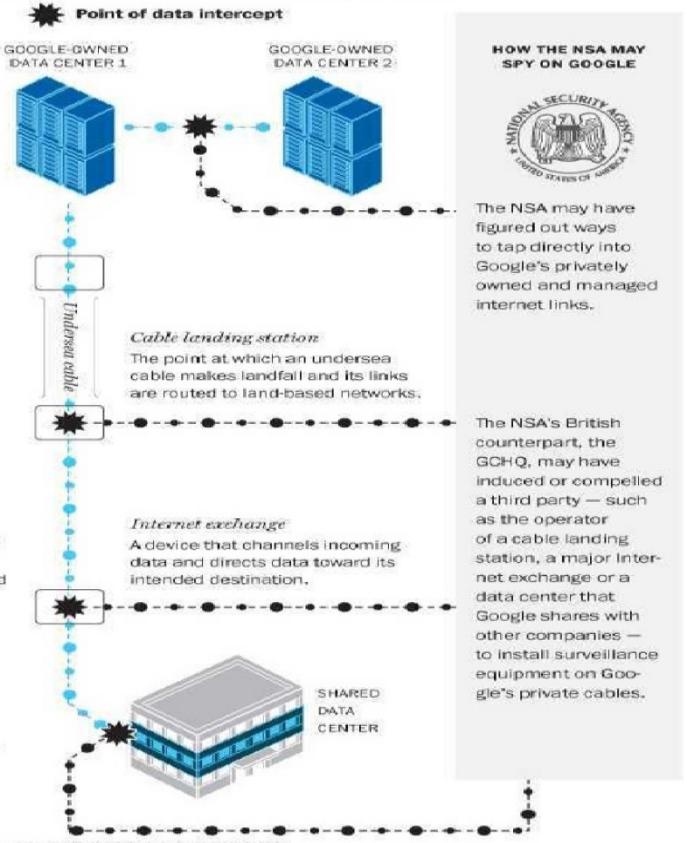
United States

- Council Bluffs, Iowa
- Douglas County, Ga.
- Lenoir, N.C.
- Mayes County, Okla.
- The Dalles, Ore.
- Berkeley County, S.C.

Note: This diagram depicts data flow, not actual fiber links.

5 How the NSA's spying on Google's internal network is intercepting data on Americans

The NSA intercepts user account information as it flows between data centers. The precise collection points and methods are unknown. These are among the possibilities:



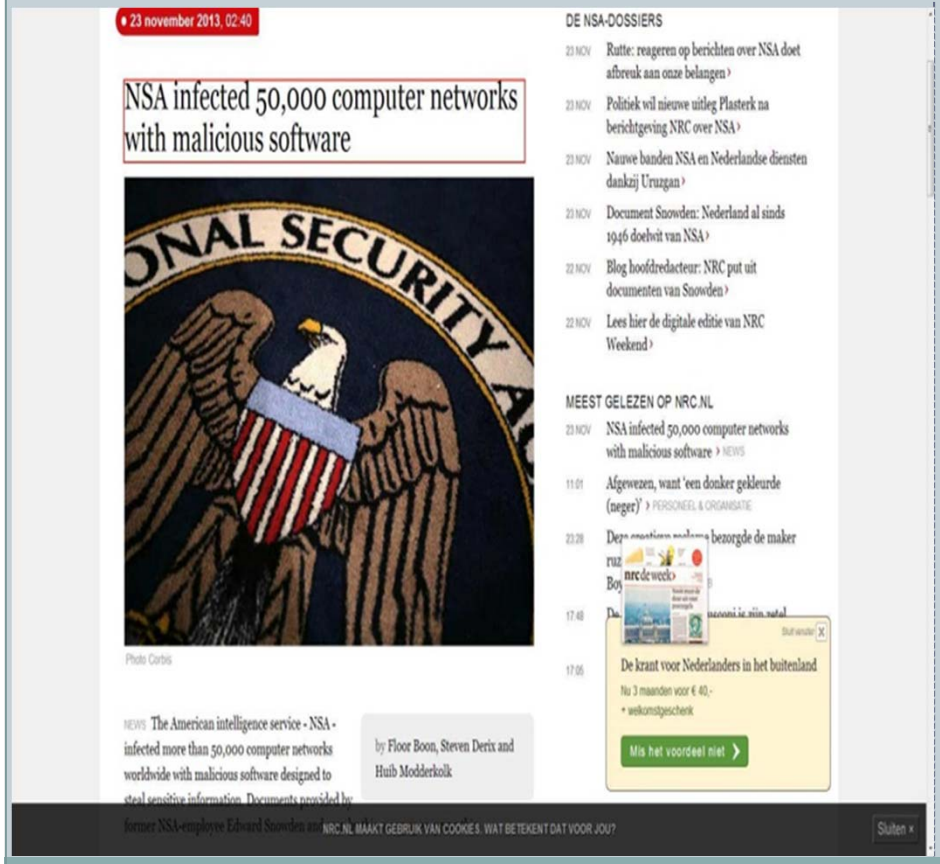
SOURCE: Staff reports; Google, www.google.com/about/datacenters

