# 雲端與物聯網時代的資安挑戰與思維

林一平

科技部 政務次長

# 簡報大綱

- 教育體系資訊安全防護架構
- 近期資安威脅案例
- 物聯網資安風險與思維
- 近期政府資安政策

# 教育體系資訊安全防護架構

## 資安防護架構

1. 建立監控及分析機制：

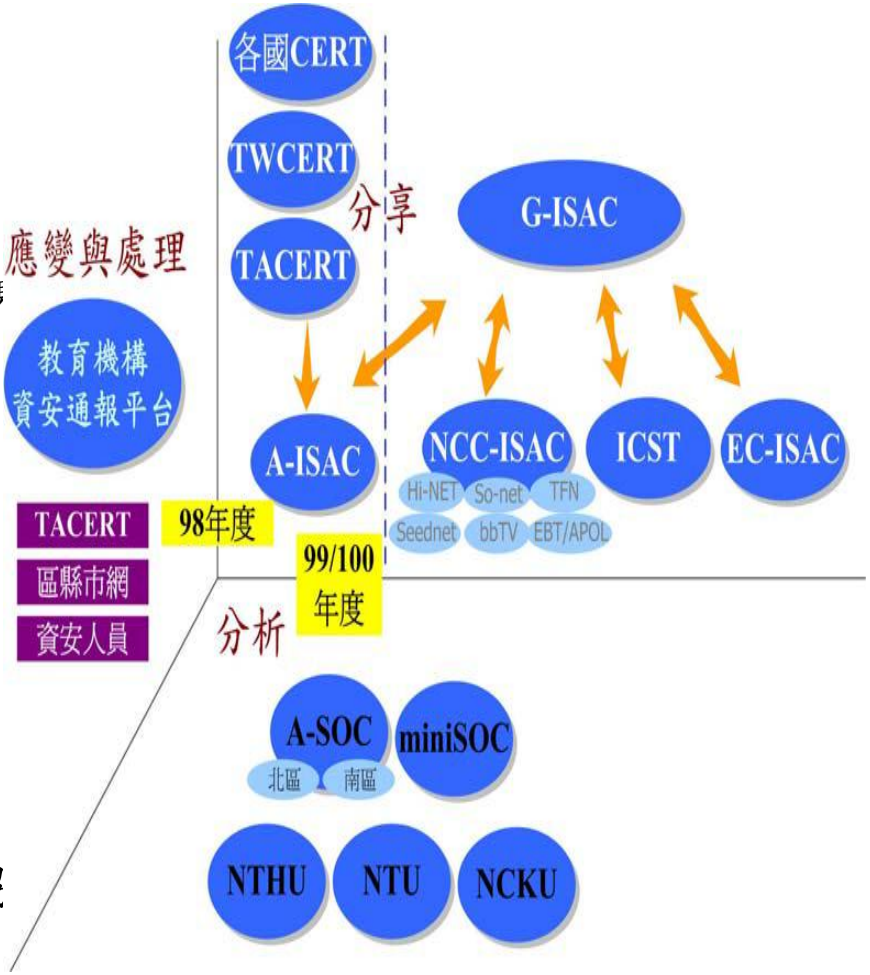
   (1)建置北區及南區資安監控中心，主動監測TANet範圍內資安事件

   (2)建置Mini-SOC以主動協助各縣市教網中心監測資安事件

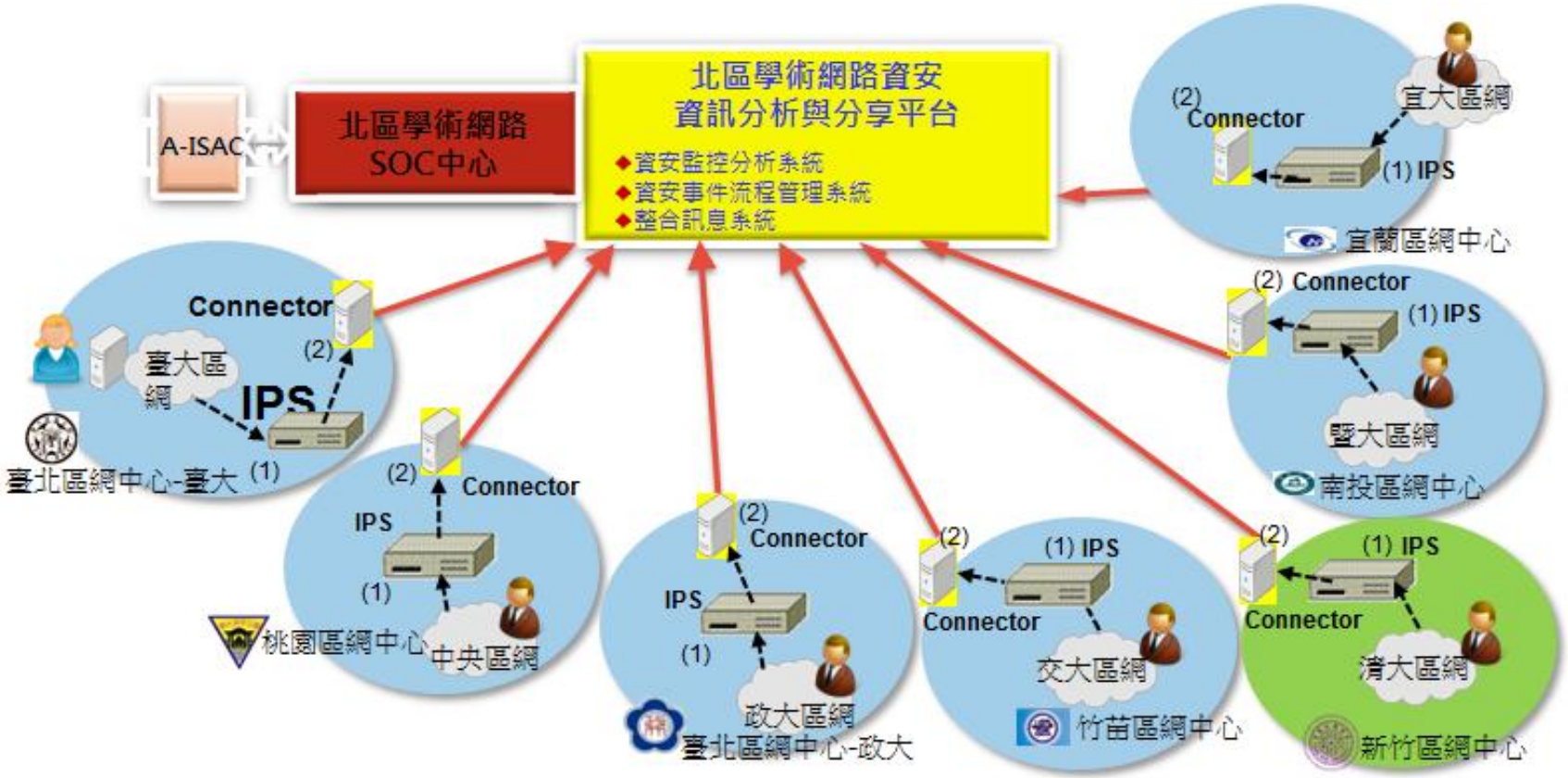
   (3)建置教育部本部資安監控中心

2. 通報及分享：建置A-ISAC自動將資安警訊通報區縣市網路中心及學校資安人員，非學術機構之資安警訊分享至G-ISAC。

3. 應變與處理：設置TACET機制，管制及協助學校對資安事件適當應變與處理

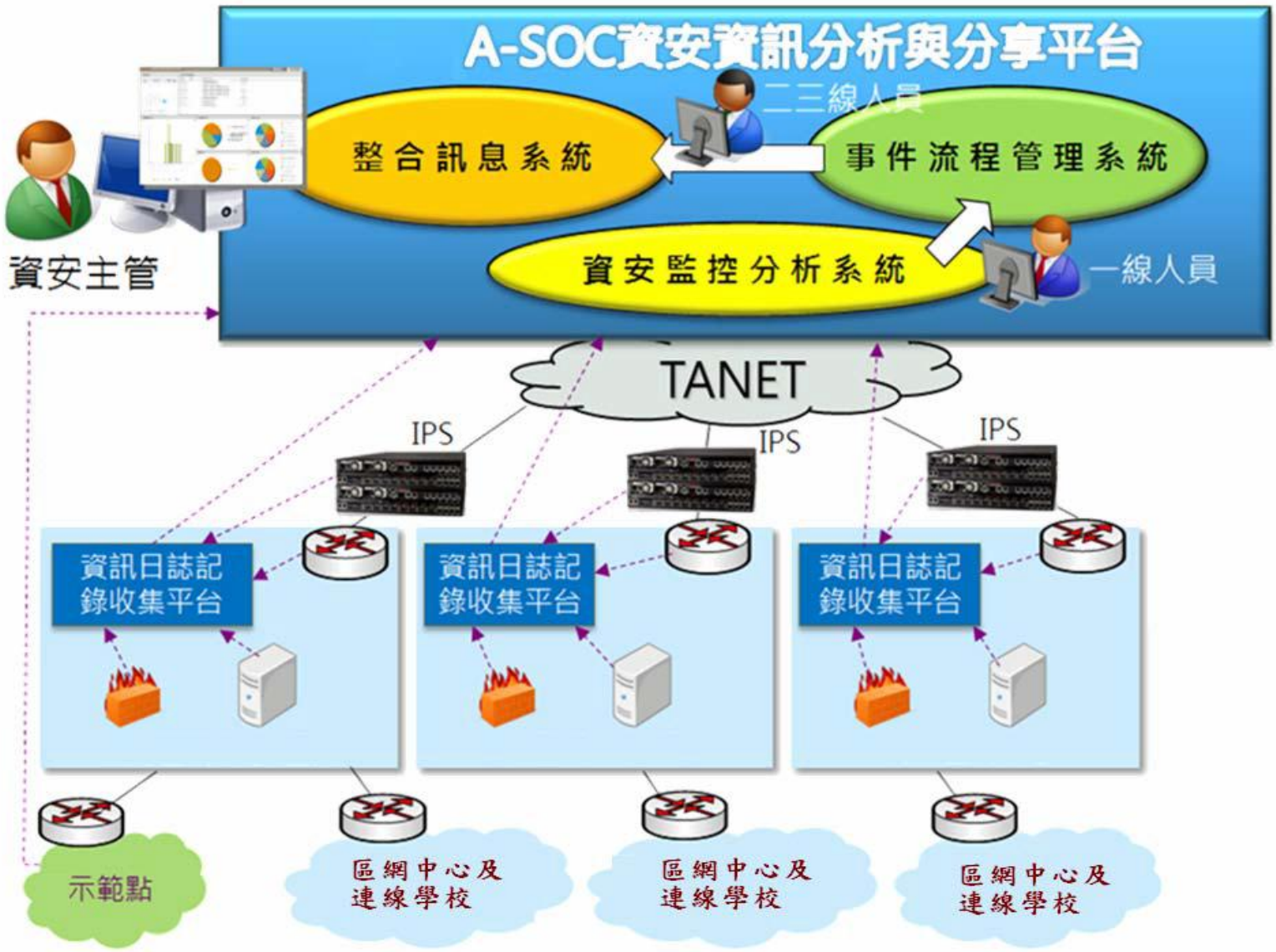


# 北區A-SOC:資安偵測架構

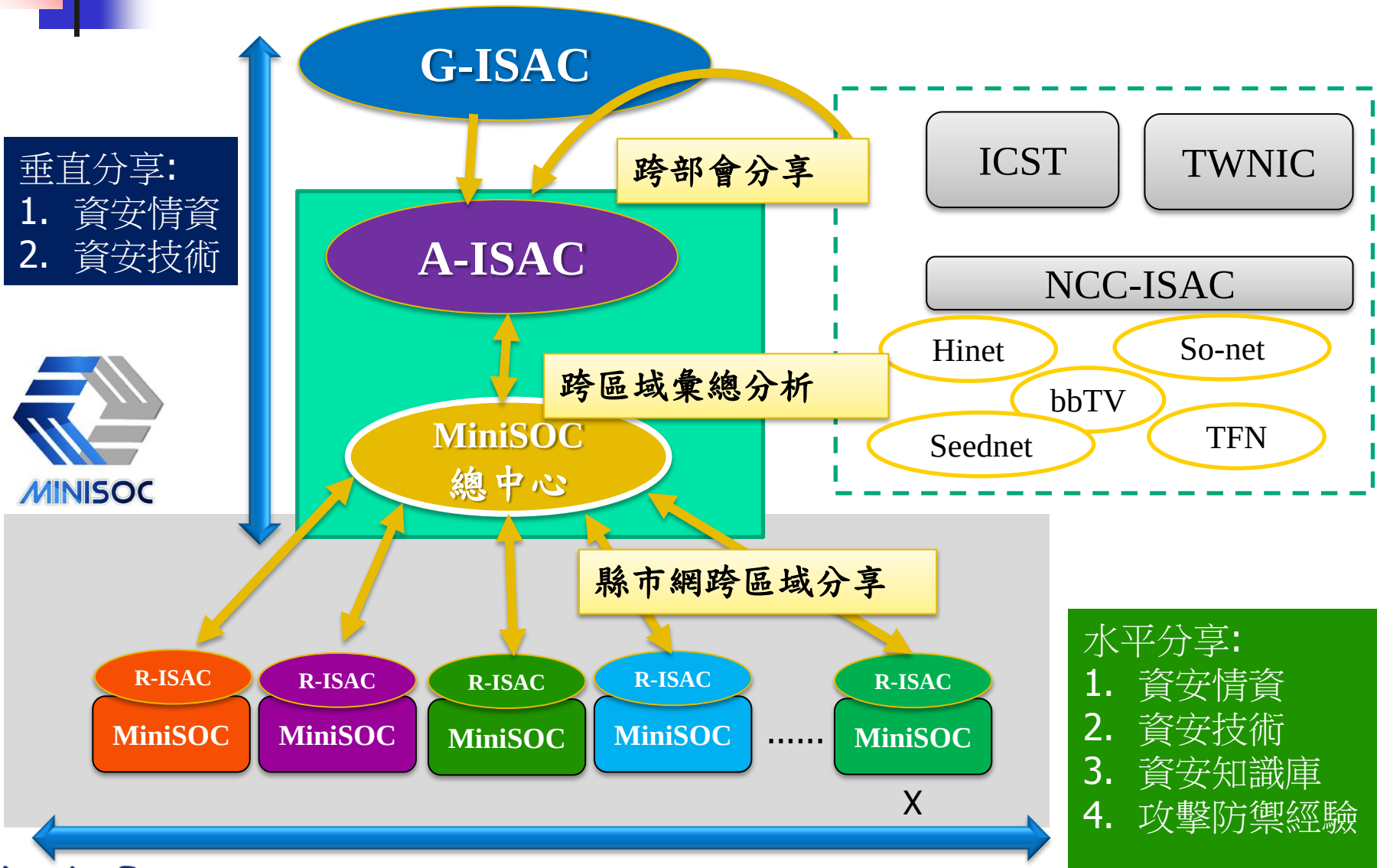



出處:北區ASOC整理

# 南區A-SOC:資安偵測架構



# MiniSOC縣市網分享架構



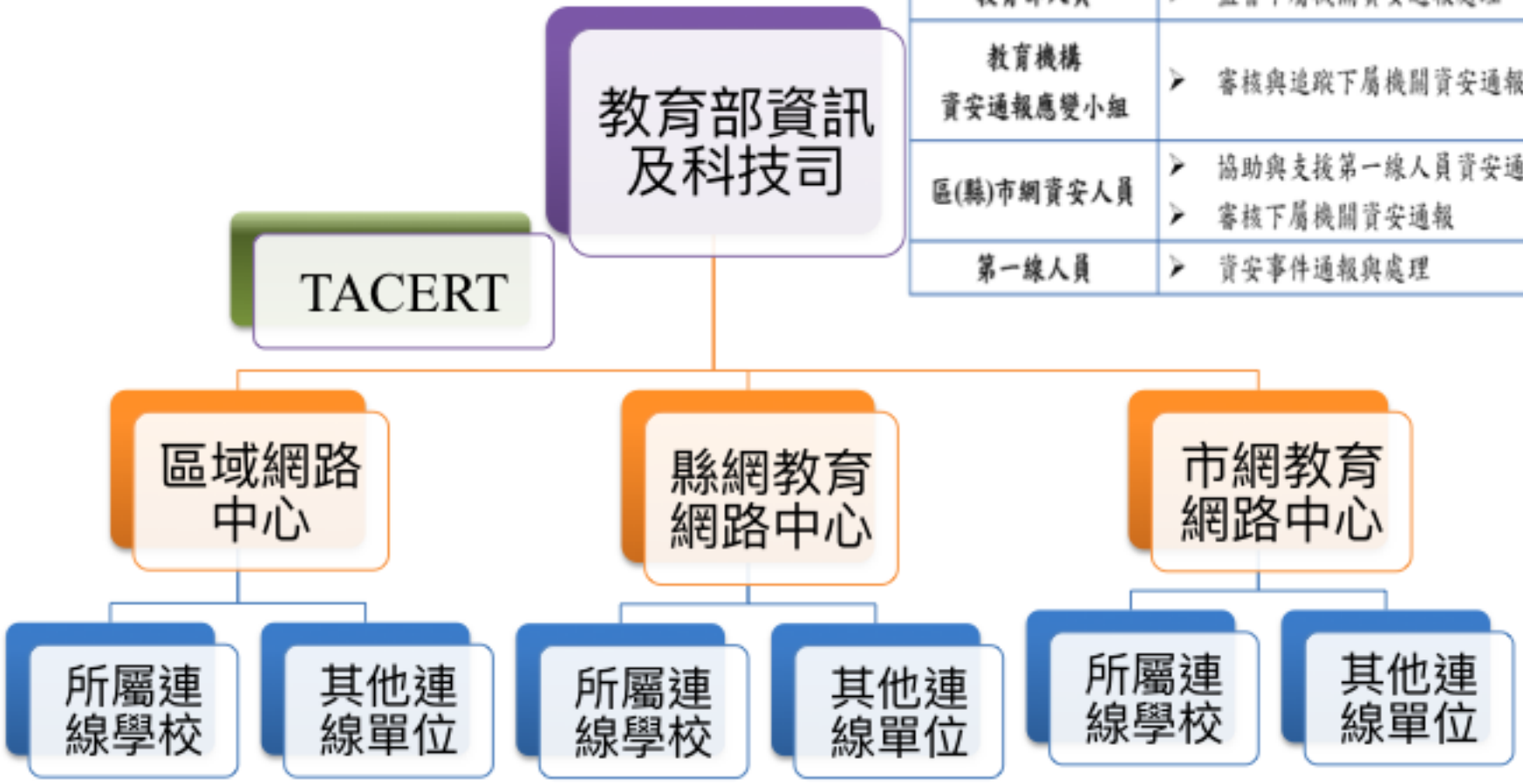

垂直分享:
1. 資安情資
2. 資安技術

水平分享:
1. 資安情資
