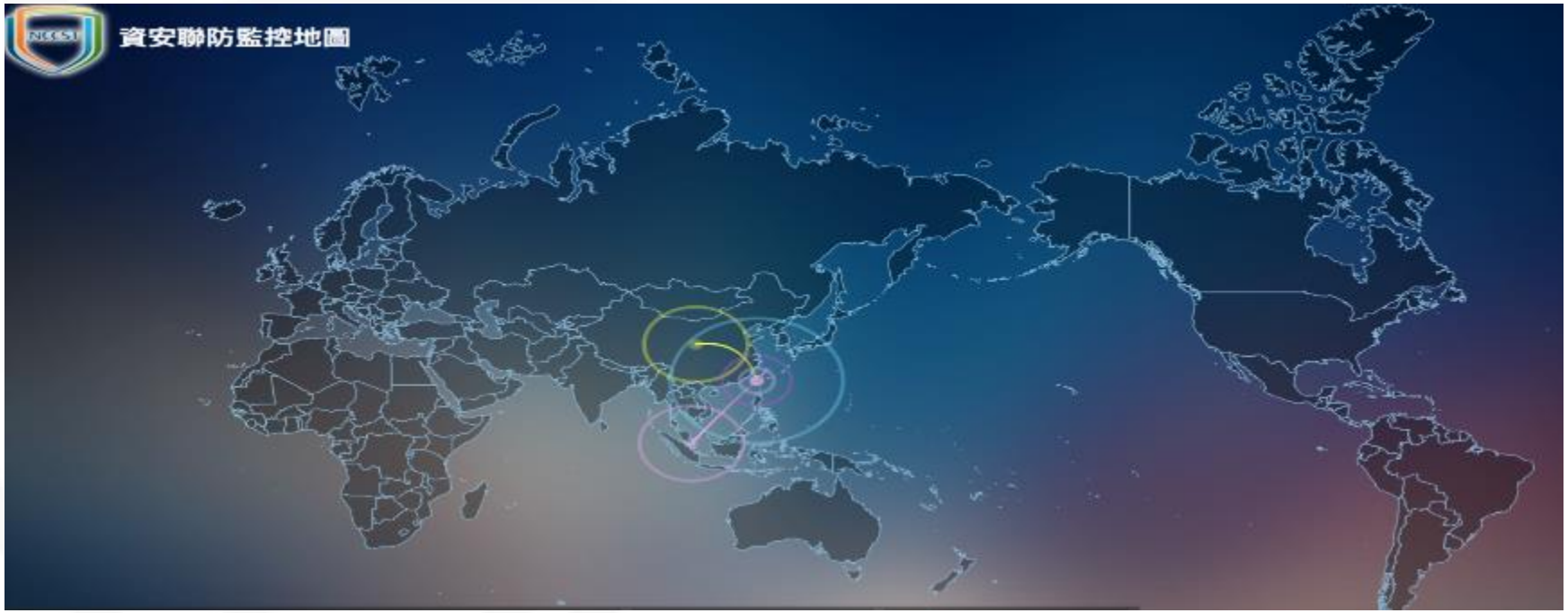
資安威脅趨勢及防護策略

行政院國家資通安全會報技術服務中心
吳啟文主任
110年3月9日

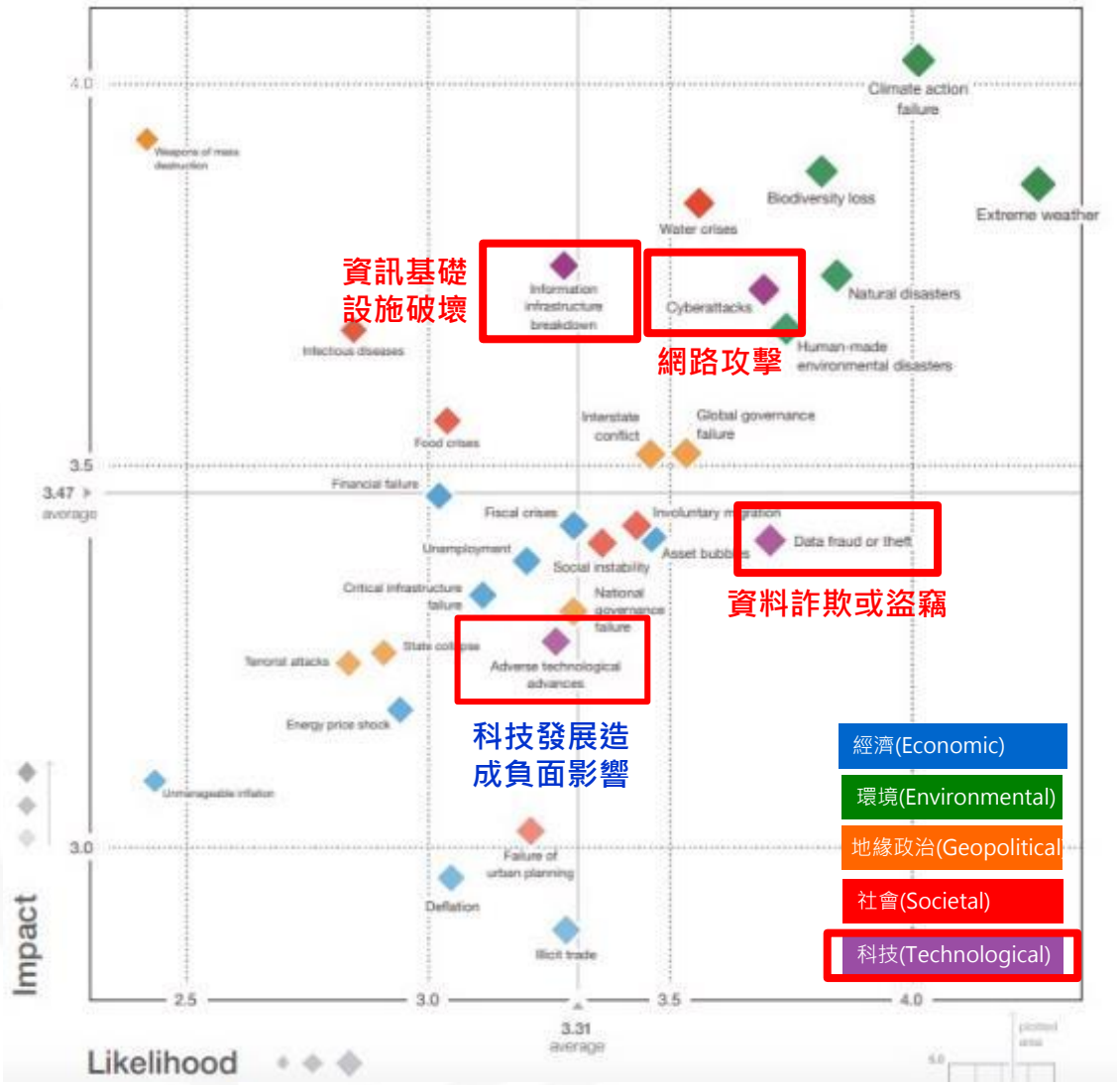
大綱

- 資安威脅趨勢
  - 國際資安威脅趨勢
  - 政府資安威脅情勢
- 資安防護策略
  - 資通安全發展方案
  - 資安防護精進作為

國際資安威脅趨勢



世界經濟論壇2020年全球風險地圖



10大影響風險

1. 緩解氣候變化與適應失敗
2. 大規模殺傷性武器
3. 生物多樣性喪失
4. 極端氣候
5. 水資源危機
6. **資訊基礎設施破壞(2019年排名第8)**
7. 重大自然災害
8. **網路攻擊(2019年排名第7)**
9. 人為環境災害
10. **傳染病傳播**

10大可能風險

1. 極端氣候
2. 緩解氣候變化與適應失敗
3. 重大自然災害
4. 生物多樣性喪失
5. 人為環境災害
6. **資料詐欺或竊盜(2019年排名第4)**
7. **網路攻擊(2019年排名第5)**
8. 水資源危機
9. 全球治理失敗
10. 資產泡沫化

資料來源：The Global Risks Report 2020 15th Edition, World Economic Forum

世界經濟論壇2021年全球風險地圖

10大影響風險

1. 傳染病(2020年排名第10)
2. 緩解氣侯變化行動失敗
3. 大規模殺傷性武器
4. 生物多樣式喪失
5. 自然資源危機
6. 人為環境災害
7. 民生危機
8. 極端氣侯
9. 債務危機
10. *資訊基礎建設破壞*(2020年排名第6)

10大可能風險

1. 極端氣侯
2. 緩解氣侯變化行動失敗
3. 人為導致的環境災害
4. 傳染病
5. 生物多樣式喪失
6. **集權控制數位資源**
7. **數位落差**
8. 國際關係裂痕
9. ***資安防護失效***
10. 民生危機