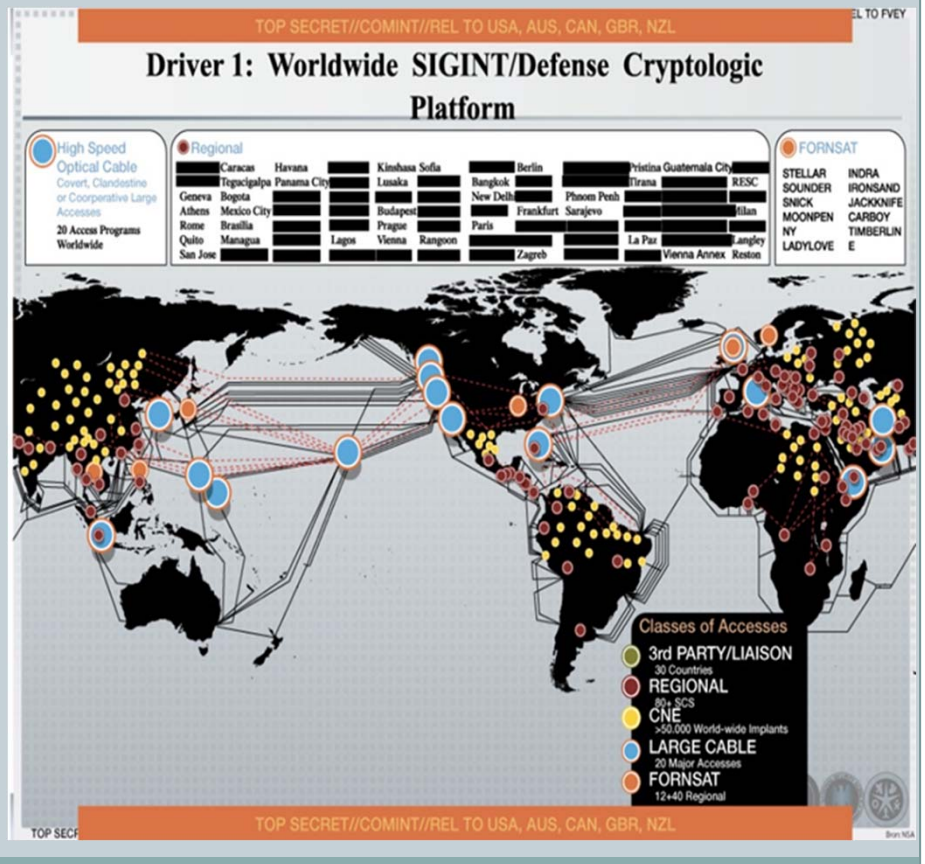
Source: The Washington Post, How the NSA is Infiltrating Private Networks, Gellman, B. et al., Oct. 30, 2013