2. 資安技術
3. 資安知識庫
4. 攻擊防禦經驗

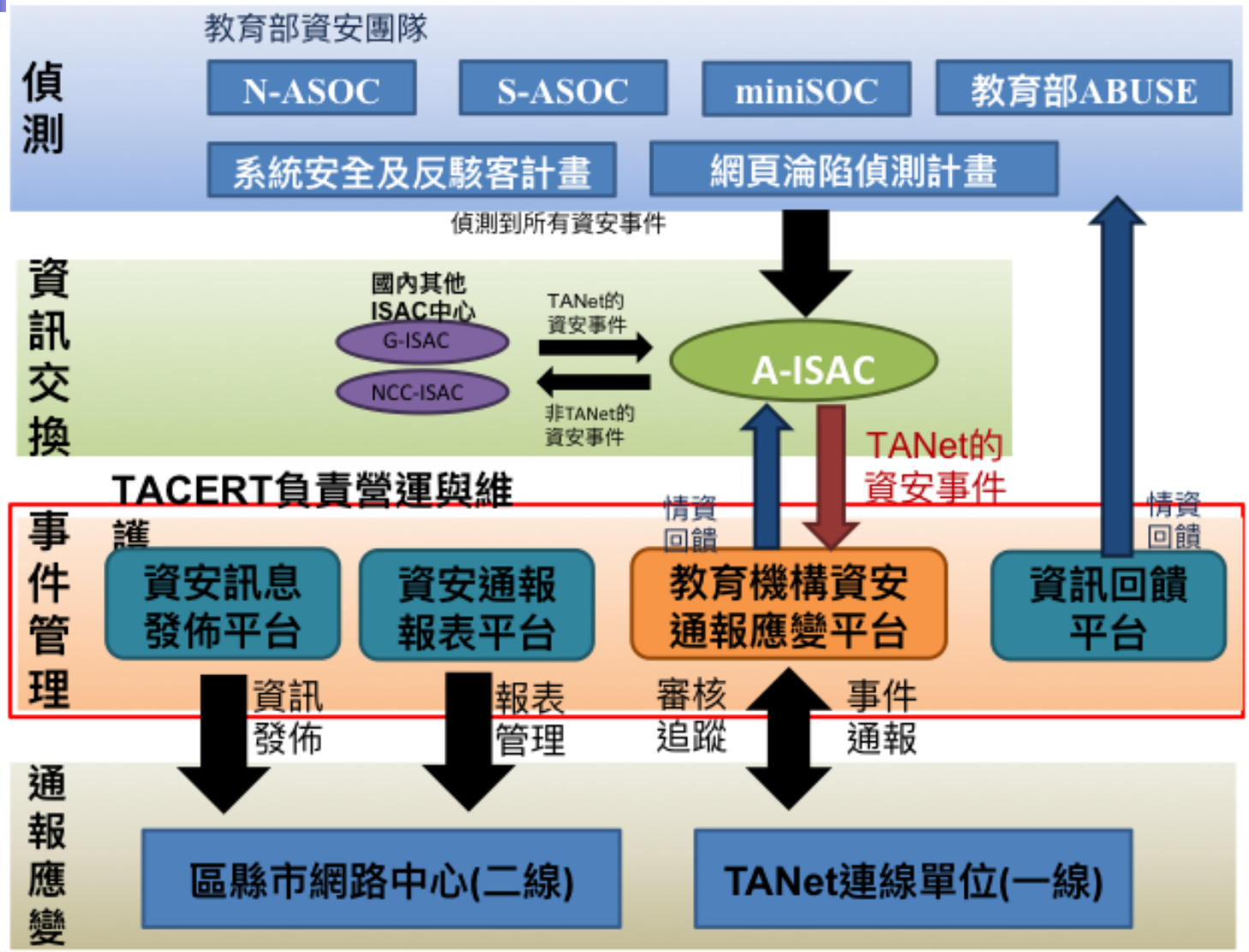
科技部 Ministry of Science and Technology

# TACERT運作方式

| 使用角色 | 工作事項 |
| --- | --- |
| 教育部人員 | ➢ 監督下屬機關資安通報處理 |
| 教育機構<br>資安通報應變小組 | ➢ 審核與追蹤下屬機關資安通報 |
| 區(縣)市網資安人員 | ➢ 協助與支援第一線人員資安通報<br>➢ 審核下屬機關資安通報 |
| 第一線人員 | ➢ 資安事件通報與處理 |



# 教育機構資安通報機制運作



# 依資安等級區分

## 1、2級資安事件

- 事件處理時間通報於24小時內完成，應變於72小時內完成（通報+應變）
- 電子郵件通知寄發
  - 事件單成立後1個小時
  - 事件單成立後每隔12個小時
  - 事件單成立後72小時後每隔12個小時寄發逾時通知

## 3、4級資安事件

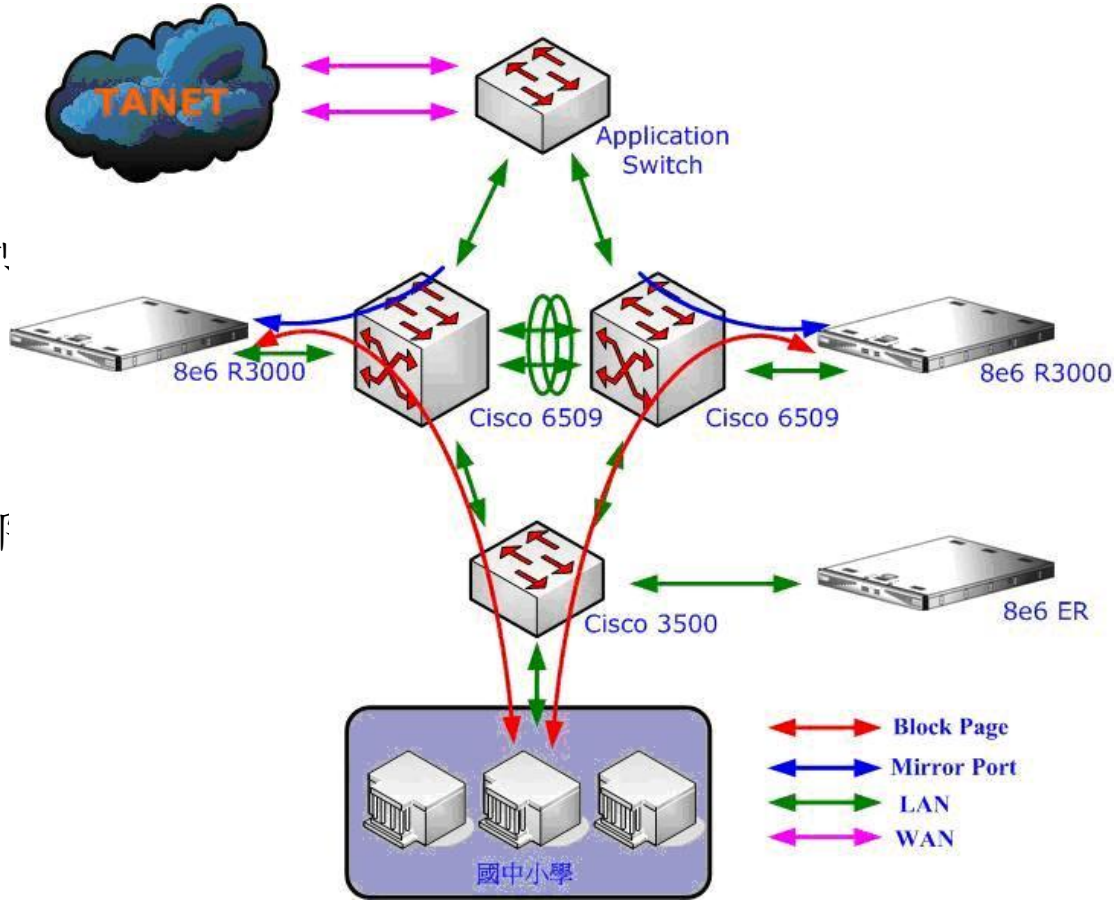
- 針對政府或國家等級之攻擊行為或其他重大資訊安全事件。
- 事件處理時間為36小時內完成
- 需和上級管理單位報備且建立連絡並指定相關人員待命追蹤處理狀況
- 電子郵件通知寄發
  - 事件單成立後1個小時
  - 事件單成立後每隔12個小時
  - 事件單成立後36小時後每隔12個小時寄發逾時通知

