# 國家資通安全發展方案

# (110年至113年)草案

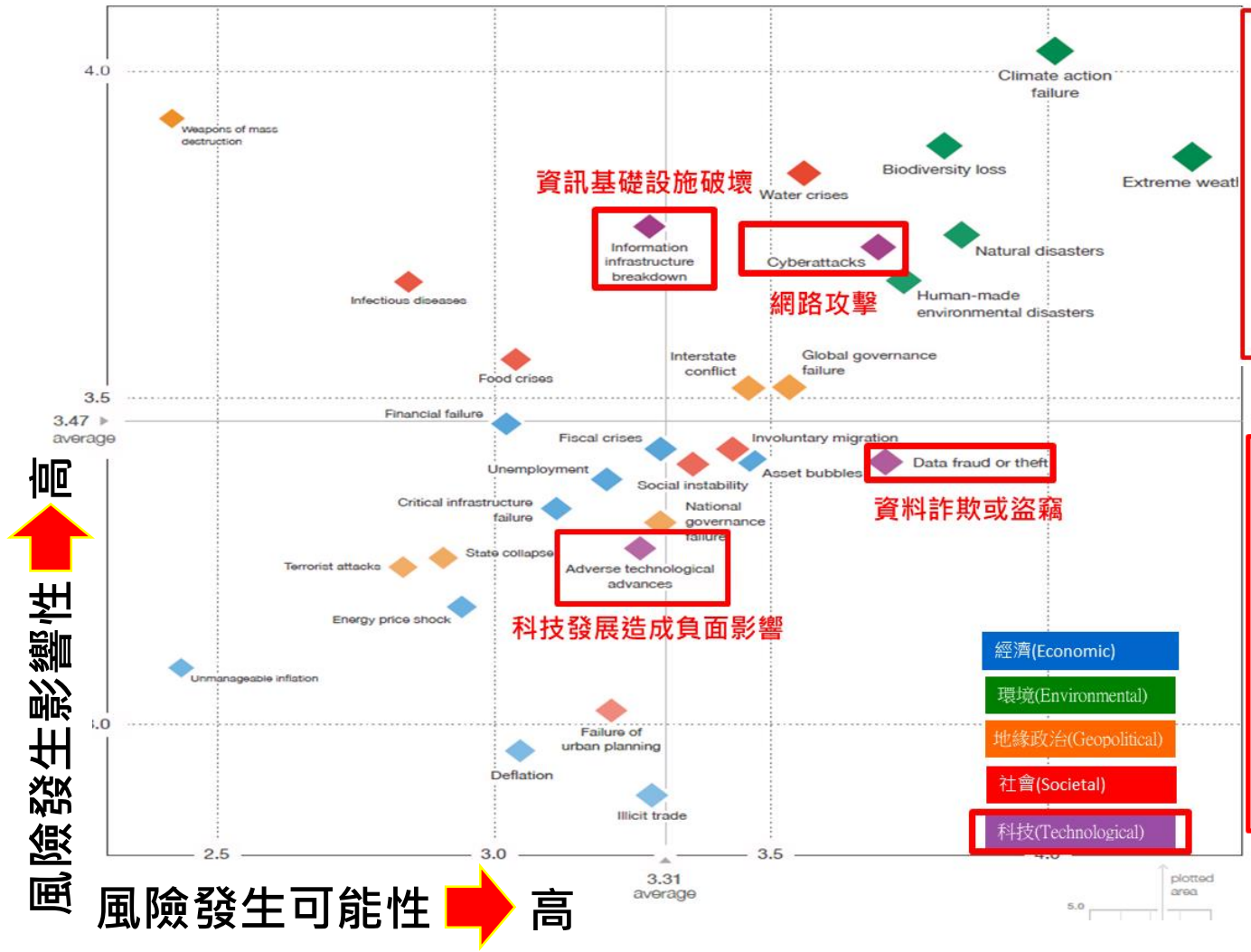
行政院資通安全處

109年12月

# 大綱

- 國際資安威脅及政策趨勢
  - 國際資安威脅
  - 國際資安政策趨勢
- 第5期國家資通安全發展方案成效
- 問題評析
  - 分析SWOT及應對策略
- 下期方案藍圖
  - 願景、目標、策略、具體措施
- 宣導事項