資料來源：The Global Risks Report 2021 16th Edition, World Economic Forum

國際資安威脅趨勢

針對性威脅攻擊
竊取機密資料

連網設備管控不佳
網路攻擊風險上升

物聯網與行動式設備
資安弱點威脅升高

關鍵資訊基礎設施
資安風險倍增

網路與經濟罪犯影響
電子商務與金融運作

資安(訊)供應商持續遭駭
破壞供應鏈安全

全球資安威脅案例

疫情讓資安風險大增 社交工程事件頻傳

2020/8/31趨勢科技統計，半年攔截880萬次COVID-19攻擊

趨勢科技2020年上半年資安總評報告顯示，6個月內即攔截880萬次新冠肺炎相關威脅，其中近92%是經由垃圾郵件散布

APT攻擊串聯網通設備漏洞發動攻擊

2020/9/14美國國土安全部公告，中國利用各大網路設備已知漏洞，對美國政府單位發動攻擊

美國國土安全部發現，中國APT駭客組織利用Citrix、微軟Exchange Server、F5及Pulse VPN等多項產品漏洞，攻擊美國政府單位

物聯網設備資安弱點威脅升高

2020/6/10 IoT裝置驚爆漏洞，恐引發資料外洩與DDoS攻擊

通用隨插即用協定用來發現其他裝置並與之互動之物聯網設備及區域網路裝置，存在CallStranger安全漏洞，可藉此漏洞竊取資料、發動分散式阻斷服務攻擊

勒索軟體轉向目標式攻擊，資安威脅遽增

2020/10/27全球受勒索軟體攻擊次數近3個月暴增5成

資安業者Check Point研究指出，相較於2020上半年，過去3個月受勒索軟體攻擊的每日平均次數增加50%，7月底Garmin傳出疑似遇害而導致服務與網站一度中斷，5月初中油、台塑、力成先後遭駭客鎖定攻擊

資料外洩，個資、商業機密全都露

2020/11 Prestige Software雲端配置錯誤，造成Booking.com、Expedia與Agoda等客戶的房客資料外洩

提供架站服務的Website Planet近日揭露，Prestige Software雲端配置錯誤造成多家住房網房客資料外洩，約10萬名房客的信用卡資訊，受害者遍及全球

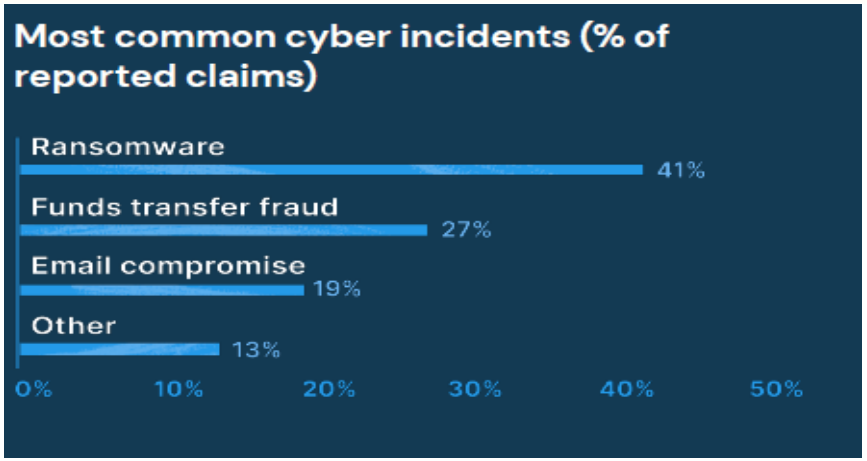
供應鏈攻擊鎖定GitHub開源軟體專案

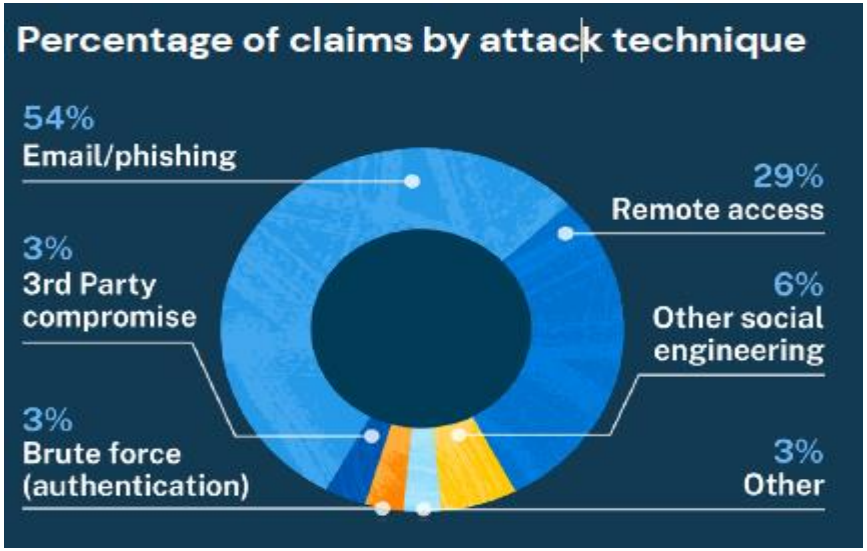
2020/5/29駭客將惡意程式注入開源專案中，透過GitHub平台上散布後門程式

GitHub發現名為Octopus Scanner惡意軟體，可進行主機遠端操控，GitHub團隊調查後發現，已有26個開源專案遭攻擊者借殼上架後門程式

資安威脅趨勢統計(1/2)

- 資安事件分類
  - 勒索軟體攻擊(41%)
  - 資金移轉詐騙(27%)
  - 電子郵件入侵(19%)
- 攻擊技術
  - 郵件釣魚(54%)
  - 遠端存取(29%)
  - 除郵件外社交工程(6%)
  - 第三方工具(3%)
  - 暴力破解(3%)