美國NSA植入大量Implants程式於電腦網路設備

荷蘭NRC Handelsblad 報紙於Nov. 23rd , 2013年報導

全球約有5萬-8.5萬（2013年底）電腦網路設備被植入





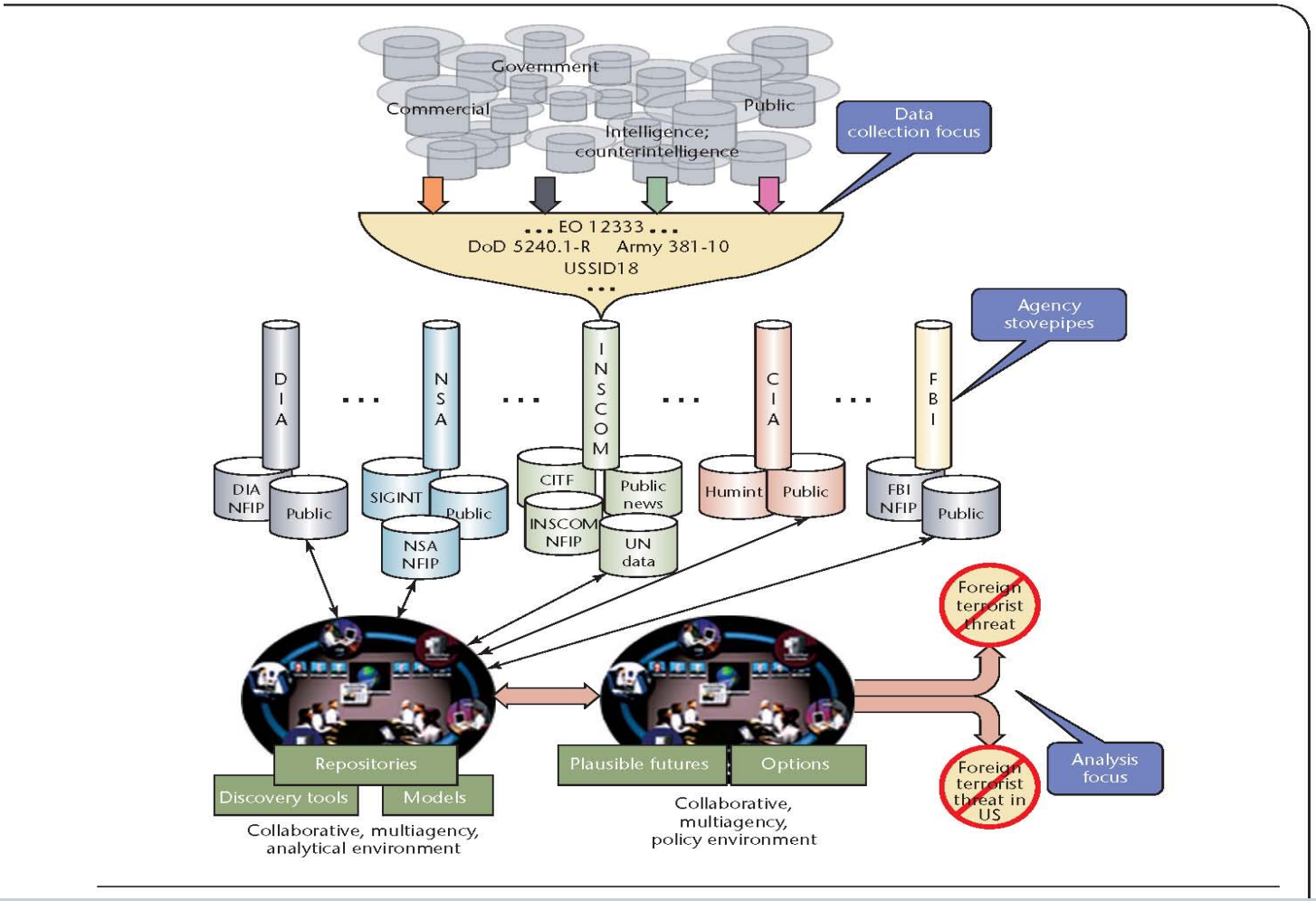
Source: http://www.nrc.nl/nieuws/2013/11/23/nsa-infected-50000-computer-networks-with-malicious-software/