# 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. 主要經濟體資產泡沫

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

# 2019年全球資通安全威脅趨勢

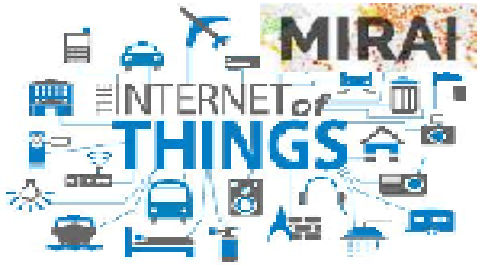
## 綜整2019年全球資安威脅與相關研究報告，歸納全球6大資安威脅趨勢

來源：108年資通安全技術年報

| | 個人資料與憑證外洩攻擊白熱化 | 勒索軟體攻擊風險激增 | IoT與行動式設備資安弱點威脅升高 | APT鎖定式攻擊竊取機密資料 | 資安(訊)供應商遭駭破壞供應鏈安全 | 關鍵資訊基礎設施資安風險倍增 |
|---|---|---|---|---|---|---|
| 趨勢科技 | ▲ | ▲ | ▲ | ▲ | ▲ | ▲ |
| IBM | ▲ | | ▲ | | | |
| Google | ▲ | ▲ | | | ▲ | |
| Akamai | ▲ | ▲ | | ▲ | | |
| CISCO | ▲ | ▲ | ▲ | | | |
| Symantec | ▲ | ▲ | ▲ | ▲ | | |


**個人資料與憑證外洩**
**攻擊白熱化**


**勒索軟體攻擊風險激增**




**IoT與行動式設備**
**資安弱點威脅升高**


**APT鎖定式攻擊**
**竊取機密資料**


**資安(訊)供應商持續遭駭破**
**壞供應鏈安全**


**關鍵資訊基礎設施**
**資安風險倍增**

# 大綱

- 國際資安威脅及政策趨勢
  - 國際資安威脅
  - 國際資安政策趨勢
- 第5期國家資通安全發展方案成效
- 問題評析
  - 分析SWOT及應對策略
- 下期方案藍圖
  - 願景、目標、策略、具體措施
- 宣導事項

# 國際參考對象遴選方式

- 透過ITU發布之2018年全球資通安全指標，針對全球分為6區：美洲區、歐洲區、亞太區、非洲區、阿拉伯區、獨立國家國協區(俄羅斯區域)。
- 選擇各區域高資安指標之國家，另加上以色列，以了解各國資安戰略發展現況，期作為我國參考借鏡。

**Americas region**

| Member State | Score | Regional Rank | Global Rank |
|---|---|---|---|
| United States of America* | 0.926 | 1 | 2 |
| Canada* | 0.892 | 2 | 9 |
| Uruguay | 0.681 | 3 | 51 |

**Europe region**

| Member State | Score | Regional Rank | Global Rank |
|---|---|---|---|
| United Kingdom | 0.931 | 1 | 1 |
| France | 0.918 | 2 | 3 |
| Lithuania | 0.908 | 3 | 4 |
| Estonia | 0.905 | 4 | 5 |
| Spain | 0.896 | 5 | 7 |

歐盟

**Asia-Pacific region**

| Member State | Score | Regional Rank | Global Rank |
|---|---|---|---|
| Singapore | 0.898 | 1 | 6 |
| Malaysia | 0.893 | 2 | 8 |
| Australia | 0.890 | 3 | 10 |
| Japan | 0.880 | 4 | 14 |
| Republic of Korea | 0.873 | 5 | 15 |