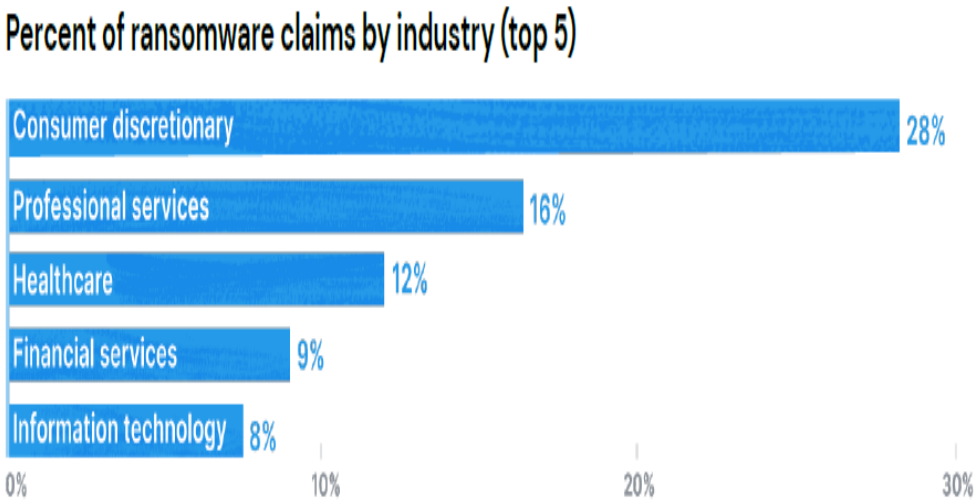




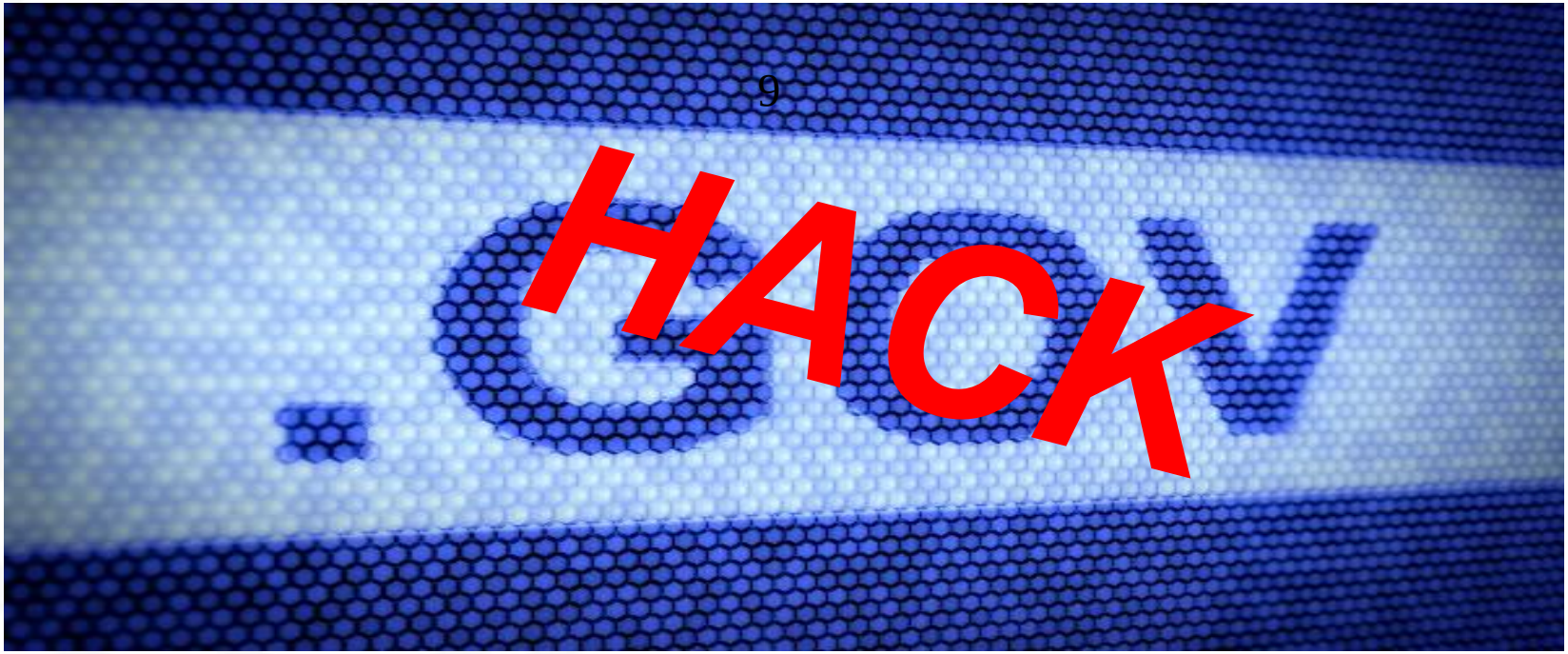
資料來源：2020網路與資訊安全保險業者Coalition上半年索賠報告

資安威脅趨勢統計(2/2)

- 被攻擊產業類別
  - 消費者領域(28%)
  - 專業服務(16%)
  - 健康照護(12%)
  - 金融服務(9%)
  - 資訊科技(8%)

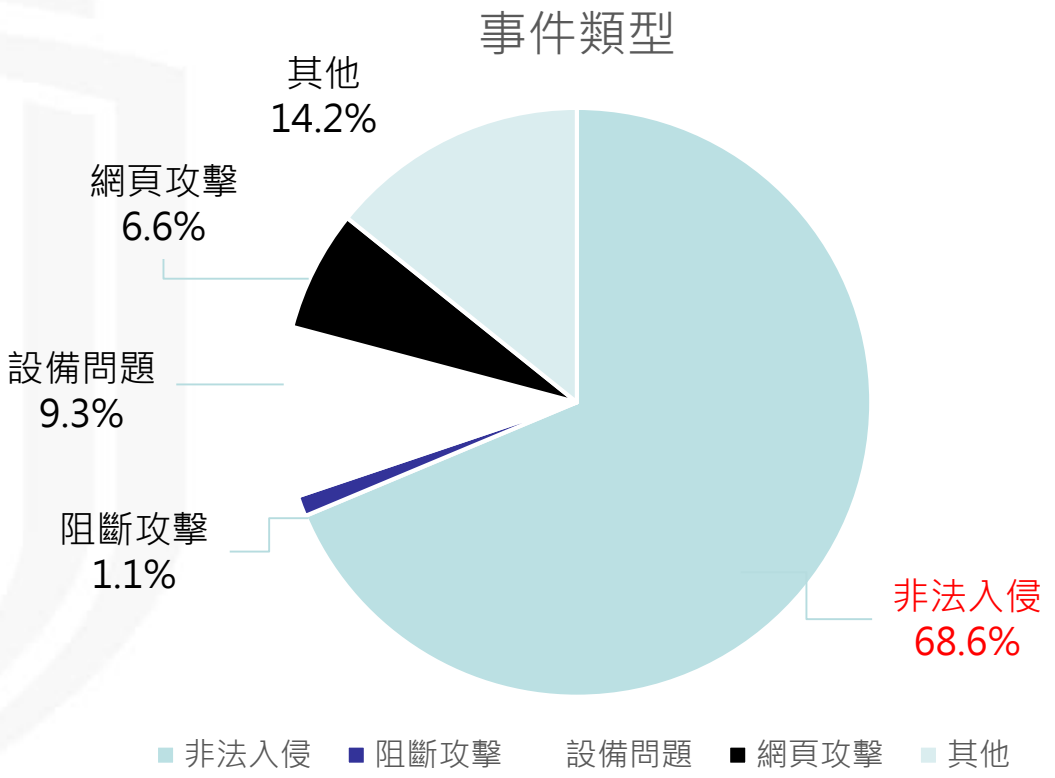


政府資安威脅情勢



政府機關資安事件通報統計

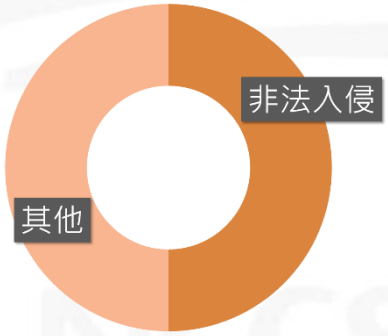
- 109年共接獲政府機關527件資安事件通報
- 通報事件等級
  - 4級資安事件：0
  - 3級資安事件：9
  - 2級資安事件：65
  - 1級資安事件：453



政府機關重大資安事件通報統計

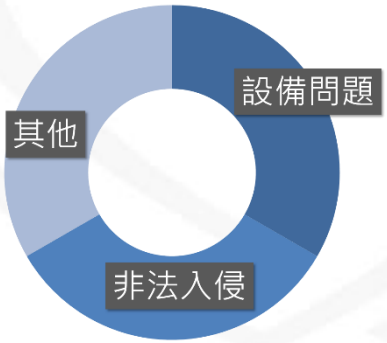
- 109年共接獲9件重大資安事件通報，6件為資料外洩，3件為核心業務中斷

資料外洩發生原因



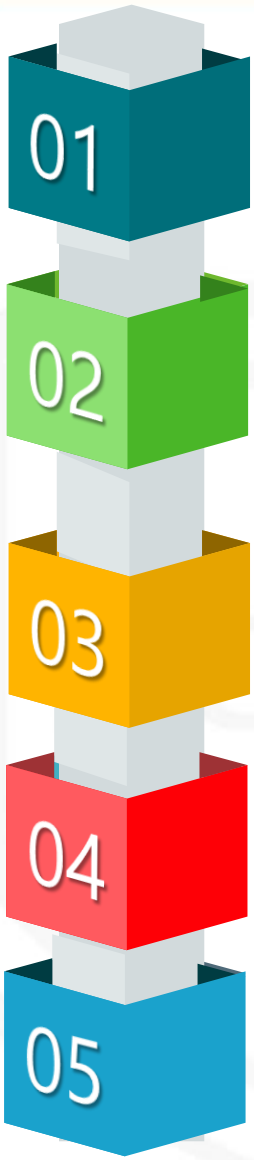
- 網站設計不當，導致網站具漏洞可存取敏感資料
- 供民眾登記資料的表單權限設定錯誤，導致可被公開檢索與編輯
- 機關內部人員疏失，將含有敏感資料檔案夾帶於信件中寄出
- 系統變更未經機關確認，系統錯誤執行並帶出疑似敏感資訊