# 臺灣學術網路不當資訊防制

目的：防制色情、暴力、毒品、賭博及其它有害身心健康的資訊侵入校園，以保護學生身心健康安全

建置及維運：包括不當資訊防制系統、統計報表系統、申訴與檢舉機制、不當資訊專屬網站。

架構：於各縣市教育網路中心部署不當資訊防制設備及系統，防制範圍為其服務連線之國中小學電腦設備。

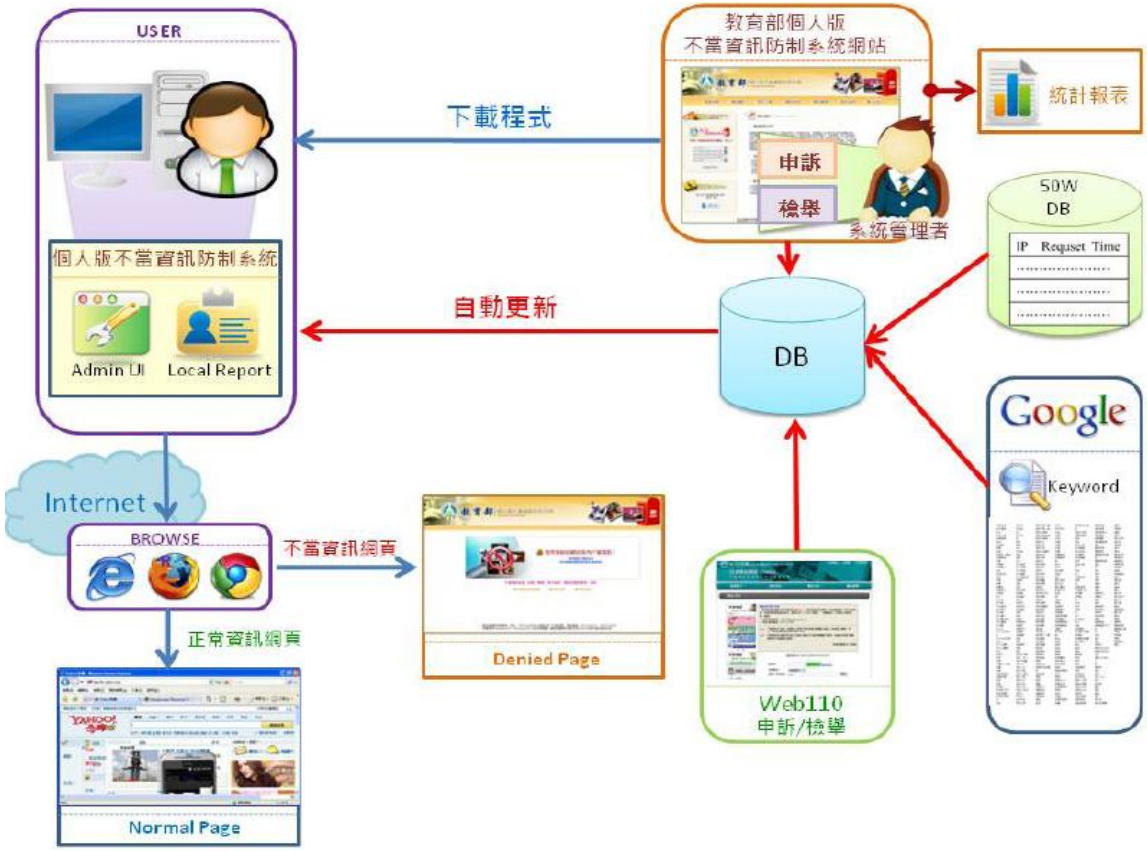



成效：對於不當資訊網站的判別正確性在95%以上。年度內成功阻擋不當資訊網站瀏覽計二億三千萬餘次。

# 網路守護天使系統(NGA)

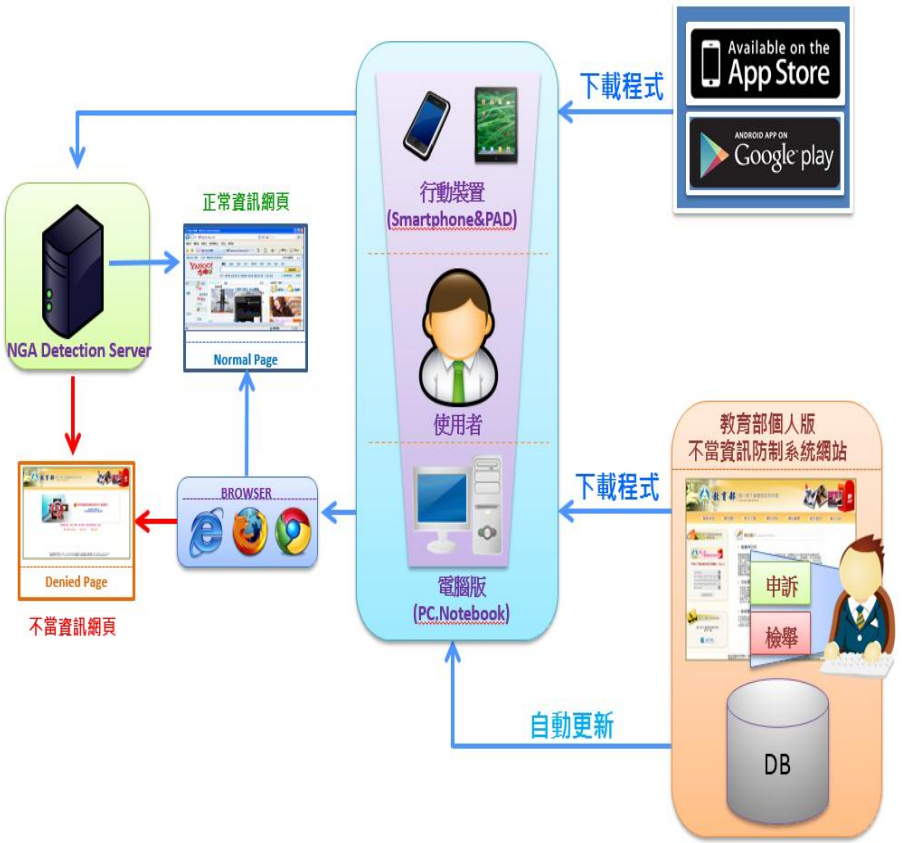
目的：提供學生及家長下載安裝「網路守護天使」軟體，自動過濾不宜瀏覽之網站，及網路使用時間設定功能，使學生養成良好的電腦及網路使用習慣。

成效：平均每月阻擋不當網站數為112,941次，103年度可望達百萬次阻擋成效。



# 網路守護天使系統-行動平臺版

- 近年來除了原本桌上型電腦之外，更是行動裝置百花齊放的時代，為了因應不同的系統，帶來不同的阻擋模式，於是建立了行動雲端偵測架構(NGA Mobile Detection Server)，在此架構下，只要不同的上網設備，安裝好NGA主程式，都可以被保護。



# 簡報大綱

- 教育體系資訊安全防護架構
- 近期資安威脅案例
- 物聯網資安風險與思維
- 近期政府資安政策

# 全球資安風險主要樣態


網路與經濟罪犯大量竊取個人隱私資料，影響電子商務與金融運作


組織型駭客以進階持續威脅(Advanced Persistent Threat)竊取公務、國防及商業機密


關鍵基礎建設透過開放系統與網際網路遭實體破壞風險倍增


資訊與資安供應商持續遭駭，破壞信任價值鏈，危及網際網路整體運作


資訊戰(Cyber-warfare)與分散式阻斷攻擊癱瘓國家網路運作

# 全球已發生近6百起個資遭竊案例

2月醫療保險業者7,880萬筆個資遭駭

Anthem. BlueCross BlueShield

9月數據處理商遭駭造成
T-Mobile 1,500萬筆個資遭駭

Experian™

itrc Identity Theft Resource Center
www.IDTheftCenter.Org

2015全球已發生591起個資竊取案例
超過175,443,888筆個資遭洩漏


7月偷情網站3,700萬筆個資遭駭

UCLA Health

9月加州大學醫療網
450萬筆個資遭駭

TalkTalk
Brighter Phone & Broadband

10月英國電信商400
萬筆個資遭駭

科技部 Ministry of Science and Technology

# 資安廠商面臨情報機構與內部洩密威脅

gemalto
security to be free

]HackingTeam[

- 全球最大SIM卡製造商，年產量20億張供應400家電信業者
- The Intercept報導指出，美英情報機構(NSA與GCHQ)自2010年起聯手駭進Gemalto內網，竊取SIM卡加密金鑰
- 據信美英已可存取核心行動網路，監控全球網路與行動通訊

- 專門協助各國政府執行監控任務並開發間諜軟體
- 駭客於網路公布400GB資料，涵蓋了內部文件、程式碼與電子郵件等，並有許多客戶相關機敏資料
- 許多專供政府機構使用的遠端控制系統(Remote Control System, RCS)原始碼也遭竊

# 美國政府遭遇史上最嚴重之APT攻擊

## ❖美國聯邦人事行政管理局兩度遭入侵

- 駭客2014年底已入侵資料庫，國土安全部安裝的「愛因斯坦」監控系統至2015年4月才偵測發現入侵行為
- 似由2015年攻擊Anthem保險公司的同一批中國大陸駭客所為

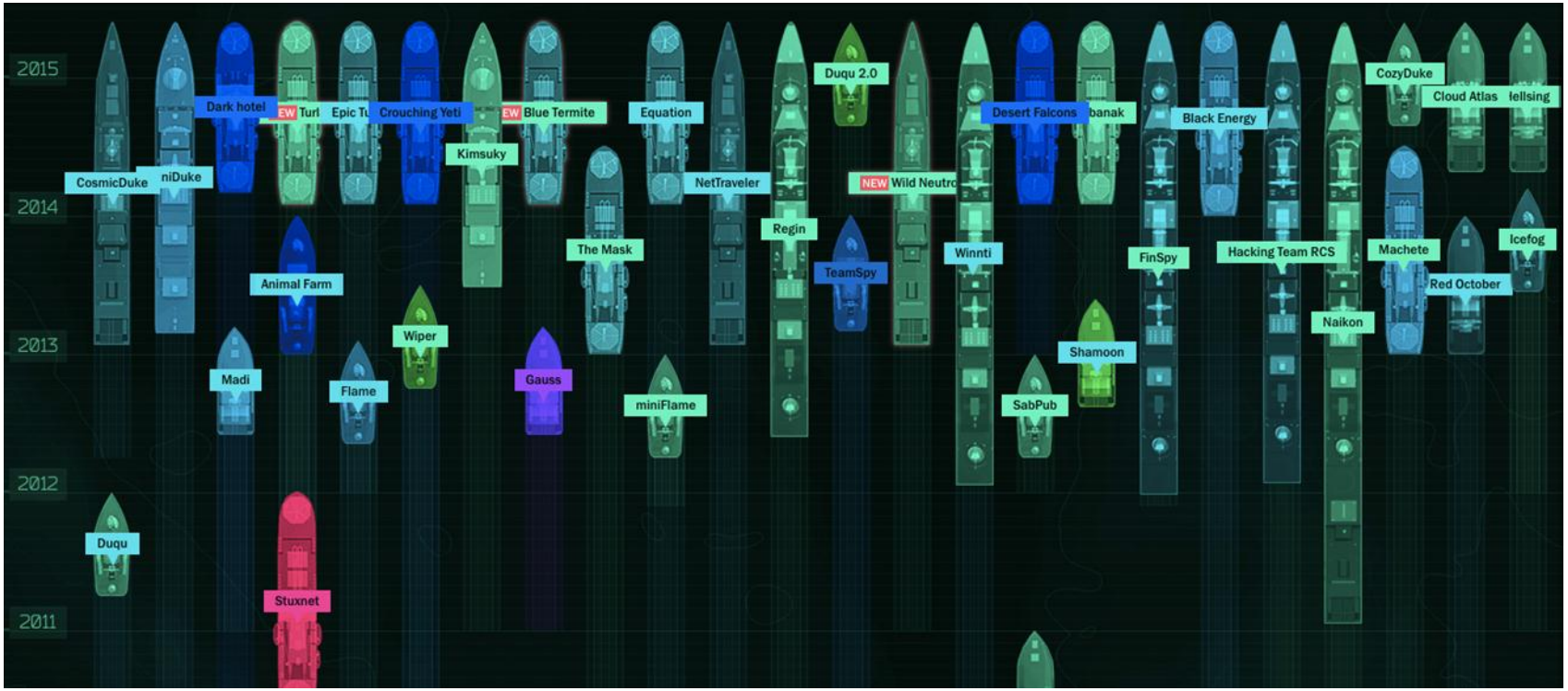
影響衝擊

- 2,210萬筆個人資料(包括現職/離職公務員、親友及承包商)、560萬筆指紋辨識資料遭竊
- 局長阿庫列塔(Katherine Archuleta)女士辭職下台
- 美國政府花費1億3千萬美金提供受害者信用監控
- 中情局將特工撤離中國大陸
- 人事資料與保險資料交叉分析將導致資安風險劇增


美國人事行政管理局網站公告入侵事件

# 世界各國競相投入建立網駭能量

- 自2014~2015年超過20個APT駭客團體被發現在全球活躍
- 除了美國、英國、中國大陸、蘇聯、以色列等外，許多新興的APT團體來自北韓、中東等國家




資料來源：https://apt.securelist.com/

# 航空業資安攻擊嚴重性持續攀升

5月FBI約談聲稱多次駭進機上娛樂系統與飛機推力管理系統之資安研究人員


1月底馬航官網遭網頁置換顯示’ 404 – Plane not found’