如何兼具國家安全與隱私保護

具個人識別碼(PII)的資通情蒐、分享、與分析

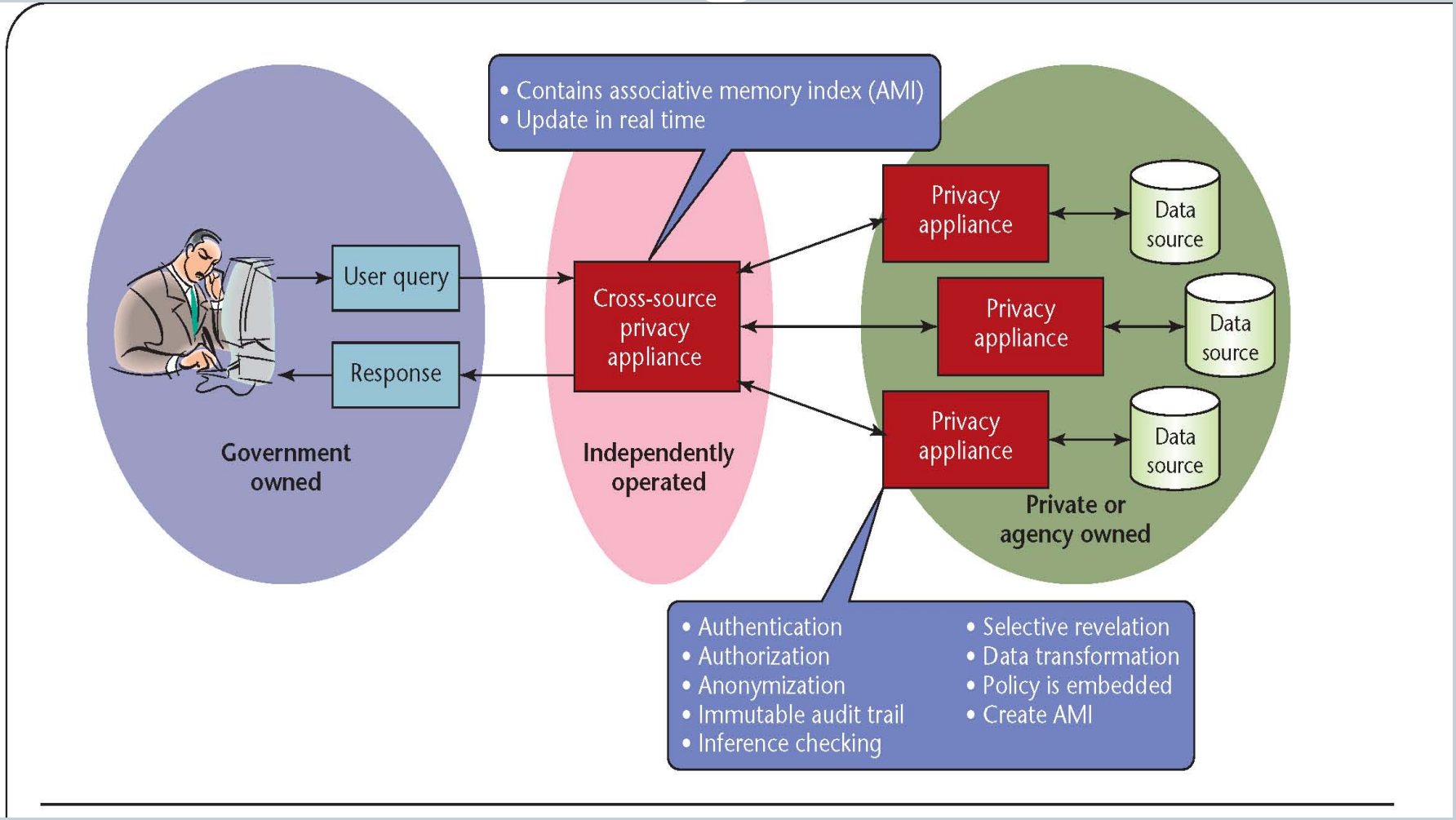
- 蒐集具個人識別碼的個人資料的情蒐、分享與分析，在法律規範的遵守與實際系統運作上則必須要更為小心，否則執法者將面臨個人隱私被侵犯的挑戰。
- 線上社群網路(Online Social Network, OSN)與電子郵件、電話的情蒐與分析，主要是針對犯罪者或恐怖份子透過電腦網路與電話溝通平台所留下紀錄。
- 個人資料蒐集與揭露、分析流程如何有效的找出背後犯罪者的人為因子而不影響他人的隱私保護，進行有效事前預防與事後調查，是執法者所面臨的最大挑戰。

大量個資蒐集、分享、與分析



Source: Popp, R. & J. Poindexter. 2006. "Countering Terrorism through Information and Privacy Protection Technologies." IEEE Computer Security 4(6):18-27.

隱私裝置(Privacy Appliance)確保個人隱私保護



Popp, R. & J. Poindexter. 2006. "Countering Terrorism through Information and Privacy Protection Technologies." IEEE Computer Security 4(6):18-27.