核心業務中斷發生原因



- 機關遭非法入侵植入勒索軟體，因無法啟用備援機制，影響核心業務運作
- 設備故障，影響涉及關鍵基礎設施維運之核心資通系統運作

近期政府機關資安威脅情勢



社交工程搭配時事議題做為攻擊主軸

攻擊啟動從釣魚郵件開始，駭客以近期受關注程度高的政經議題為由施行攻擊，例如肺炎疫情、總統520就職等，鎖定特定相關機關進行攻擊

APT類型攻擊轉而利用商用工具軟體與服務

駭客利用網路上現成的工具程式或商用軟體進行入侵攻擊，並滲透與掌控AD系統，利用政府導入政府共通組態基準(GCB)以合法的服務，透過GPO派送惡意程式進行橫向擴散

供應鏈攻擊活動加劇

入侵系統委外廠商後，以其做為跳板，滲透客戶組織
駭客藉由入侵特定軟/韌體開發公司或人員電腦，進行竄改程式或下載連結等行為，造成大範圍的感染與擴散

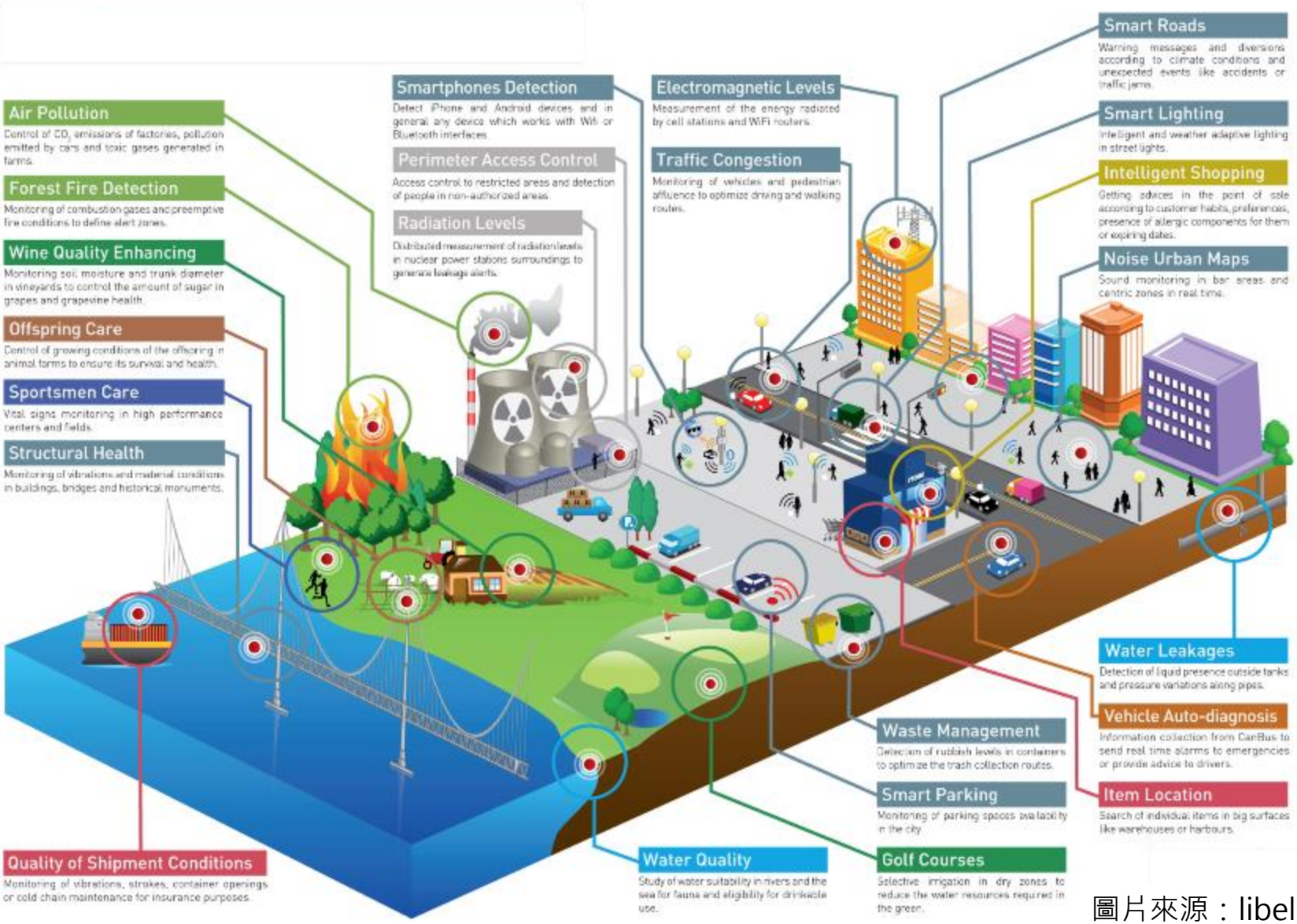
物聯網攻擊鎖定監視與網通設備

鎖定機關監視器與網通設備做為攻擊標的，以弱密碼/預設密碼配合已知弱點攻擊程式進行探測並入侵控制

勒索軟體攻擊風險激增

由亂槍打鳥轉向特定目標，遭鎖定對象包含委外廠商、機關人員、公文系統資料庫主機、對外服務網站、環控系統、檔案分享系統等，藉以癱瘓系統運作，中斷服務提供

萬物聯網時代來臨



行動化(M)

雲端化(C)

IOT(I)

+

AI(A)

大數據(B)

+

5G

圖片來源：libelium.com

大綱

- 資安威脅趨勢
  - 國際資安威脅趨勢
  - 政府資安威脅情勢
- 資安防護策略
  - 資通安全發展方案
  - 資安防護精進作為

資通安全發展方案

我國資通安全推動歷程

我國資安發展階段

第一期機制計畫

建構資安防護體系，完成政府機關分級機制

- 界定分級標準
- 推動實施資訊安全管理制度
- 資安認知推廣

90 - 93

第二期機制計畫

健全資安防護能力，成立國家資安監控中心

- 重新界定分級標準，實施範圍擴及教育體系
- 建置國家資通安全防護管理平台，提供一般監控與預警服務
- 推動資訊安全長制度

94 - 97

第三期發展方案

強化資安整體應變能力，精進通報應變機制

- 加強實施各項資安作業，共規劃30個行動方案
- 提高資安法規完備度 ex.個人資料保護法

98 - 101

第四期發展方案

加強資安防護管理二線監控機制與資安情報分享

- 完成二線資安監控服務的SOC平臺
- 修訂「政府機關(構)資通安全責任等級分級作業規定」

102 - 105

第五期發展方案

打造安全可信賴的數位國家

- 建構國家資安聯防體系
- 提升整體資安防護機制
- 強化資安自主產業發展

106 - 109

第五期國家資通安全發展方案(106-109年)

願景

打造安全可信賴的數位國家

目標

建構國家資安聯防體系
提升整體資安防護機制
強化資安自主產業發展

推動策略

完備資安基礎環境	建構國家資安聯防體系	推升資安產業自主能量	孕育優質資安人才

具體措施

1. 完備我國資安相關法規及標準 2. 強化基礎通訊網路韌性及安全 3. 建立政府資安治理模式	4. 強化關鍵資訊基礎設施資安防護 5. 建立跨域資安聯防機制 6. 精進網路犯罪防制能量	7. 發展新興資安產業 8. 輔導資安產業升級 9. 鏈結產學研能量發展新興資安技術	10. 增加產業資安人才供給 11. 提升政府資安人力專業職能

第六期國家資通安全發展方案(110-113年)

願景

打造堅韌安全之智慧國家

目標

- 成為亞太資安研訓樞紐
- 建構主動防禦基礎網路
- 公私協力共創網安環境

推動策略

吸納全球高階人才培植自主創研能量	推動公私協同治理提升關鍵設施韌性	善用智慧前瞻科技主動抵禦潛在威脅	提升民間防護能量維護公眾隱私安全

具體措施

1.擴增高教資安師資員額與教學資源 2.挹注資源投入高等資安科研 3.培育頂尖資安實戰及跨域人才	1.建立各領域公私協同治理運作機制 2.增強人員資安意識與能力建構 3.公私合作深化平時情資交流與應變演練	1.賡續推動政府資訊(安)集中共享 2.擴大國際參與及深化跨國情資分享 3.制敵機先阻絕攻擊於邊境 4.提升科技偵查能量防制新型網路犯罪	1.輔導企業強化數位轉型之資安防護能量 2.強化供應鏈安全管理 3.建構公共物聯網安全環境

策略一推動架構

成為亞太高階資安人才及技術創新基地

- 擴增高教資安教學資源
  - 擴增資安師資員額
  - 大學區網中心場域
  - 政府開放場域
- 設立資安卓越中心
  - 關鍵核心前瞻研究
  - 深耕學術資安研究
  - 跨國交流合作研究
- 培育資安實戰跨域人才
  - 培育在學資安人才
  - 培訓在職資安人才
  - 研訓頂尖實戰人才

策略一：吸納全球高階人才 培植自主創研能量

1. 擴增高教資安師資員額與教學資源
   ① 專案增加師資員額
   ② 開放學術區域網路中心、政府網路等場域供實習、實戰用
2. 挹注資源投入高等資安科研
   ① 發展國家任務導向型及關鍵(核心)資安型前瞻研究
   ② 深耕學術型資安研究
   ③ 跨國人才交流與研究合作
3. 培育頂尖資安實戰及跨域人才
   ① 培育在學、在職及政府資安人才
   ② 培育實戰型之頂尖資安人才