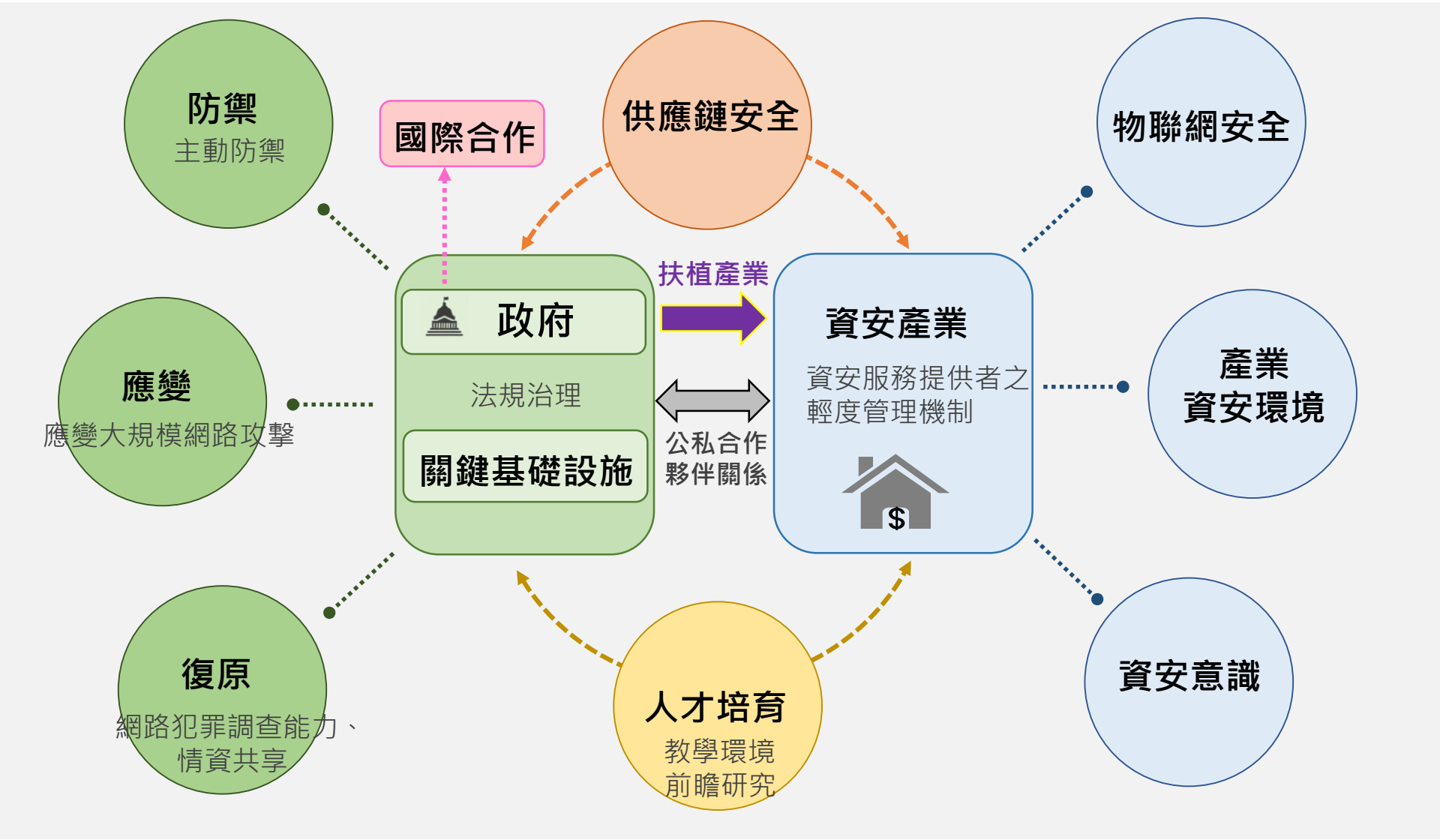
# 國際資安戰略發展現況 (1/2)