相關研究

- 國家(資訊)關鍵基礎設施安全防護政策與執行的現況(科顧組，2009；科顧組，2011；國土辦，2012；技服中心，2013)。
- 資訊安全與通訊知名大廠如RSA(EMC), Symantec, McAfee, Verizon所提的研究報告（Baker, et al, 2010; Curry, et al., 2011; Symantec, 2013）。
- 美國國家科學院報告(National Academy of Science, 2008)與Wiley/IEEE所出版的專書(Popp & Yen, 2006)。
- 資訊安全與資訊戰的年度知名國際研討會，如（歐洲）Annual European Conference of Cyber Warfare and Security (ECCWS)，（美國）International Conference on Information Warfare and Security (ICCWS), Journal of Information Warfare (Abouzakhar, 2013; Hutchins, et al., 2011)。

結論與未來研究

- 具體且有效的整合資安監控中心(SOC)、電腦危機處理應變中心(CERT)、資訊分享與分析中心(ISAC)三種類型資安事件情蒐、分享、與分析平台。
- 透過雲端運算共購機房整合資訊安全系統平台的運作以強化國家關鍵資訊基礎設施防護網。
- 在雲端運算分散式平台上整合巨量資料分析的新技術，強化新型態網路攻擊與入侵資安事件的預防與偵測能力。
- 參考歐美相關資訊系統與法律規範、因地制宜建置一套兼顧國家安全與個人隱私保護的資通與個人情資蒐集與分析系統。

參考文獻

一、　　中文文獻

- 行政院科技顧問組（科顧組），2009，《國家資通訊安全發展方案》，行政院國家資通安全會報
- 行政院科技顧問組（科顧組），2011，《關鍵資訊基礎建設保護政策指引》，行政院國家資通安全會報
- 行政院國土安全辦公室（國土辦），2012，《國家關鍵基礎設施安全防護計畫指導綱要》
- 行政院國家資通安全會報技術服務中心（技服中心），2013，《國內資通訊情蒐分析架構的現況分析與優缺點》

參考文獻

二、　外文文獻

- Abouzakhar, N. 2013. Critical Infrastructure Cybersecurity: A Review of Recent Threats and Violations. 12th Annual European Conference of Cyber Warfare and Security (ECCWS). University of Jyväskylä, Finland.
- Baker, W. et al.. 2010. 2010 Data Breach Investigation Report. Verizon Inc.
- Cardenas, A. A, et al.. 2013. Big Data Analytics for Security Intelligence. Cloud Security Alliance.
- Curry, S. et al.. 2011. RSA Security Brief: Mobilizing Intelligent Security Operations for Advanced Persistent Threats. EMC, RSA.
- Giura, P. & W. Wang. 2012. Using Large Scale Distributed Computing to Unveil Advanced Persistent Threats. New York, NY. AT&T Security Research Center.
- Hutchins, M. E., et al.. 2011. Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. 6th Annual International Conference on Information Warfare and Security. Washington, DC.

參考文獻

- Krekel, B., et al... 2009. Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation, Prepared for The US-China Economic and Security Review Commission. Washington, DC, Research Report. Northrop Grumman.
- Manyika, J., et al.. 2011. Big Data: the Next Frontier for Innovation, Competition, and Productivity. Technical Report, McKinsey Global Institute.
- National Academy of Sciences. 2008. Protecting Individual Privacy in the Struggle Against Terrorists. Washington, DC, USA. The National Academies Press.
- Popp, R. & J. Poindexter. 2006. "Countering Terrorism through Information and Privacy Protection Technologies." IEEE Computer Security 4(6):18-27.
- Popp, R. & J. Yen, eds.. 2006. Emerging Information Technologies and Enabling Policies for Counter-Terrorism. Wiley & Sons/IEEE Press.
- PREDICT. 2011. Protected Repository for the Defense of Infrastructure Against Cyber Threats (PREDICT). https://www.predict.org/ .

參考文獻

- Rinaldi, M. S., et al. 2001. Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies. IEEE Control System Magazine 11-25.
- Symantec. 2013. Internet Security Threat Report 2013. CA, USA. Symantec Corp.
- WOMBAT. 2011. Worldwide Observatory of Malicious Behaviors and Attack Threats (WOMBAT). http://www.wombat-project.eu/ .