策略二推動架構

行政院資通安全處

1. 賡續推動資通安全管理法
2. 建立模擬場域，作為實證應處能力及進行教學訓練
3. 建構工控領域資安治理成熟度
4. 推動國家層級資安風險評估

辦理關鍵基礎設施跨領域攻防演練

中央目的事業主管機關

1. 定期稽核所屬關鍵基礎設施提供者
2. 精進關鍵基礎設施資安聯防機制(情資分享、通報應變、資安監控)

定期於場域進行公私聯合攻防演練

關鍵基礎設施提供者

1. 設置資安長並強化人員資安專業能力
2. 落實資安防護基準

策略二：推動公私協同治理 提升關鍵設施韌性

1. 建立各領域公私協同治理運作機制
   - ① 賡續推動落實資通安全管理法，並適時檢討以因應國際資安防護趨勢
   - ② 推動落實關鍵基礎設施資安防護基準
   - ③ 建構工控領域資安治理成熟度
   - ④ 推動國家層級資安風險評估
2. 增強人員資安意識與能力建構
   - ① 設置資安長並強化人員資安專業能力
   - ② 建立模擬場域，作為實證應處能力及納入資安情境進行教學訓練
3. 公私合作深化平時情資交流與應變演練
   - ① 精進關鍵基礎設施資安聯防機制(情資分享、通報應變、資安監控)
   - ② 定期於場域進行公私聯合攻防演練
   - ③ 辦理關鍵基礎設施跨領域攻防演練

策略三推動架構

藉由網路攻擊狙殺鏈(Cyber Kill Chain)

偵查 (Reconnaissance)

武裝 (Weaponization)

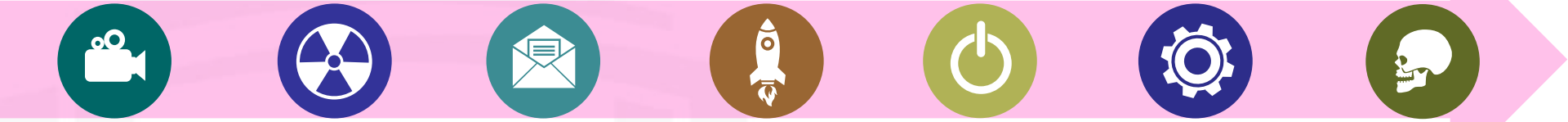
遞送 (Delivery)

攻擊 (Exploitation)

安裝 (Installation)

發令與控制 (Command and Control)

採取行動 (Actions on Objectives)



推動政府大內網及資安防護向上集中

整合國內外情資來源，並深化國際合作

建立資通系統弱點之主動發掘、通報及修補機制

應用新興技術淬鍊有效情報，發展主動式防禦前瞻研究及技術應用

完善政府網際服務網防禦深廣度

提升科技偵查能量防制新型網路犯罪

強化新型網路犯罪偵防能量

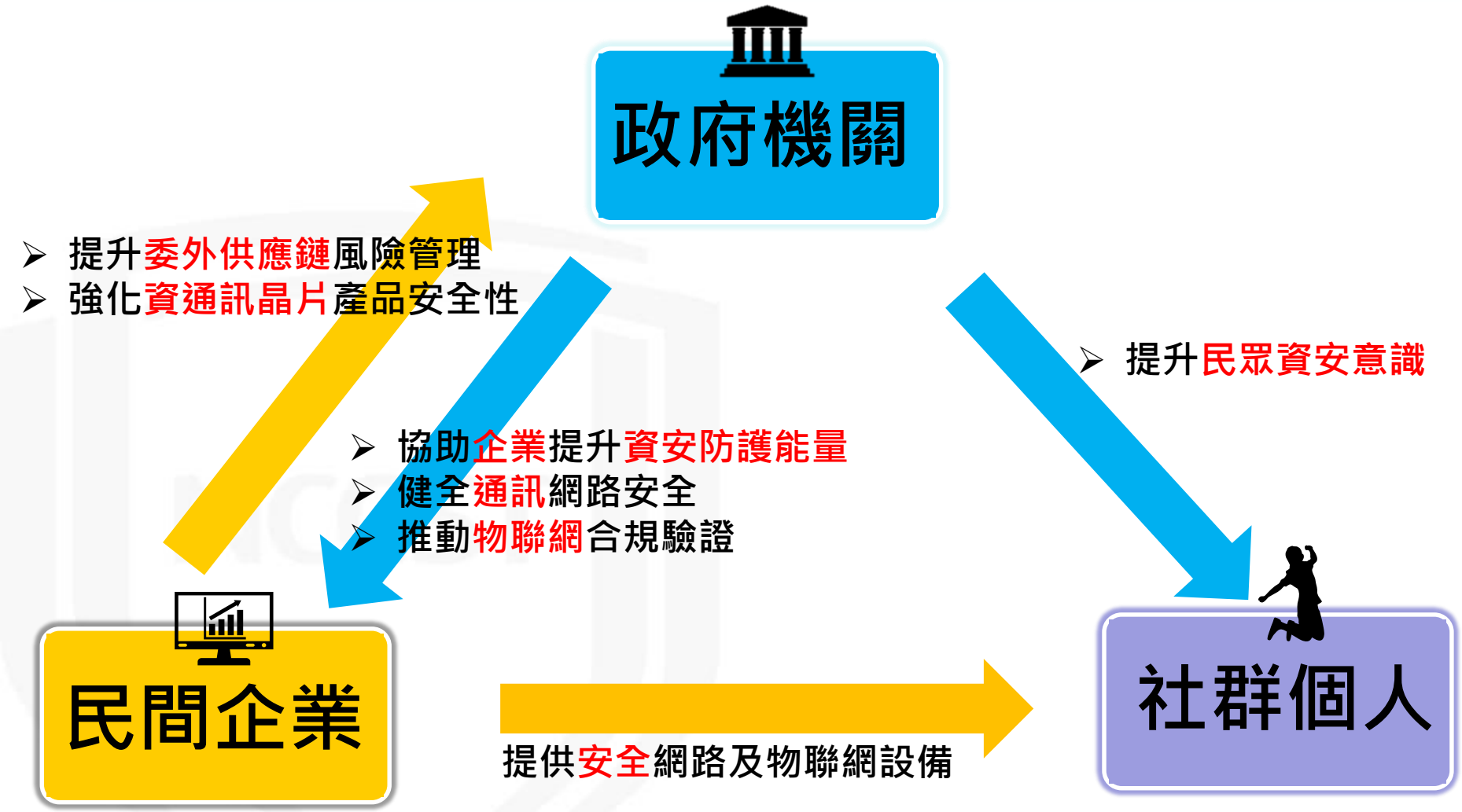
提升資安事件溯源追蹤能力

加強跨境網路犯罪偵查機制

策略三：善用智慧前瞻科技 主動抵禦潛在威脅

1. 賡續推動政府資訊(安)集中共享
   ① 推動政府大內網及資安防護向上集中
   ② 建立資通系統弱點之主動發掘、通報及修補機制
2. 擴大國際參與及深化跨國情資分享
   ① 發展主動式防禦前瞻研究及技術應用
   ② 整合國內外情資來源，並深化國際合作
3. 制敵機先阻絕攻擊於邊境
   ① 應用新興技術淬鍊有效情報，發展主動式防禦技術
   ② 完善政府網際服務網防禦深廣度
4. 提升科技偵查能量防制新型網路犯罪
   ① 強化新型網路犯罪偵防能量
   ② 提升資安事件溯源追蹤能力
   ③ 加強跨境網路犯罪偵查機制

策略四推動架構


政府機關
提升委外供應鏈風險管理
強化資通訊晶片產品安全性
協助企業提升資安防護能量
健全通訊網路安全
推動物聯網合規驗證
提升民眾資安意識
民間企業
提供安全網路及物聯網設備
社群個人

策略四：建構安全智慧聯網 提升民間防護能量

1. 輔導企業強化數位轉型之資安防護能量
   ① 結合民間資源，建立公私協同合作機制，協助企業提升資安防護能量
   ② 提升民眾資安意識
2. 強化供應鏈安全管理
   ① 強化委外供應鏈風險管理
   ② 聚焦資通訊晶片產品安全性
3. 建構智慧國家安全環境
   ① 健全新世代行動通訊技術網路安全
   ② 推動物聯網合規驗證及場域實證

資安防護精進作為

主動式防禦推動策略

網路攻擊狙殺鏈(Cyber Kill Chain)