| 國家 | 公布/施行 | 國家資安戰略 | 戰略方向 |
|---|---|---|---|
| 美國  | 2018.09 | 國家網路戰略 | 4大構面、10項目標<br>主要採取主動防禦，保護國家資產及民眾隱私，並提高惡意者攻擊代價 |
| 加拿大  | 2019.05 | 國家資通安全行動計畫 2019-2024 | 3大目標：1.強化關鍵基礎設施防護並增強網路犯罪調查能力、2.支持前瞻研究並協助創新企業、3.國內與各省及民間合作，國外結合盟友共同塑造環境 |
| 歐盟  | 2019.06 | 資通安全法 | 強化治理權限，提高人力、財務資源分配，建立「歐盟網路安全驗證框架」驗證計畫，評估資通訊產品、服務及製程是否符合安全 |
| 英國  | 2016.11 | 國家資通安全戰略 2016-2021 | 3大戰略目標：防禦、嚇阻、發展<br>1.防護政府網路及關鍵基礎設施<br>2.扼制網路犯罪<br>3.發展網路安全相關科學研究 |
| 澳洲  | 2020.08 | 2020澳洲資通安全戰略 | 預計將於10年內投資16.7億澳幣，主要投入：<br>1.強化對人民、企業及關鍵基礎設施的保護<br>2.保護企業產品和服務免受威脅或弱點的侵害<br>3.透過公私協力，促進網路安全 |

# 國際資安戰略發展現況 (2/2)

| 國家 | 公布/施行 | 國家資安戰略 | 戰略方向 |
|---|---|---|---|
| 日本  | 2018.07 | 資通安全戰略 | 3大目標，包含4項策略：1.實現網路安全供應鏈及架構安全IoT系統；2.建構大學教研環境；3.制定網路犯罪對策；4.強化政府網路防禦、抑制網路攻擊能力與應變大規模攻擊之能力 |
| 韓國  | 2019.04 | 國家資通安全戰略 | 具有6個目標，包含加強國家核心基礎設施安全、提高網路攻擊應變能力、建立具信任和管理的網路治理、奠定網路安全產業基礎環境、培養網路安全文化、領導國際網路安全合作 |
| 新加坡  | 2018.03 | 資通安全法 | 達成安全網路空間，包含CI防護、對抗網路攻擊、情資共享及資安服務提供者輕度管理機制 |
| 以色列  | N/A | 各部會施政計畫 | 透過軍、官、民合作，建構資通安全機制，分平常、一般及國家層級事件三層防護，透過主管機關提供資源因應；並鼓勵資安等產業創新 |