7月波蘭航空地面操作系統遭DDoS攻擊癱瘓，1,400名旅客受困機場5小時

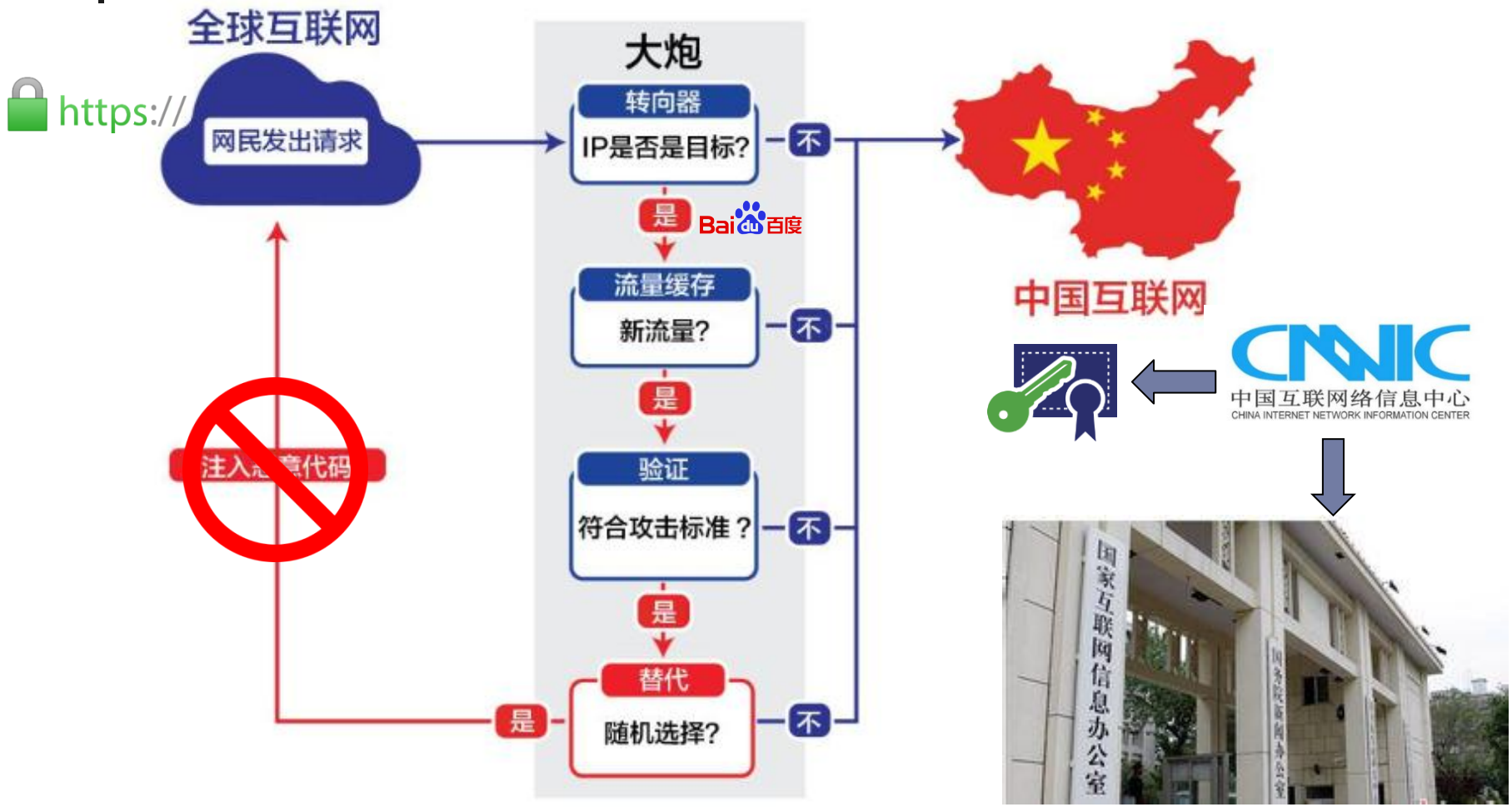

4月瑞安航空購買燃油電子轉帳過程遭竊500萬元美金

American Airlines AAdvantage

MileagePlus UNITED

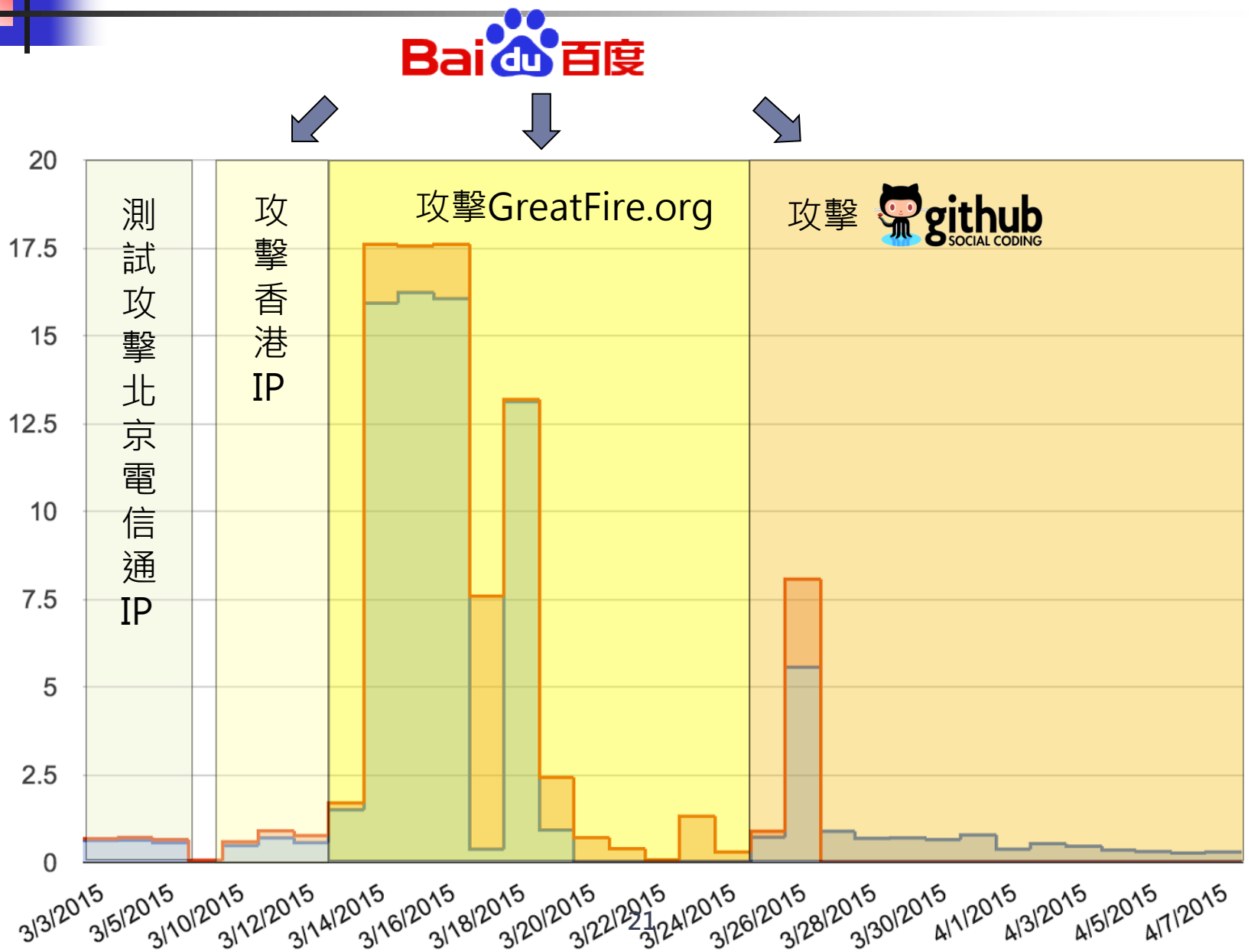
1月初萬名美國航空與聯合航空旅客帳戶哩程遭竊

# 中國大陸發展網路大砲系統

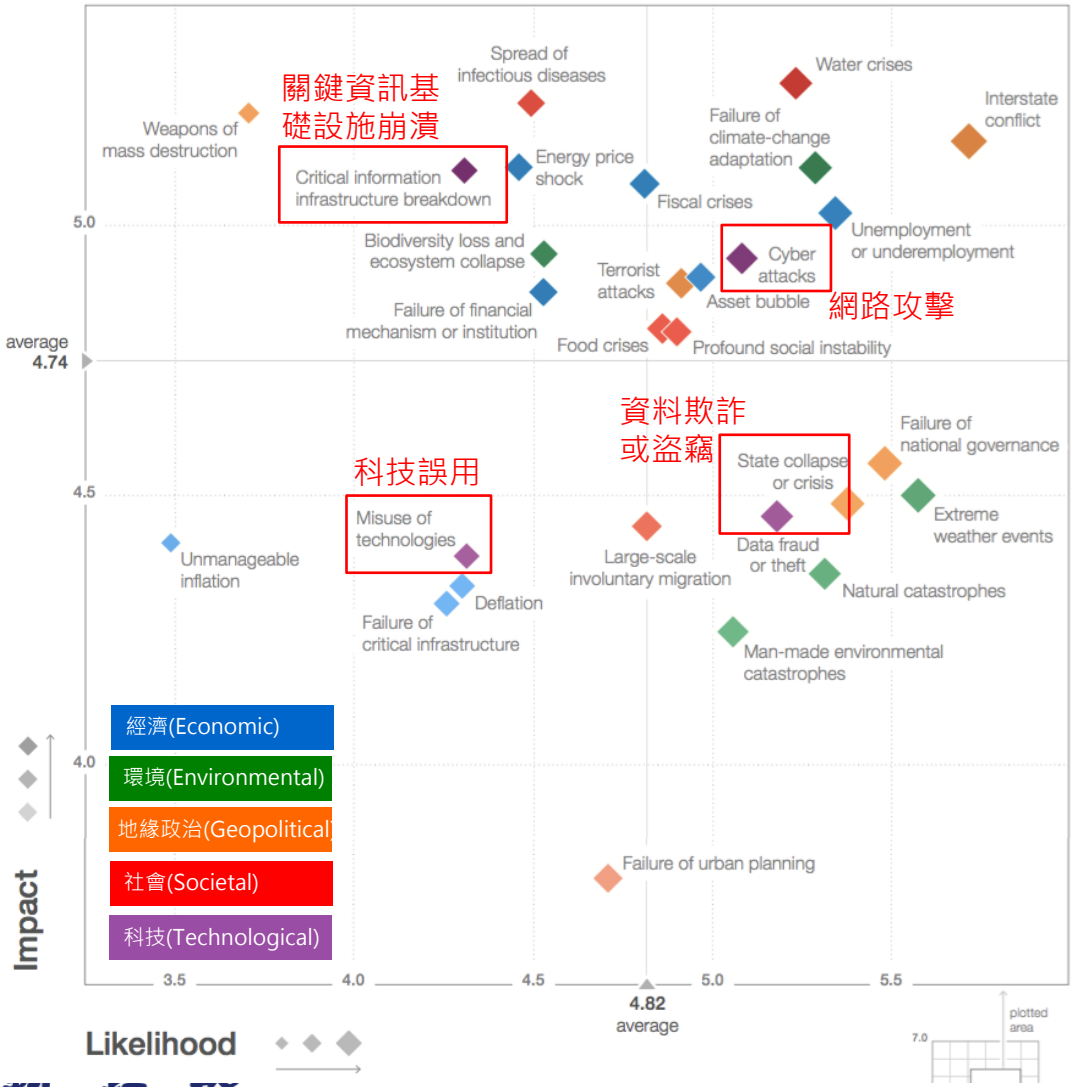



即使百度和其他中國大陸網站全面實施加密(https)，只要中國大陸政府命令交出憑證私鑰，加密只能給用戶安全假象

# 網路大砲發起四波癱瘓式攻擊



# 世界經濟論壇2015全球風險調查報告




## 10大可能風險

1. 跨境衝突(Interstate conflict)
2. 極端氣候事件(Extreme weather events )
3. 國家治理失敗(Failure of national governance)
4. 國家崩潰或危機(State collapse or crisis)
5. 失業或就業不足(Unemployment or underemployment)
6. 自然災害(Natural catastrophes)
7. 氣候變化適應失敗(Failure of climate-change adaptation)
8. 水危機(Water crises)
9. 資料欺詐或盜竊(Data fraud or theft)
10. 網路攻擊(Cyber attack)

## 10大衝擊風險

1. 水危機(Water crises)
2. 感染性疾病傳播(Spread of infectious diseases)
3. 大規模殺傷性武器(Weapon of mass destruction)
4. 跨境衝突(Interstate conflict)
5. 氣候變化適應失敗(Failure of climate-change adaptation)
6. 能源價格衝擊(Energy price shock)
7. 關鍵資訊基礎設施崩潰(CII breakdown)
8. 財政危機(Fiscal crises)
9. 失業或就業不足(Unemployment or underemployment)
10. 生物多樣性喪失和生態系統崩潰 (Biodiversity loss and ecosystem collapse)

## Top 5 Global Risks in Terms of Likelihood

| | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 | 2013 | 2014 | 2015 |
|---|---|---|---|---|---|---|---|---|---|
| 1st | Breakdown of critical information infrastructure | Asset price collapse | Asset price collapse | Asset price collapse | Storms and cyclones | Severe income disparity | Severe income disparity | Income disparity | Interstate conflict with regional consequences |
| 2nd | Chronic disease in developed countries | Middle East instability | Slowing Chinese economy (<6%) | Slowing Chinese economy (<6%) | Flooding | Chronic fiscal imbalances | Chronic fiscal imbalances | Extreme weather events | Extreme weather events |
| 3rd | Oil price shock | Failed and failing states | Chronic disease | Chronic disease | Corruption | Rising greenhouse gas emissions | Rising greenhouse gas emissions | Unemployment and underemployment | Failure of national governance |
| 4th | China economic hard landing | Oil and gas price spike | Global governance gaps | Fiscal crises | Biodiversity loss | Cyber attacks | Water supply crises | Climate change | State collapse or crisis |
| 5th | Asset price collapse | Chronic disease, developed world | Retrenchment from globalization (emerging) | Global governance gaps | Climate change | Water supply crises | Mismanagement of population ageing | Cyber attacks | High structural unemployment or underemployment |

## Top 5 Global Risks in Terms of Impact

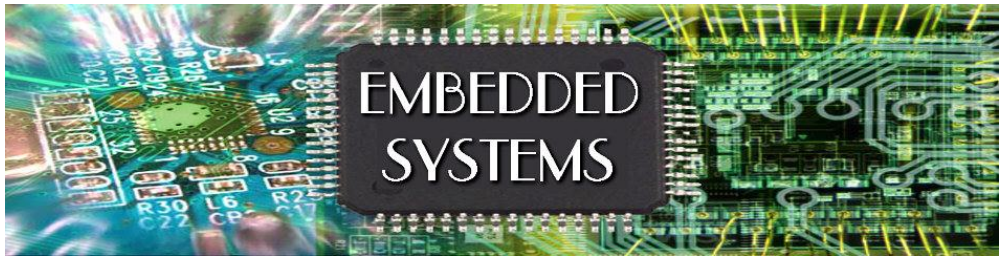
| | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 | 2013 | 2014 | 2015 |
|---|---|---|---|---|---|---|---|---|---|
| 1st | Asset price collapse | Asset price collapse | Asset price collapse | Asset price collapse | Fiscal crises | Major systemic financial failure | Major systemic financial failure | Fiscal crises | Water crises |
| 2nd | Retrenchment from globalization | Retrenchment from globalization (developed) | Retrenchment from globalization (developed) | Retrenchment from globalization (developed) | Climate change | Water supply crises | Water supply crises | Climate change | Rapid and massive spread of infectious diseases |
| 3rd | Interstate and civil wars | Slowing Chinese economy (<6%) | Oil and gas price spike | Oil price spikes | Geopolitical conflict | Food shortage crises | Chronic fiscal imbalances | Water crises | Weapons of mass destruction |
| 4th | Pandemics | Oil and gas price spike | Chronic disease | Chronic disease | Asset price collapse | Chronic fiscal imbalances | Diffusion of weapons of mass destruction | Unemployment and | Interstate conflict with regional consequences |
| 5th | Oil price shock | Pandemics | Fiscal crises | Fiscal crises | Extreme energy price volatility | Extreme volatility in energy and agriculture prices | Failure of climate change adaptation | Critical information infrastructure breakdown | Failure of climate-change adaptation |