偵查
(Reconnaissance)
研究、識別及選擇目標，可以在網際網路上搜尋相關資訊，或是利用工具掃描或探測目標環境。

武裝
(Weaponization)
針對特定的安全漏洞，設計遠端存取木馬程式，包裹在可遞送的資料中，多數以自動化工具產生，且利用常見資料檔案進行偽裝。

遞送
(Delivery)
設法將惡意程式傳送到目標環境，如電子郵件附件、網站及可移動的USB媒體等遞送管道。

攻擊
(Exploitation)
惡意程式遞送到目標主機後，將觸發內部的程式碼，以應用程式或作業系統的安全弱點為目標，開始進行攻擊。

安裝
(Installation)
於受駭主機安裝遠端存取的木馬或後門程式，而攻擊者可繼續隱藏於受駭環境中。

發令與控制
(Command and Control)
受駭主機須向外連結網際網路上的控制伺服器，以建立控制通道，攻擊者便可利用此通道遠端操控受駭主機。

採取行動
(Actions on Objectives)
攻擊者開始採取行動，如竊取資料、破壞資料的完整性與可用性、或是做為入侵其他系統的跳板。

情蒐研析

- 提升**威脅情蒐**與**主動偵測**能量，跨國部署蜜罐系統增加**情蒐廣度**
- 配合資源向上集中，部署偵測機制增加**情蒐深度**

縱深防禦

- 建立**零信任網路架構**資安防護驗證環境
- 強化**SOC監控**有效性
- 推動**VANS系統**，提升弱點防護能力
- 推動**端點偵測**資安防護

主動防制

- 以攻擊思維撰擬情境，進行**主動防制技術**實作
- 發展**自動化控制平台**，及早掌握攻擊行為

溯源阻斷

- **強化事件處理與協防成效**，關聯駭客攻擊情勢
- 建立偵測規則部署與回傳機制，**即時告警阻斷攻擊**

1. 情資研析

- 從網際網路、政府網際服務網及政府機關3個面向，蒐集各種威脅資訊，並提供預防性情資，以達早期預警

縱深情蒐

網際網路(Internet)

蜜網網路攻擊威脅情蒐

網路威脅誘捕情蒐

- 物聯網攻擊威脅偵測
- 工控系統與網通設備

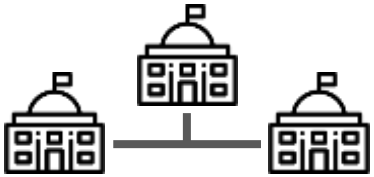
掃描探測

政府網際服務網(GSN)

骨幹閘道偵測機制

政府網路威脅情蒐

- 機關網路威脅與惡意連線偵測
- 叢集式社交工程威脅檢測



入侵攻擊

政府機關(Agency)

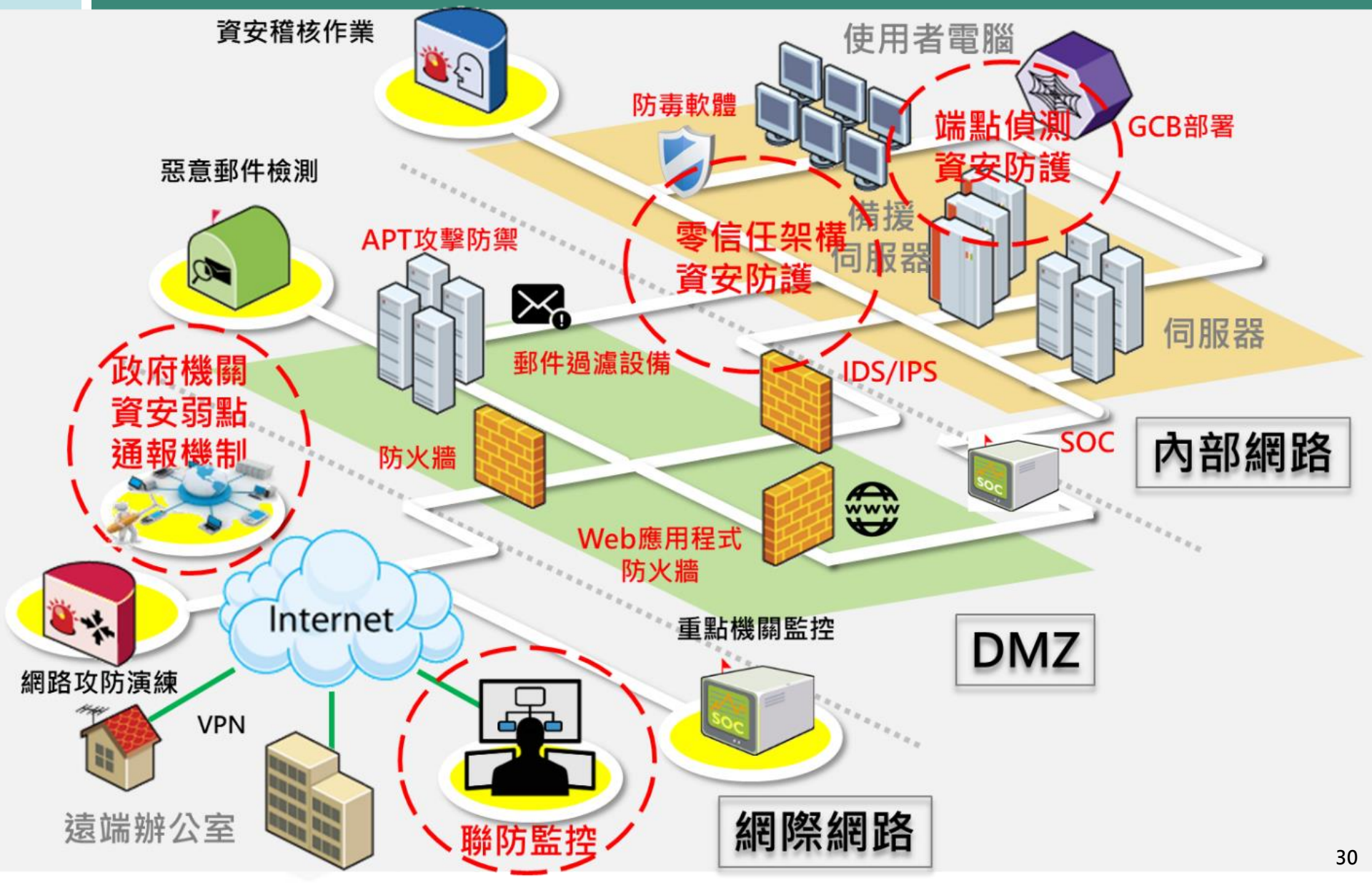
使用者端點郵件防護

使用者端點威脅情蒐

- 釣魚郵件與惡意附檔分析
- 分散式社交工程威脅檢測

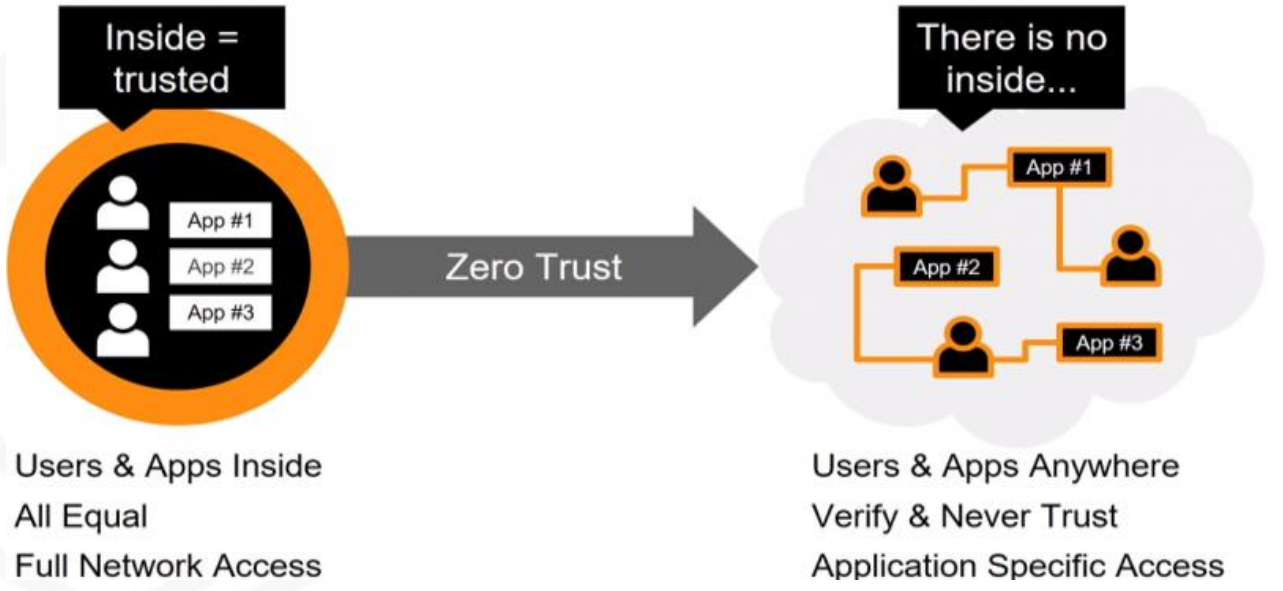
社交工程

2. 縱深防禦


資安稽核作業
使用者電腦
防毒軟體
端點偵測
資安防護
GCB部署
惡意郵件檢測
備援
伺服器
APT攻擊防禦
零信任架構
資安防護
伺服器
郵件過濾設備
IDS/IPS
政府機關
資安弱點
通報機制
防火牆
SOC
內部網路
Web應用程式
防火牆
Internet
重點機關監控
DMZ
網路攻防演練
VPN
遠端辦公室
聯防監控
網際網路