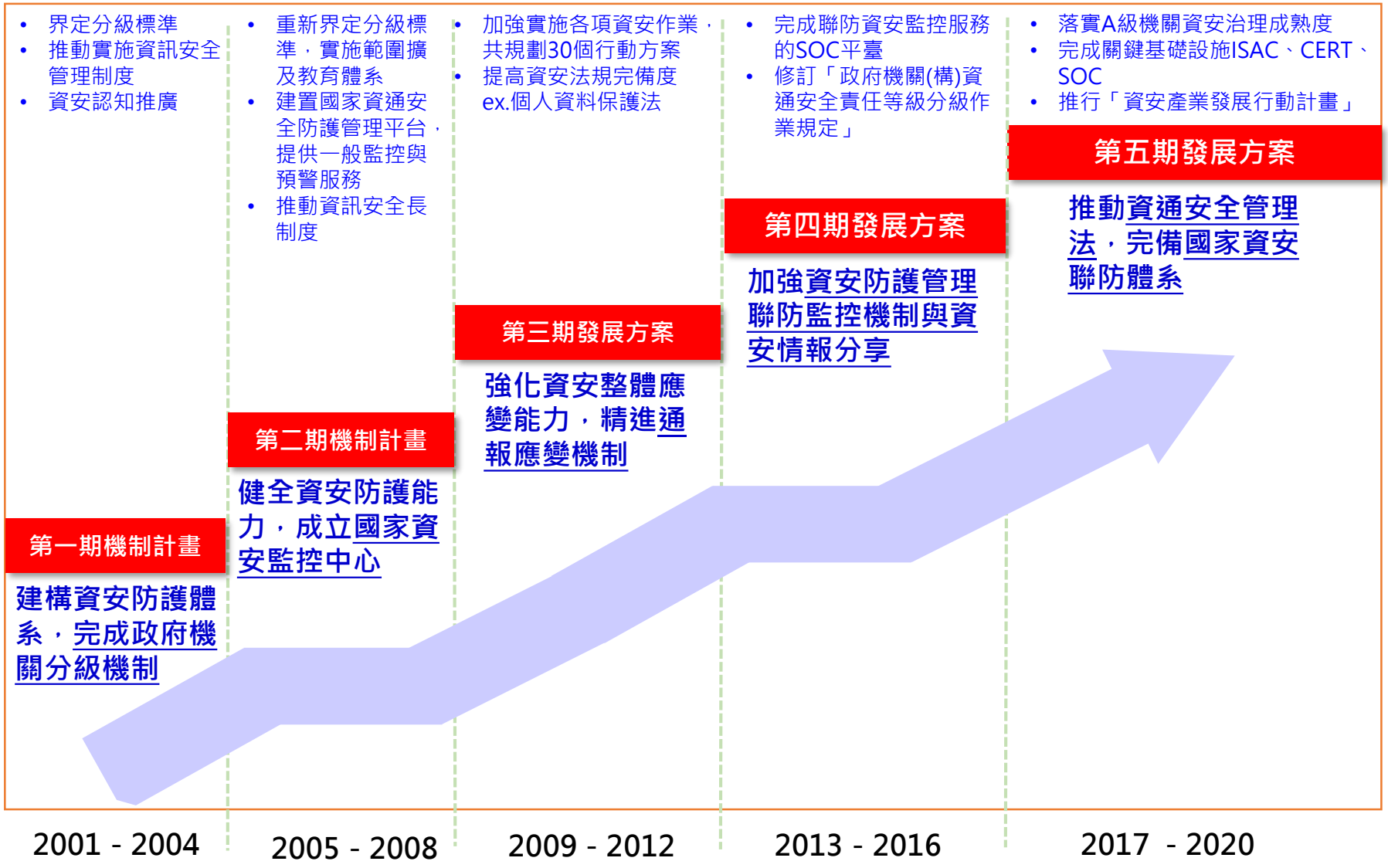
# 國際資安戰略發展分析


防禦
主動防禦
國際合作
供應鏈安全
物聯網安全
扶植產業
政府
法規治理
關鍵基礎設施
資安產業
資安服務提供者之
輕度管理機制
$
公私合作
夥伴關係
應變
應變大規模網路攻擊
產業
資安環境
復原
網路犯罪調查能力、
情資共享
人才培育
教學環境
前瞻研究
資安意識

# 大綱

- 國際資安威脅及政策趨勢
  - 國際資安威脅
  - 國際資安政策趨勢
- 第5期國家資通安全發展方案成效
- 問題評析
  - 分析SWOT及應對策略
- 下期方案藍圖
  - 願景、目標、策略、具體措施
- 宣導事項

# 我國資安推動進程


界定分級標準
推動實施資訊安全管理制度
資安認知推廣
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
2001 - 2004
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
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
2005 - 2008
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
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
2009 - 2012
完成聯防資安監控服務的SOC平臺
修訂「政府機關(構)資通安全責任等級分級作業規定」
第四期發展方案
加強資安防護管理聯防監控機制與資安情報分享
2013 - 2016
落實A級機關資安治理成熟度
完成關鍵基礎設施ISAC、CERT、SOC
推行「資安產業發展行動計畫」
第五期發展方案
推動資通安全管理法，完備國家資安聯防體系
2017 - 2020

# 資通安全發展方案與各計畫關聯

## 第5期資安發展方案策略

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

**資安旗艦計畫**

**技術服務計畫**

**數位國家資通安全**

**前瞻基礎建設計畫**

- 強化國家資安基礎建設計畫
- 強化政府基層機關資安防護及區域聯防計畫

**資安產業發展行動計畫**

# 完備資安基礎環境

## 強化國家安全第一道防線

完成國家通訊暨網際安全中心(NCCSC)建置，持續優化系統及擴充納管業者，包括DNS 9家(100%)、海纜8家(100%)、行網5家(100%)、固網4家(100%)、衛星4家(100%)、有線電視64家(100%)及無線廣播(109年新增25家)與無線電視(109年新增5家)，並採7*24小時即時監控，亦於特定期間加強資安監控，強化通訊傳播事業資安事件通報及應變之時效性