# 簡報大綱

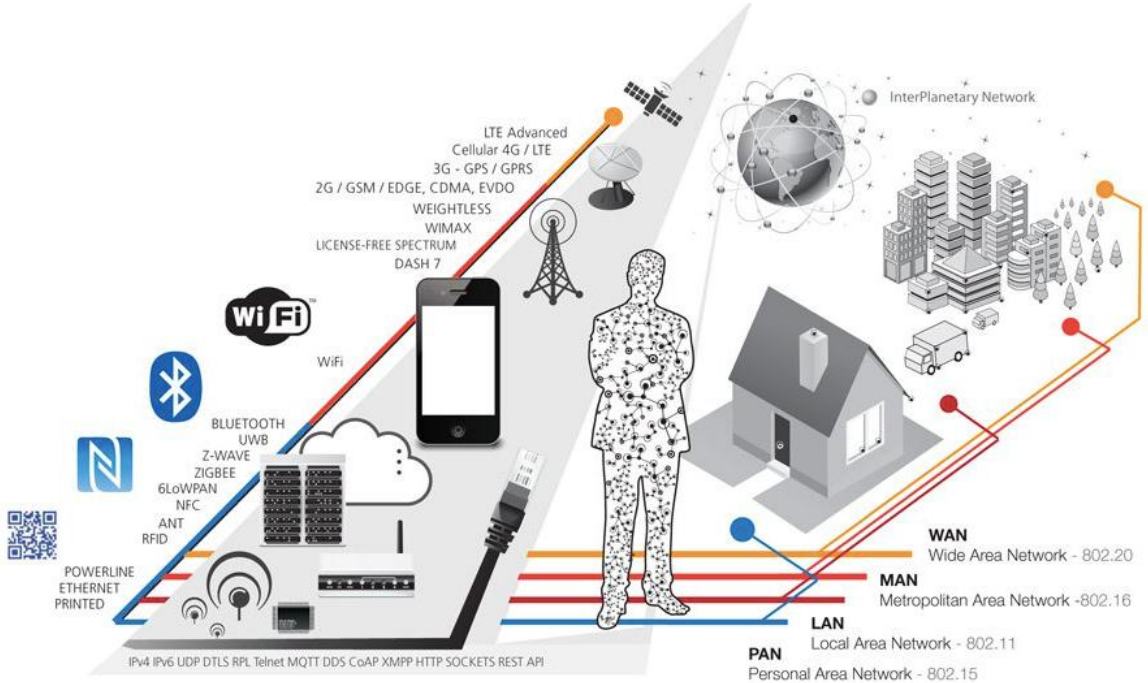
- 教育體系資訊安全防護架構
- 近期資安威脅案例
- 物聯網資安風險與思維
- 近期政府資安政策

# 物聯網的組成要素

ACTUATORS




Sensors

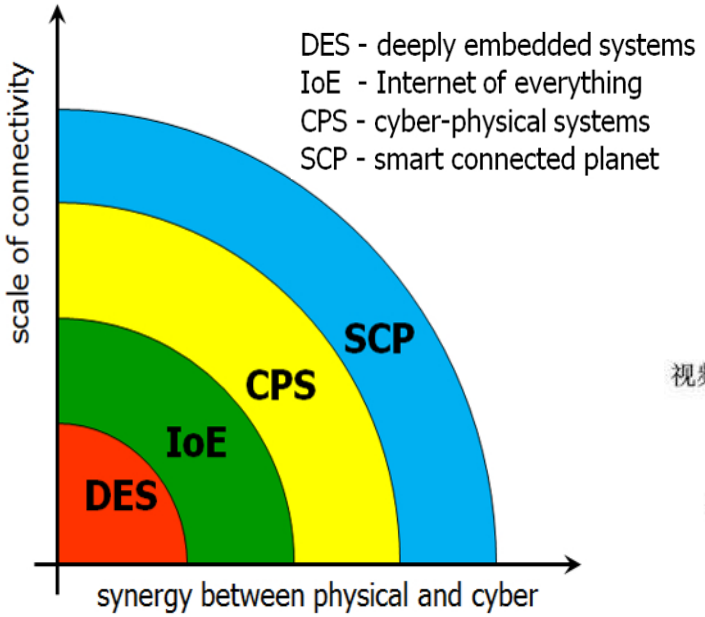


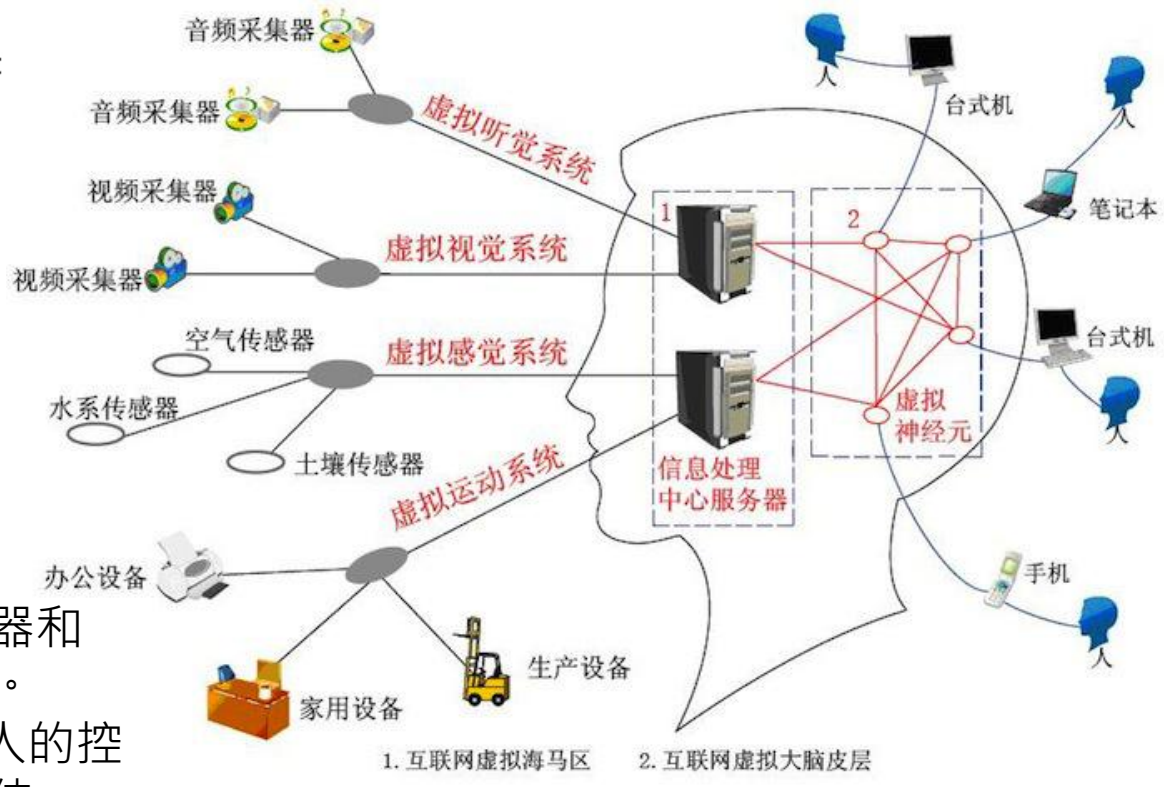


Connectivity

Process

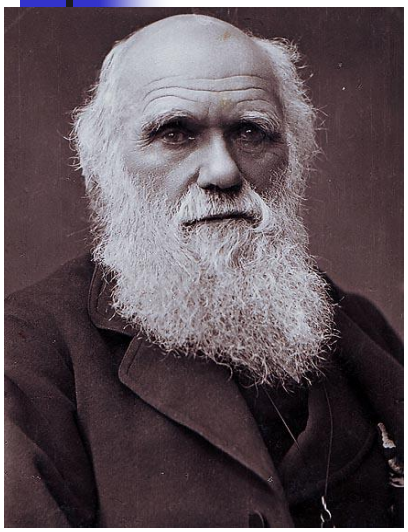
# 網宇實體系統(Cyber Physical System)

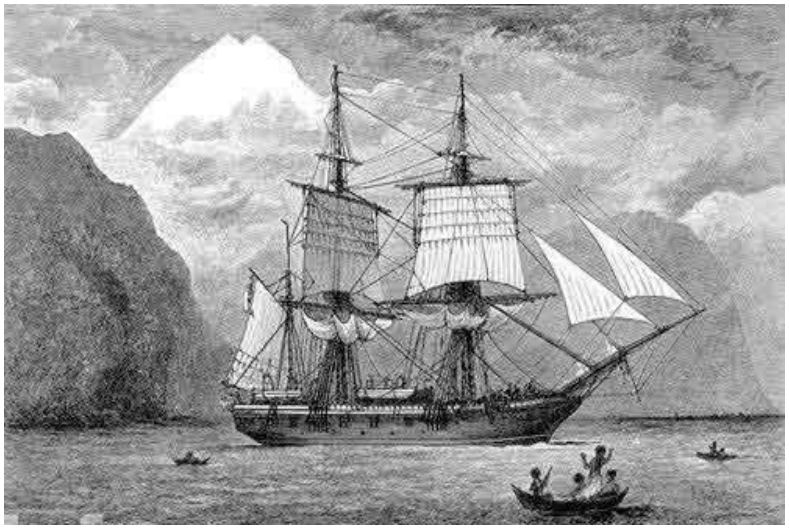


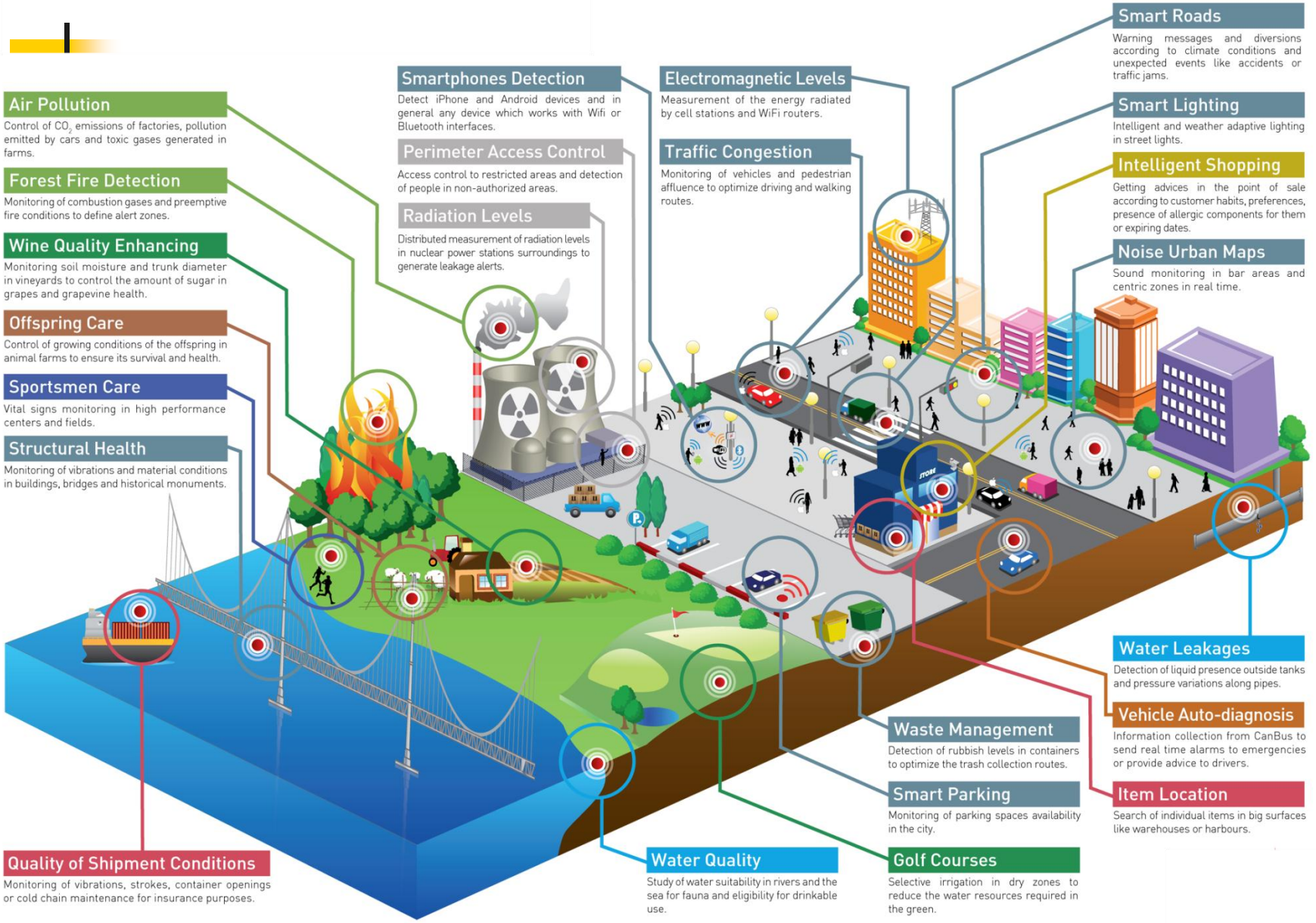

- 結合電腦運算領域以及感測器和致動器裝置的整合控制系統。
- CPS是借用技術手段，實現人的控制在時間、空間等方面的延伸
- CPS系統的本質就是人、機、物的融合計算