2.1 零信任概念

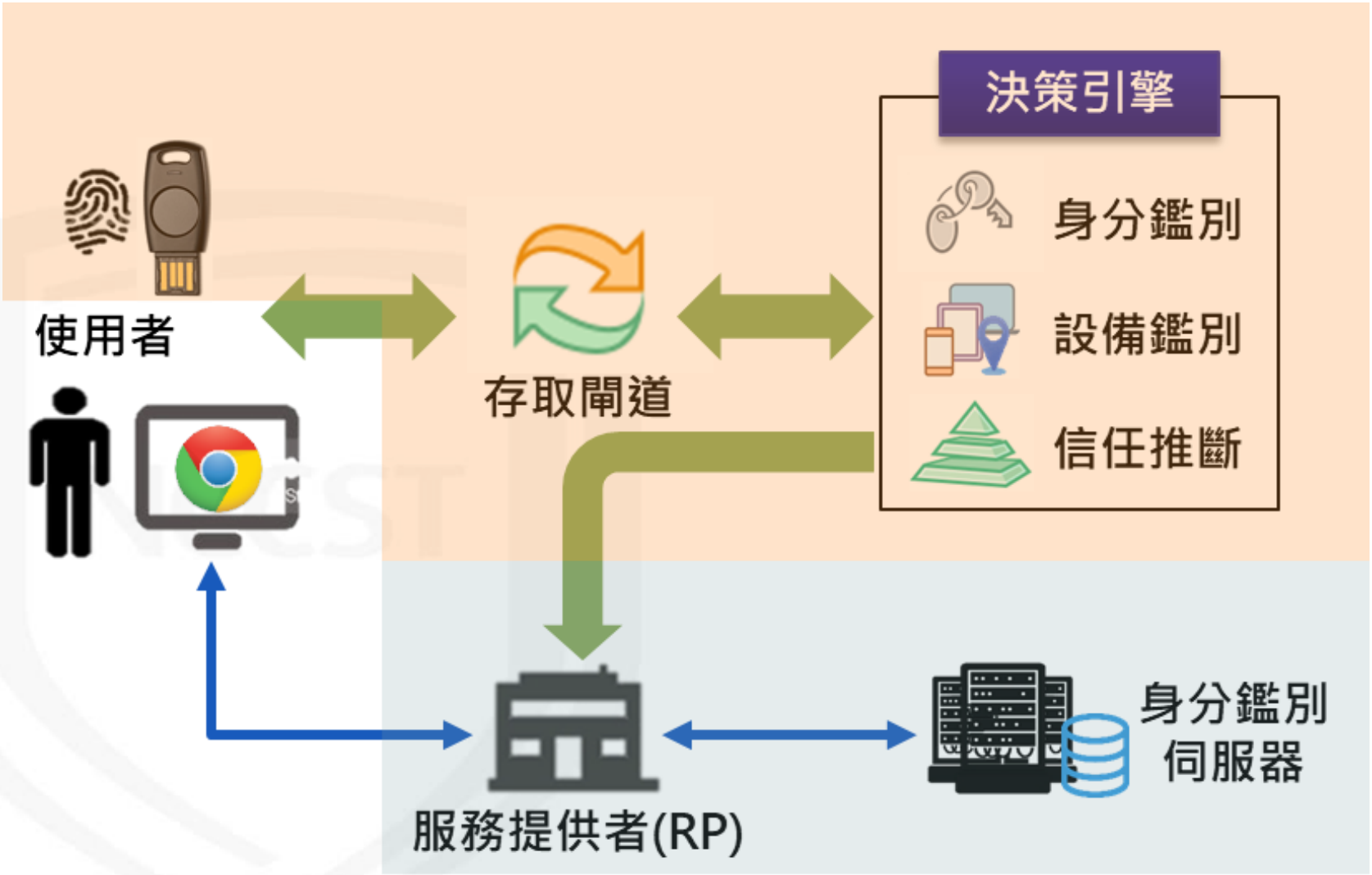
- 零信任希望突破傳統網路模型的資安窘境，並能保護資料存取
  - 不是保護網路存取，而是保護資料/應用存取
  - 無具體邊界，使用者/設備與資料/應用無處不在
  - 任何資料存取永不信任且必須驗證



零信任關鍵技術

- 身分鑑別
  - 無密碼且多因子身分認證
- 設備鑑別
  - 區別並追蹤企業擁有/非企業擁有與私有/公開設備
  - 設備健康檢查，包含組態設定、作業系統與漏洞更新狀態及攻擊情資等
- 存取授權
  - 支援決定最小存取授權之信任推斷或情境感知存取等

零信任網路架構



2.2 政府領域資安聯防監控

SOC監控有效性驗證規劃

- 針對政府機關完善資安監控範圍
- 針對資安監控服務廠商以技服中心掌握之攻防演練、資安警訊及資安通報，分析廠商監控成效

政府機關資安監控範圍

- 法定之資通安全防護項目與核心資通系統(含AD)等相關之資訊設備紀錄與服務/應用程式紀錄，納入監控範圍

資通安全防護	•防毒軟體 •網路防火牆 •電子郵件過濾機制
	•入侵偵測及防禦機制 •應用程式防火牆
	•進階持續性威脅攻擊防禦措施

SOC監控偵測能力分析

- 資安防護項目回傳率
- 資安防護項目涵蓋率
- 網路攻防演練驗證
- 技服中心資安警訊驗證
- 機關資安事件通報驗證

SOC資安監控情資品質分析

- 基本SOC回傳之資安監控情資品質分析
- 關聯威脅情資回饋能量

SOC監控防護能力分析

- 情資分析單回傳率

2.3 政府機關資安弱點通報機制

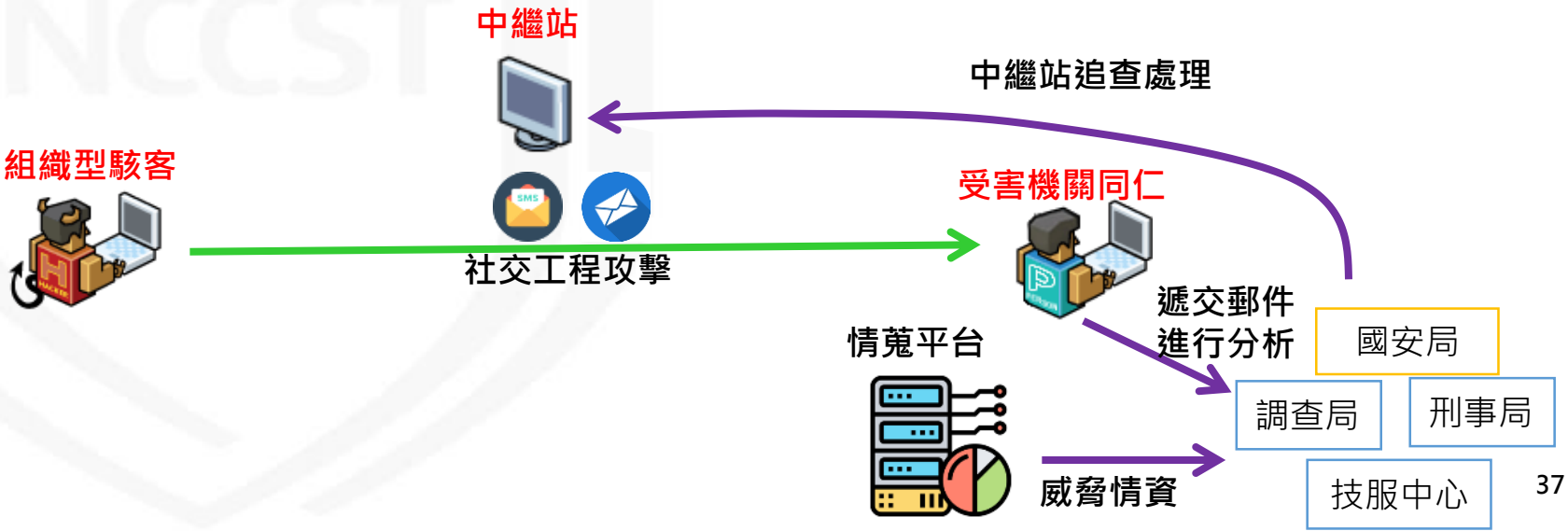
- 推動政府機關資安弱點通報機制(Vulnerability Alert and Notification System, VANS)，結合資訊資產與弱點管理，提升弱點防護能力