# 當虛擬遇上實體





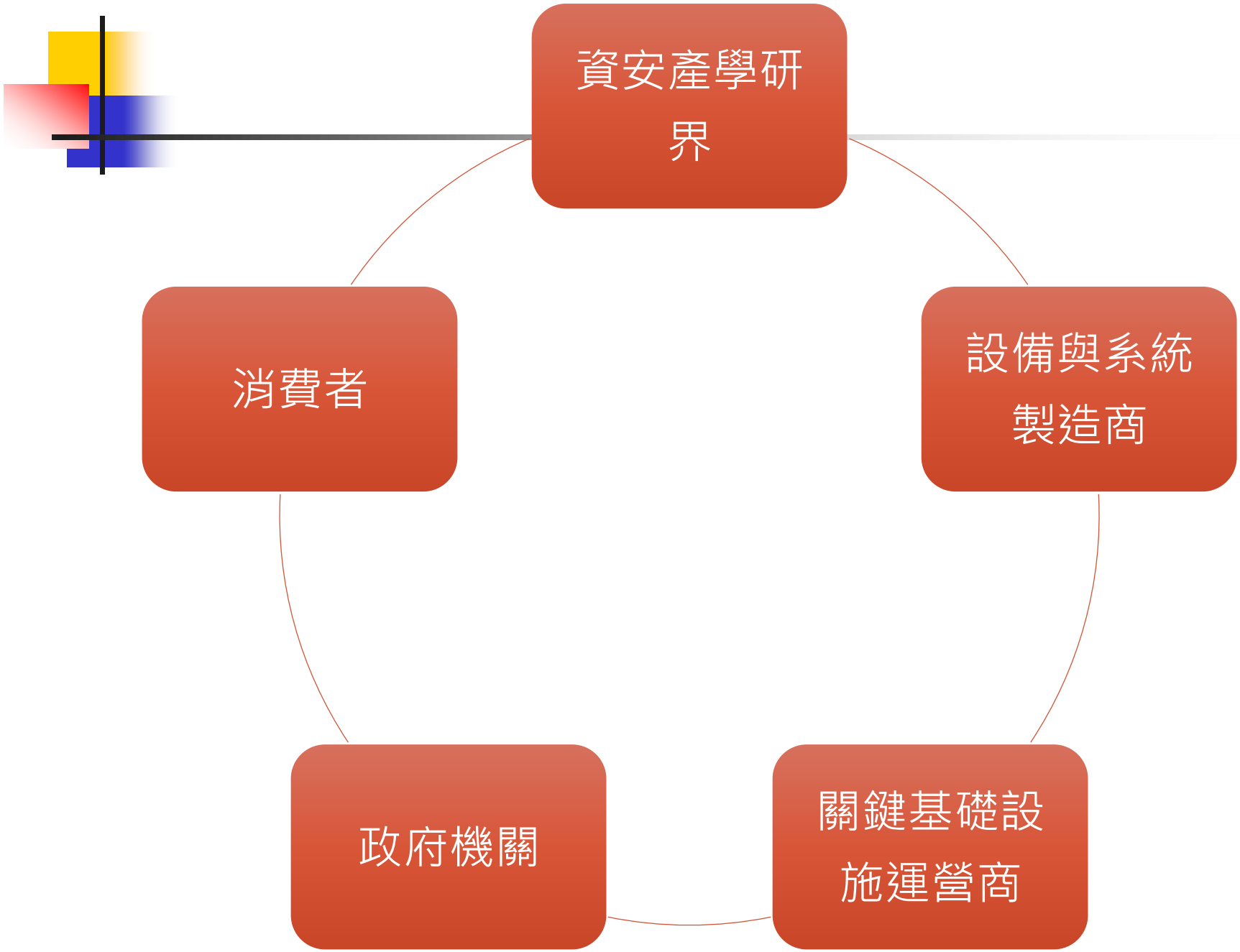
- 越來越多的外來物種被引進，導致當地生物鏈紊亂
- 紅火蟻、山羊和黑莓，都對當地的生態造成了極大傷害




實體世界的弱點 X 實體世界的威脅 X 虛擬世界的弱點 X 虛擬世界的威脅

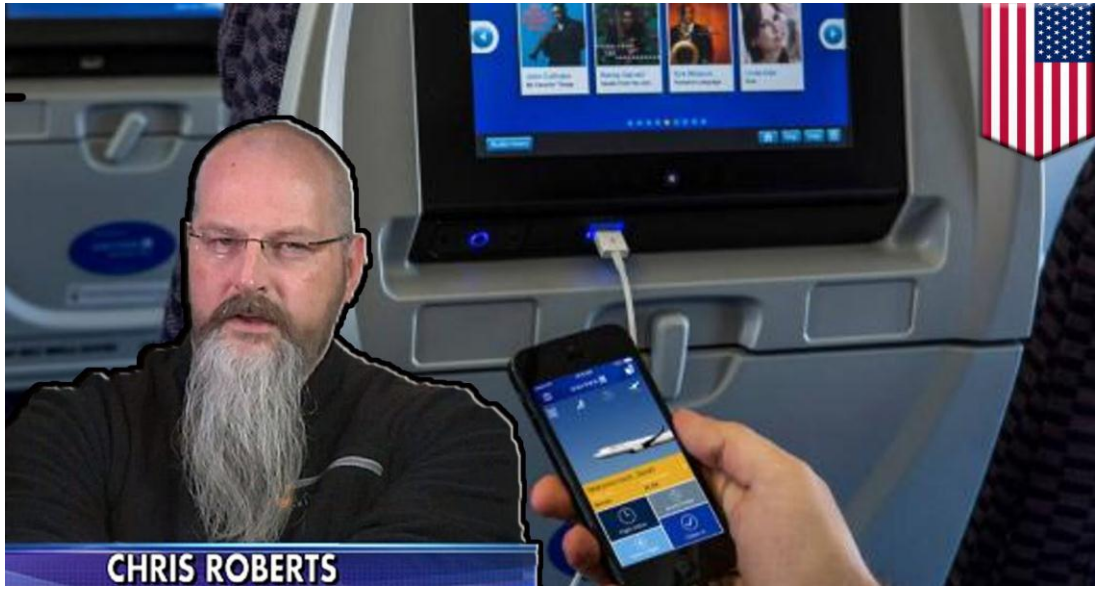
**Risks & Consequences**

圖片來源：libelium.com


資安產學研界
設備與系統製造商
關鍵基礎設施運營商
政府機關
消費者

# 資安產學研界

- Be a break and evangelist of the hype





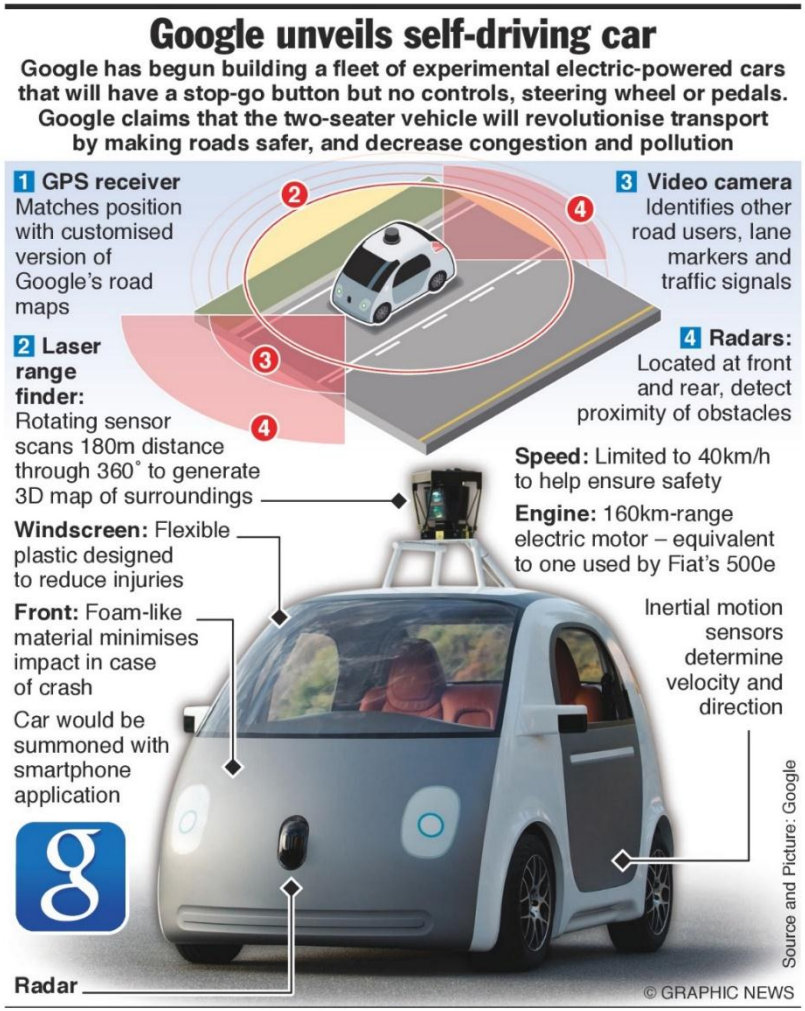

Flight Management System

# 資安產學研界

- Be a break and evangelist of the hype


# 資安產學研界

- Be a break and evangelist of the hype

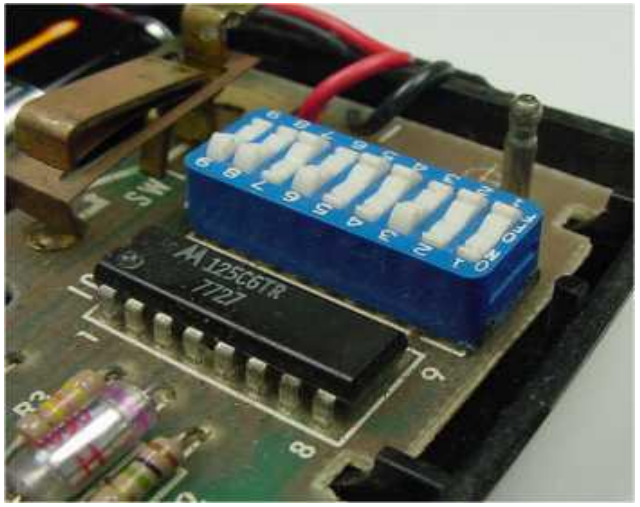



# 資安產學研界

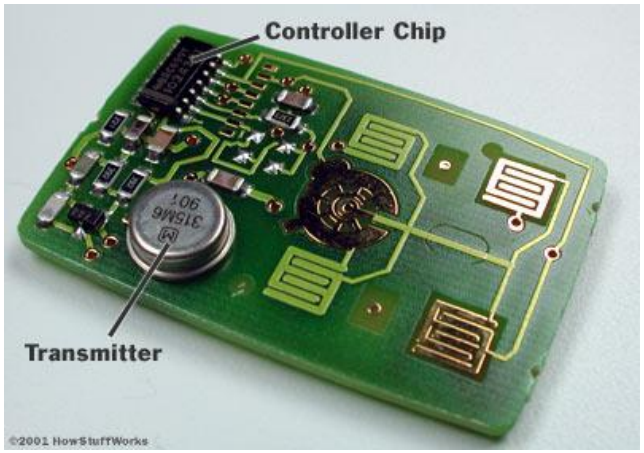
- Be an innovator

# 設備與系統製造商

- Security through obscurity will not prevail in cyber

1950 -> 1970



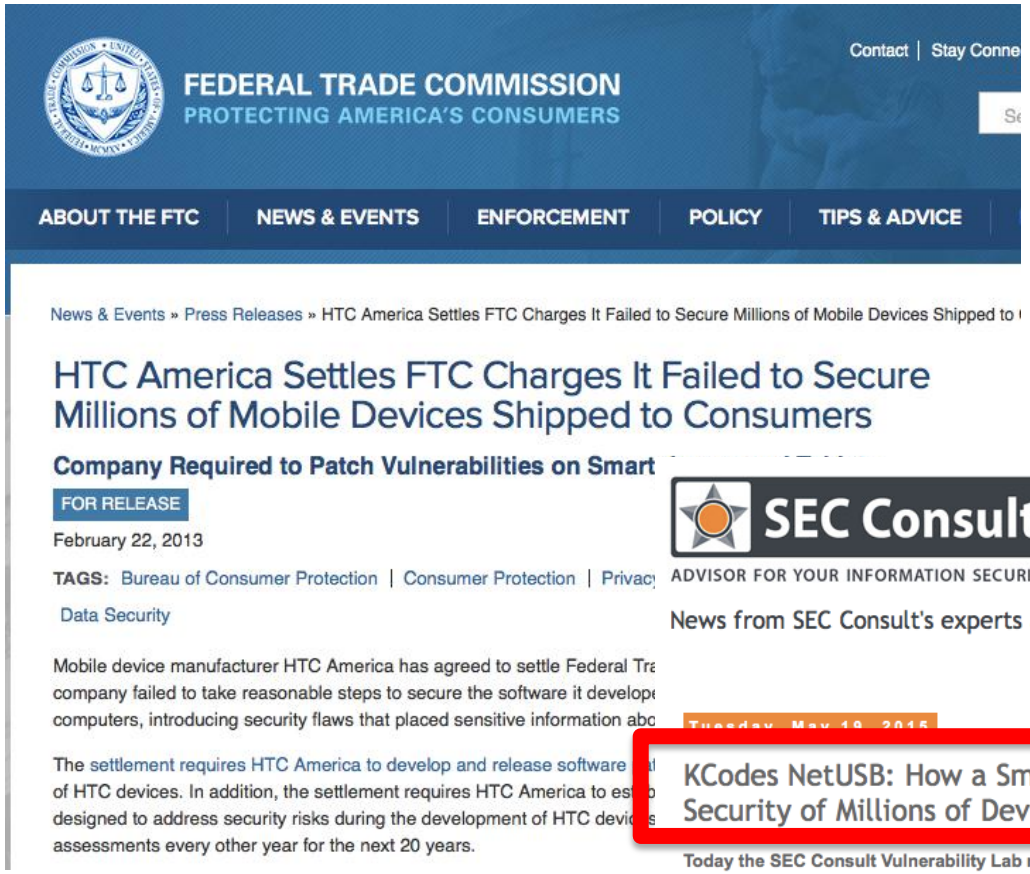

| Make | Models |
|---|---|
| Alfa Romeo | 147, 156, GT |
| Audi | A1, A2, A3, **A4 (2000)**, A6, A8, Allroad, Cabrio, Coupé, Q7, S2, S3, S4, S6, S8, **TT (2000)** |
| Buick | Regal |
| Cadillac | CTS-V, SRX |
| Chevrolet | Aveo, Kalos, Matiz, Nubira, Spark, Evanda, Tacuma |
| Citroën | **Jumper (2008)**, Relay |
| Daewoo | Kalos, Lanos, Leganza, Matiz, Nubira, Tacuma |
| DAF | CF, LF, XF |
| Ferrari | California, 612 Schaglietti |
| Fiat | Albea, Doblò, Idea, Mille, Multipla, Palio, **Punto (2002)**, Seicento, Siena, Stilo, **Ducato (2004)** |
| Holden | Barina, Frontera |
| Honda | Accord, Civic, CR-V, FR-V, HR-V, Insight, **Jazz (2002)**, Legend, Logo, S2000, Shuttle, Stream |
| Isuzu | Rodeo |
| Iveco | Eurocargo, Daily |
| Kia | Carnival, Clarus, Pride, Shuma, Sportage |
| Lancia | Lybra, Musa, Thesis, Y |
| Maserati | Quattroporte |
| Opel | Frontera |
| Pontiac | G3 |
| Porsche | 911, 968, Boxster |
| Seat | Altea, Córdoba, Ibiza, Leon, Toledo |
| Skoda | **Fabia (2011)**, Felicia, Octavia, Roomster, Super, Yeti |
| Ssangyong | Korando, Musso, Rexton |
| Tagaz | Road Partner |
| Volkswagen | Amarok, Beetle, Bora, Caddy, Crafter, Cross Golf, Dasher, Eos, Fox, Gol, **Golf (2006, 2008)**, Individual, Jetta, Multivan, New Beetle, Parati, Polo, Quantum, Rabbit, Saveiro, Santana, **Scirocco (2011)**, Touran, Tiguan, Voyage, **Passat (1998, 2005)**, Transporter |
| Volvo | C30, **S40 (2005)**, S60, S80, V50, V70, XC70, XC90, XC94 |