2.4 端點偵測資安防護

- 規劃公務機關端點偵測機制，接收A、B級公務機關之EDR掃描結果
  - 為了解各機關EDR偵測情形，透過建立EDR事件資料庫，並設計統一傳輸格式，以利接收不同EDR廠商之偵測結果，藉以掌握駭客活動

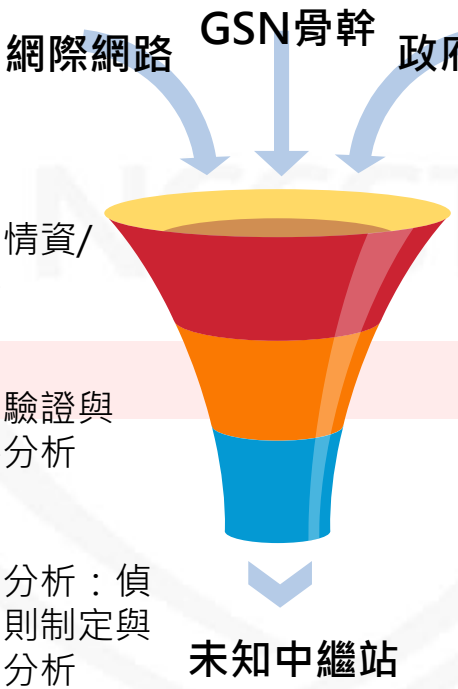
3. 主動防制

- 透過主動出擊，減弱與破壞駭客相關資源，協助政府機關防護
  - 109年4月微軟偕台灣在內之35國執法單位，摧毀Necurs殭屍網路
- 進行主動防制合作與技術研究
  - 針對郵件與簡訊之社交工程手法，進行攻擊分析
  - 透過威脅情資，及時掌握駭客活動
  - 搭配適時處理與應變防制，降低政府機關資安風險



4. 溯源阻斷

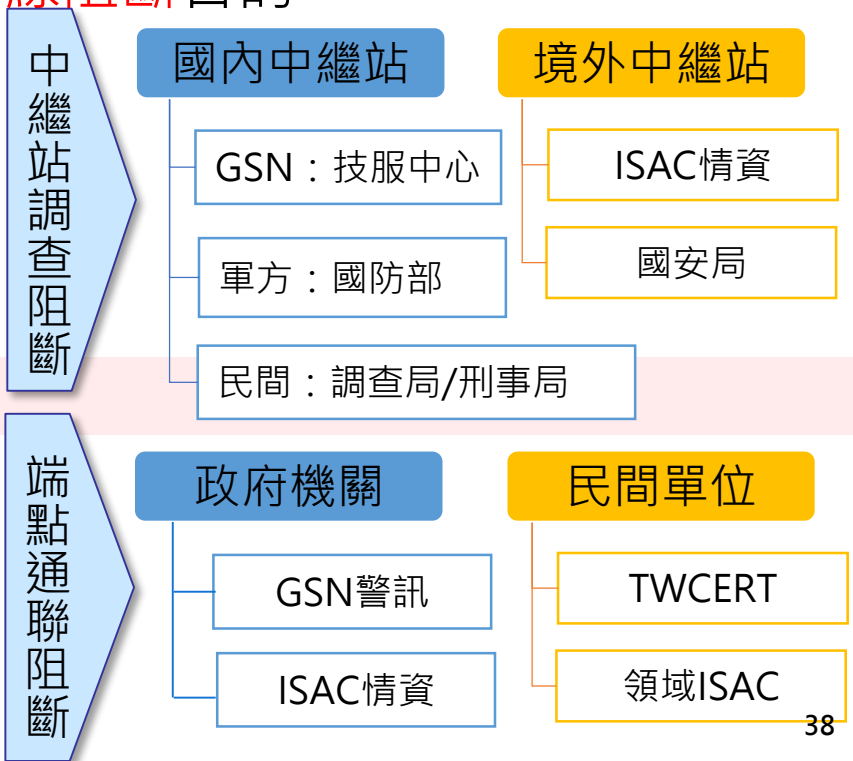
- 當資安事件發生，啟動聯防作業，透過鑑識調研，掌握攻擊來源，並阻斷攻擊行為
  - 針對發現之國內外中繼站，協同外單位共同調研取證，進一步追查攻擊來源，達到追蹤溯源目的
  - 配合端點鑑識即時告警，達到連線阻斷目的



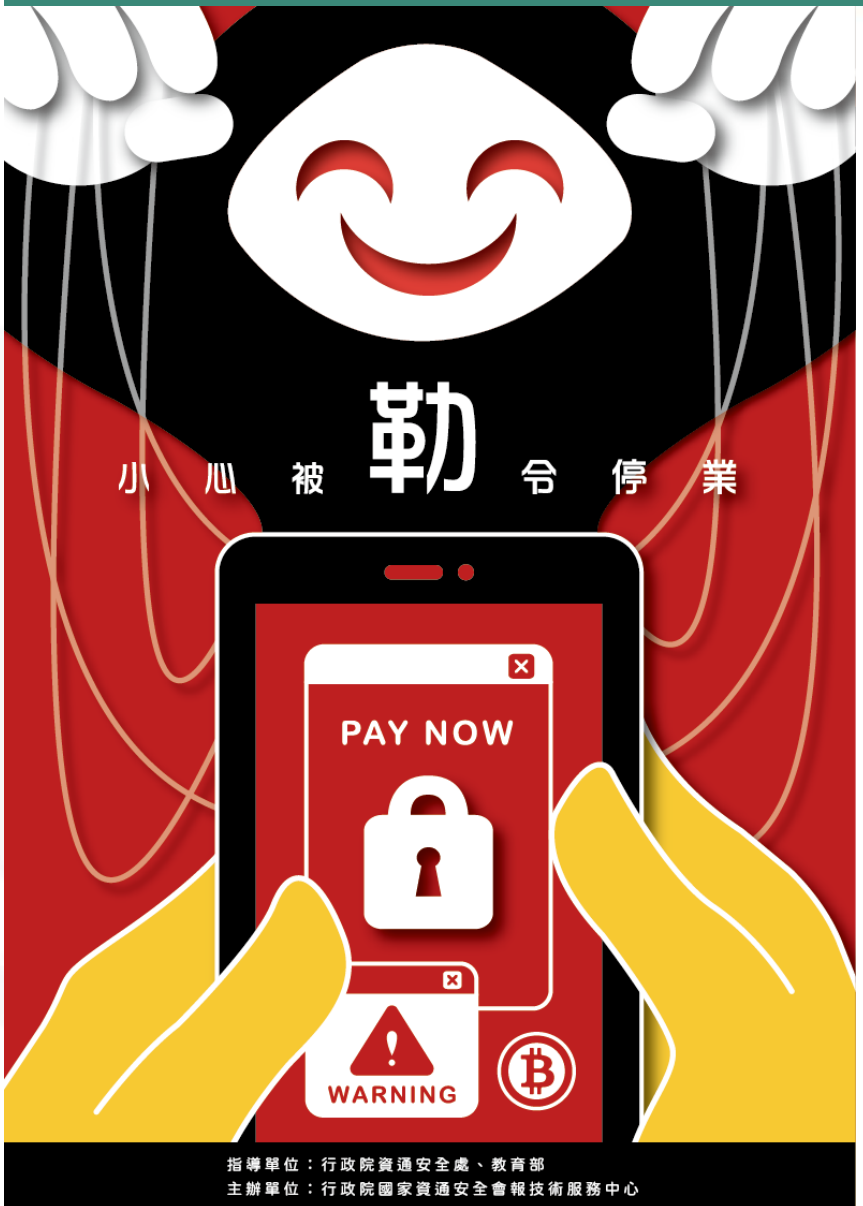
網際網路
- 國內/外攻擊來源IP
- 國內資訊設備弱點通知
- 惡意程式資訊分享

GSN骨幹
- GSN骨幹異常連線通知
- 惡意程式偵測防護

政府機關
- 攻擊手法
- 惡意程式資訊分享
- 廠商資訊



109年資安海報第一名作品



報告完畢
敬請指教