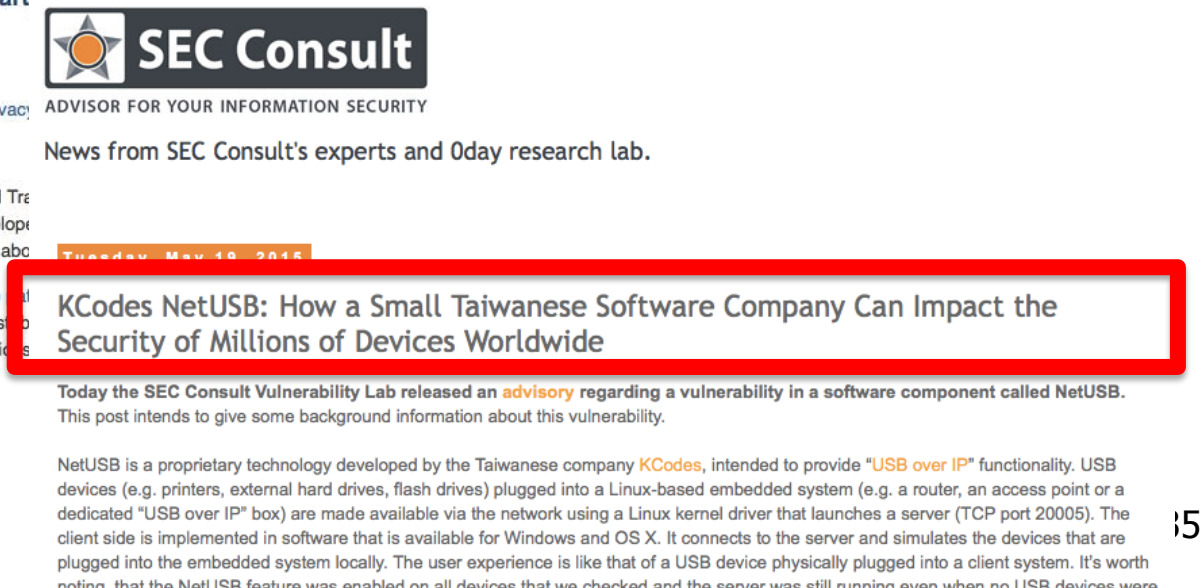
Figure 2: Vehicles that used Megamos Crypto for some version/year [39]. Boldface and year indicate specific vehicles we experimented with.

Megamos Crypto vulnerability

# 設備與系統製造商

- Realize cyber security will be a market differentiator



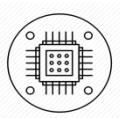
# 關鍵基礎設施運營商

- Preparedness averts peril









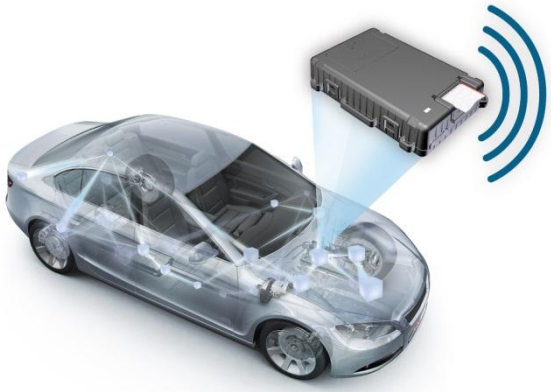



IoT devices are actively penetrating some of the **world's most regulated industries** including healthcare, energy infrastructure, government, financial services, and retail.

*The 2015 Internet of Things in the Enterprise Report by OpenDNS*

# 關鍵基礎設施運營商

- Supply Chain Security



# 政府機關

- Regulate, but don't over regulate


The Locomotive Act 1865 (Red Flag Act)

# 政府機關

- Facilitate R&D





# 消費者

- Awareness and use buying power

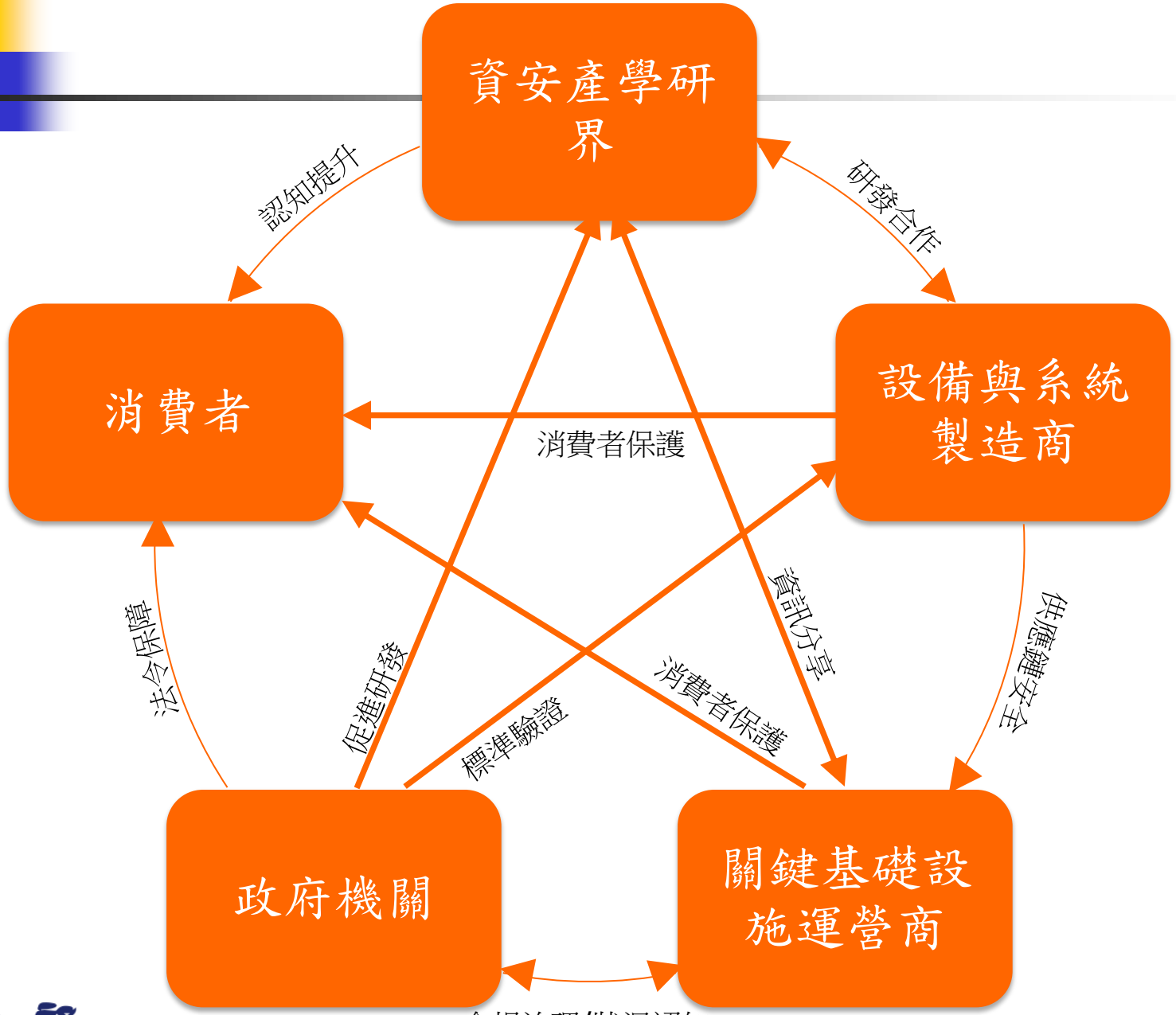
*"Researchers must encourage the automotive industry to consider seriously the security as a mandatory requirement for the safety of car owners; most important is that car owners in the next future will chose their cars also based on security features implemented by the automakers."*

The Nightmare of Car Hacking

http://resources.infosecinstitute.com/the-nightmare-of-car-hacking/

by Pierluigi Paganini

(CISO Bit4Id and Member of the ENISA Threat Landscape Stakeholder Group)


資安產學研界
認知提升
研發合作
消費者
設備與系統製造商
消費者保護
法令遵循
促進研發
標準驗證
資訊分享
消費者保護
供應鏈安全
政府機關
關鍵基礎設施運營商

合規治理/狀況認知

# 簡報大綱

- 教育體系資訊安全防護架構
- 近期資安威脅案例
- 物聯網資安風險與思維
- 近期政府資安政策

# 國家資通安全政策

## 國家安全

- 網路國家主權
- 網路戰戰略
- 網路戰部隊
- 供應鏈安全
- 國家風險管理
- 國家通訊應變計畫

## 資安管理

關鍵資訊基礎設施保護

**1.中央與地方政府**

2.能源
3.水資源
4.通訊傳播
5.交通
6.銀行與金融
7.緊急救援與醫院
8.高科技園區

## 產業發展

資安應用

- Open Data
- Smart City
- Smart Grid
- Smart Home
- Smart Car

**網路智慧新台灣白皮書、生產力4.0**

## 科技研發

- Cloud
- Big Data
- Mobile
- **IoT**
- **SCADA**
- **Cyber-Physical**
- …

## 人才養成

1.科技法律
2.資安管理
3.數位鑑識
4.資安檢測
5.軟體安全
6.系統安全
7.網路安全
8.通訊安全
9.資料科學
10.密碼模組

價值創造、永續發展

# ide@Taiwan 2020 – 網路資安隱私

為因應網路智慧新台灣之發展，進而確保民眾數位生活福祉、新興資安產業發展及數位國土國家安全，我國應打造安全的網際生態體系，建立法制化且受信任之智慧聯網空間，吸引全球頂尖資安人才與資源，達成保障「智慧生活」與「網路經濟」自由發展之願景。

**防治網路犯罪**

加強網路犯罪的防治與執法能量，以充分保障企業與消費者的福祉與權益

**資安隱私保護**

資訊安全與隱私保護是一個國家在數位時代發展的最重要基石

**資安法規遵循**

定義可供遵循的資安標準，輔以資安法令與法規，確保標準在任何狀況下都能夠被遵守

**數位國土安全**

打造台灣成為「亞太網路中心」，推動成為全球物聯網創新聚落

**發展願景**

**目標一**

提升資安治理與法規遵循強度，使資訊安全成為企業社會責任的一環

**目標二**

強化網路犯罪預防、偵查及起訴能量，充分保障企業與消費者之權益

**目標三**

促進資安供需平衡，創造產業發展契機，使資安產業具備國際競爭能力

**目標四**

落實數位智慧國土安全，達成關鍵資訊基礎設施防護之國家安全戰略目標

科技部 Ministry of Science and Technology

# ide@Taiwan 2020 – 網路資安隱私策略

## 推動策略具體作法

- 規劃適合我國之資安治理架構
- 建構適用於我國之資安治理成熟度評估機制
- 積極研議我國資安作用法並推動立法

**短期策略**

**健全資安法令標準**


**擴大公私協同合作**

- 處理來自企業與民間各領域之資安事件通報與諮詢
- 研議企業與民間情資交換安全標準
- 與國內外各領域CERT建立資訊共享系統或平台

**強化網路犯罪執法**

- 健全資安及網路犯罪通報
- 擴大偵查組織架構與人才進用
- 加強兩岸及跨國共同打擊犯罪
- 加強數位證據保全與程序
- 加強網路犯罪宣導面向
- 每年定期參與相關國際會議

**落實人才訓用合一**

研議由課程、平臺、競賽、實習及產學合作等五大主軸擴大資安人才培育，落實訓用合一

**推升智慧商務安全**

- 盤點資安自主技術，發展優先項目
- 發展虛實整合的關鍵防護安全技術
- 軟體工程加入資安與隱私保護的設計
- 提出最佳商務安全實務與解決方案
- 發展民眾有感智慧商務App

# ide@Taiwan 2020 – 網路資安隱私策略

## 中長期策略

- 訂定合理資訊(安)人力及預算配比
- 研議成立資安專戶或基金
- 篩選資安產業潛在價值與利基之產品適度扶植

**改善政府資源配置**

**建置前瞻實驗場域**

- 結合產、學、研資源建置前瞻實驗場域
- 研究關鍵資訊基礎設施存在之弱點、模擬外來之攻擊威脅及測試驗證創新之資安防護技術實驗場所

**接軌國際實務標準**

- 發展讓消費者放心與安心之產品技術、及服務標準
- 研議資服產業安全分級機制
- 鼓勵國內學研與廠商加入國際產業標準協會

# 資通安全管理法草案

- 以建構安全資通環境，邁向優質網路社會為願景

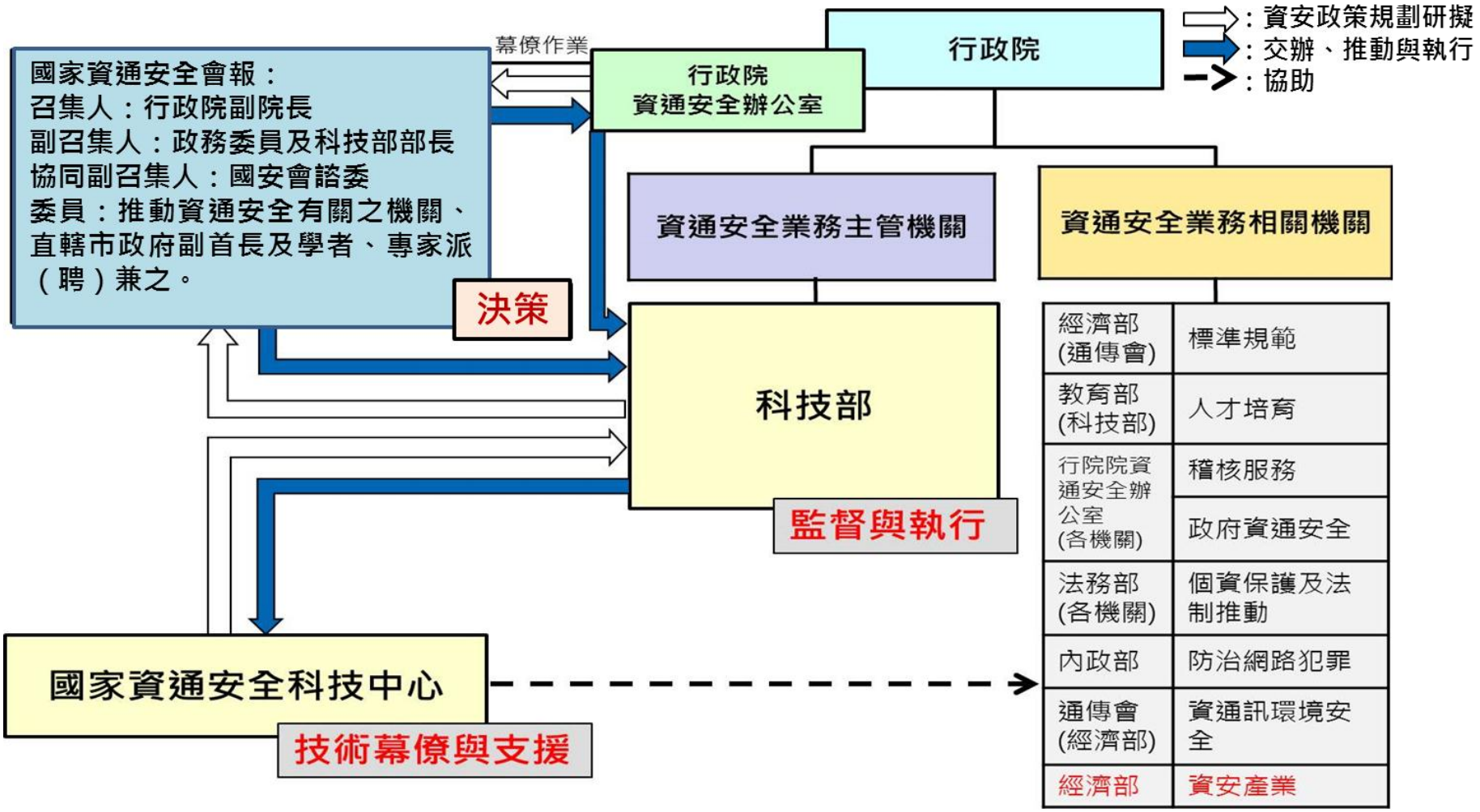
# 資通安全管理法草案架構

- 以資通安全保護為核心，計6章，33條

資通安全管理法草案

| | |
|---|---|
| 第1章 總則(§1~§6) | 立法目的、名詞定義、主管機關及中央目的事業主管機關權責分工、委外、基金設置 |
| 第2章 資通安全推動組織(§7~§9) | 國家資通安全會報及其幕僚之設立、任務與組成；科技部與國家資通安全科技中心之任務 |
| 第3章 公務機關資通安全管理(§10~§15) | 資安責任等級分級、資通安全管理與維護責任、資通安全長之設置、資通安全維護計畫之制定與實施、資通安全查核、年度資通安全報告之提出、資通安全事件預防通報及應變、獎懲制度 |
| 第4章 非公務機關資通安全管理(§16~§21) | 非公務機關、受指定非公務機關之產品或服務及關鍵基礎設施提供者資通安全維護業務之指導、監督與管理、資通安全維護計畫之制定與實施、行政檢查、行政救濟 |
| 第5章 罰則(§22~§28) | 行政處分 |
| 第6章 附則(§29~§33) | 資通安全情資分享、人力與預算編列、資通安全產業之推動、施行細則授權、施行日期 |

# 資通安全推動組織(§4、§7~ §9)



# 保護客體與適用主體(§2~§4、§16、§17)

**保護客體**

資通安全：指防止資通系統及透過其運作之資訊免於遭受未經授權之存取、使用、控制、洩漏、破壞、修改、銷毀或其他作為，以確保其機密性、完整性及可用性。

**適用主體**

**公務機關**

① 指依法行使公權力之中央或地方機關或行政法人

② 依資安責任等級分級(現行分為三級，分別是A級、B級、C級)

**由科技部管理**

**非公務機關**

① 指本法所稱之公務機關以外的法人或團體

② 區分為三類：未經指定之非公務機關、經指定非公務機關之產品或服務、關鍵基礎設施提供者

**由中央目的事業主管機關管理**

# 公務機關資通安全管理(§9~§14、§30)

擬定資通安全責任等級
報請行政院核定

國家資通安全會報

資通安全稽核

科技部(幕僚：國家資通安全科技中心)

資通安全事件通報

公務機關
-設置資通安全長

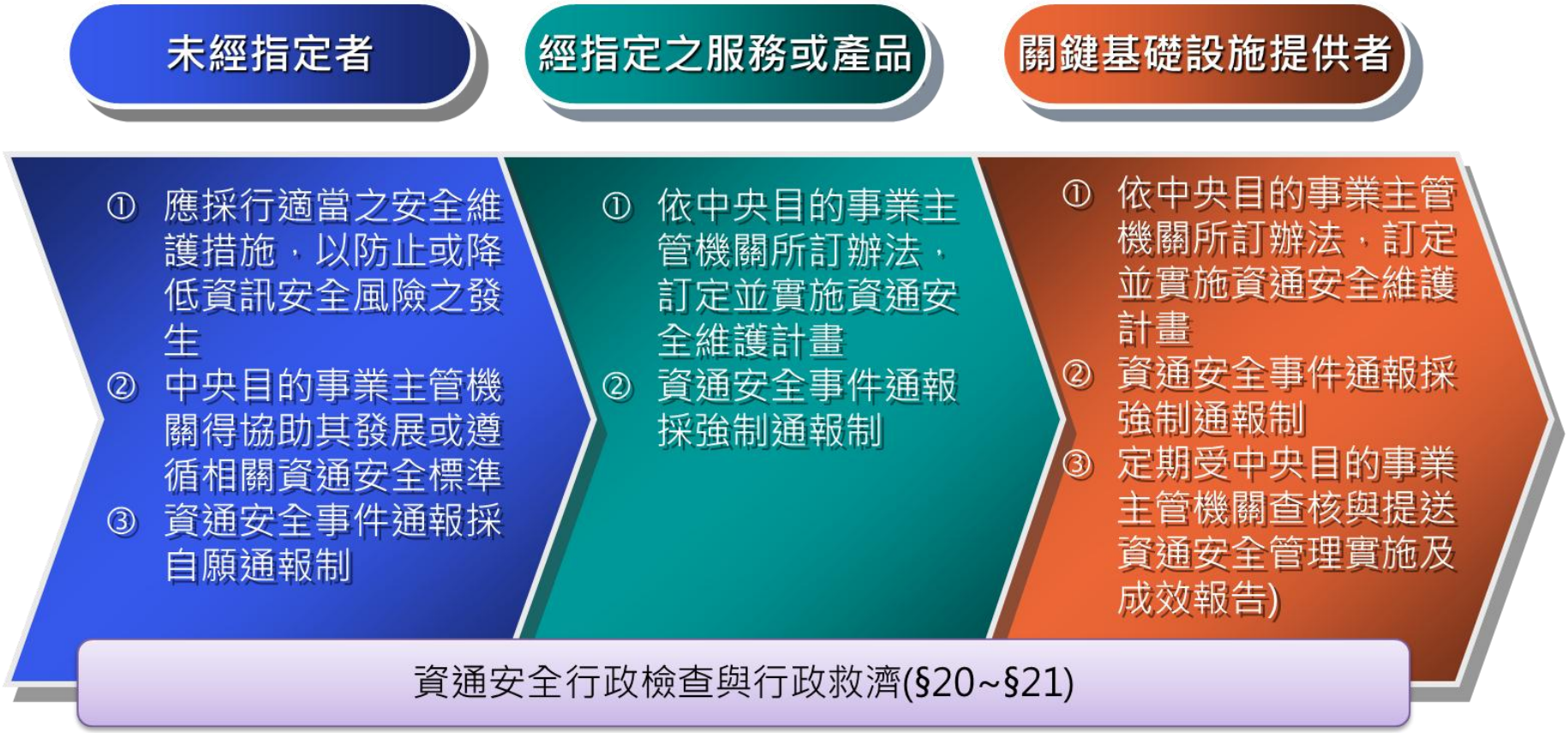
整體公務機關資通安全維護計畫實施情形及所管產業資安維護之指導


依資安責任等級制定與實施資訊安全維護計畫

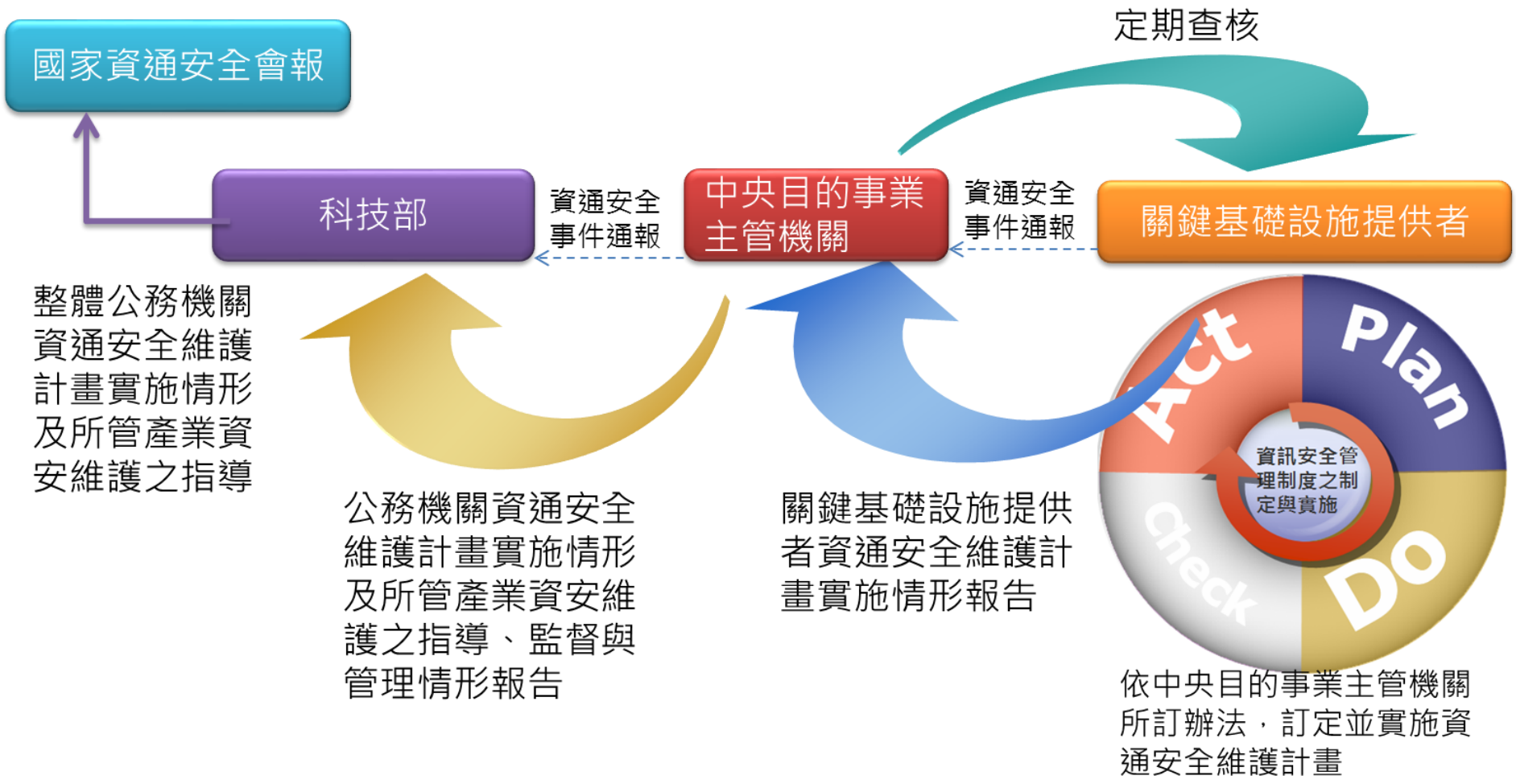
① 資通安全查核缺失矯正預防計畫
② 資通安全事件矯正預防計畫
③ 公務機關資通安全維護計畫實施情形及所管產業資安維護之指導、監督與管理情形報告

**政府應依法編列人力與經費，確保有效推動資通安全政策相關事項**

# 非公務機關資通安全管理(§16~§19)



# 關鍵基礎設施提供者管理(§17~§19)



# 資通安全事件通報暨情資分享機制 (§14、§19、§29)

情資分享

資通安全事件通報機制

公務機關資通情資分享平台
(科技部建置與維護§29)

主管機關 科技部

中央目的事業主管機關 經濟部、金管會、交通部、NCC...等

公務機關資通安全事件通報(§14)(強制通報)

公務機關

非公務機關資通安全事件通報(§19)(強制通報)

關鍵基礎設施提供者 + 經指定非公務機關之產品或服務

非公務機關資通安全事件通報(自願通報)

未指定之非公務機關

涉有刑責之情形，應保存資料，主動通報司法單位

# 發展資通安全產業，以提升資通安全(§31)

提供充份資源 + 整合民間力量

1. 資通安全專業人才之培育
2. 資通安全科技之研發、整合、應用、產學合作及國際交流合作之推動
3. 資通安全標準及其認驗證機制之發展及推動
4. 資通安全產業之發展及推動

科技部 Ministry of Science and Technology

# 結論

- 雲端運算、物聯網與大數據時代來臨的趨勢已然確立，而資訊安全對政府、關鍵基礎設施及資通訊產業均是無法迴避的重要議題
- 我國政府透過行政院資安會報長期推動政府體系之資訊安全，未來將配合生產力4.0與網路智慧新台灣的政策發展，強化資安產業發展與人才培育
- 我國政府正草擬資安管理法，預期未來通過後成為政府資安推動組織、政策草擬及推動落實關鍵資訊基礎設施資安管理之重要依據