## 建立國內物聯網資安標準生態系


推動國內自有物聯網資安標準，制定影像監控(IP CAM, NVR, DVR)3項、智慧巴士(車載機與智慧站牌)2項及智慧路燈(燈控器與照明閘道器)2項等共7項物聯網資安標準，其中IP Cam資安產業標準已成為國家標準(CNS 16120)

## 推動「資通安全管理法」成為我國首部資安專法

107年5月11日經立法院三讀通過資通安全管理法，6月6日總統令公布，12月5日函頒施行令；於108年1月1日正式施行，8月26日檢討修正「資通安全責任等級分級辦法」部分條文；並於109年6月啟動資通安全管理法及其子法檢討作業

# 建構國家資安聯防體系-中央機關

## N-ISAC (National ISAC)

**能源&水資源整合**
完成E-ISAC，並與水資源、民營能源、油電水ISAC平台介接，已納入 28 個經濟部所屬財團法人

**民營能源**
完成PE-ISAC，累計25家會員，並完成資訊資產盤點與風險評估方法

**通訊傳播**
完成C-SOC、C-ISAC及C-CERT平台，並持續納入通傳CII業者，累計188家加入平台

**高科技園區**
完成SP-ISAC平台，科學園區廠商累計1,210家參與

協助各CI主管機關建置領域ISAC及CERT，並與N-ISAC及N-CERT介接，完成**跨域資安聯防**

**水資源**
完成W-ISAC、W-SOC平台，彙整水資源資安監控事件，進行根因分析並研擬防範措施

**緊急醫療**
完成H-ISAC及H-CERT累計208家醫院加入，並建立資安防護策略與防護基準，提供CI醫院據以落實資安管理

**交通運輸**
完成T-ISAC及T-CERT累計260個會員，並進行CIP的ICS之SOC可行性評估。

**金融**
完成F-ISAC及F-CERT累計376個會員，並與國際ISAC組織協同合作，擴增金融業專屬情資來源

**學術網路**
完成TANet骨幹智慧聯防平臺，自動化派送資安威脅情資至13個區域網路中心

**犯罪偵防**
建置6都跨域鑑識服務分區中心及警政體系資安事件與鑑識相關系統

**外館資安健診制度化**
歐洲、東北亞、美洲、東南亞4區域、13駐外館處

**強化政府A級機關資安防護**
總統府、國安會、審計部、本院國土辦等

# 建構國家資安聯防體系-地方政府

## 共同成果

1.建置區域ISAC並成為N-ISAC會員。
2.建置區域CERT
3.完成一線SOC涵蓋率近達8成。

桃園市區域聯防建構情資分享平台，並辦理通報演練就多種入侵手法與情境下進行實地攻擊。

臺中市區域聯防建構區域聯防APT動態威脅偵測系統，對可疑惡意程式進行沙箱分析，並將產出之特徵碼，同步派送至聯防縣市。

臺南市區域聯防提供實證場域予成功大學，對市府資訊系統進行滲透測試活動，找出相關弱點並修復，建立官學合作。

臺北市區域聯防建構端點防禦機制，108年已找出14個新種惡意程式及1個系統0-day漏洞。

新北市區域聯防建構區域聯防平台涵蓋聯防縣市共325個機關(單位)，另推動公私協同合作，提供實證場域予國內業者建置Honey Pot。

高雄市區域聯防建置自動化弱點掃描系統，已收納聯防縣市70個機關共127個系統，並可排程掃描、弱點追蹤並自動複驗等，有效節省人力成本。


桃園市政府
1. 新竹縣
2. 新竹市
3. 苗栗縣

新北市政府
1. 宜蘭縣
2. 基隆縣

臺北市政府
1. 金門縣
2. 連江縣
3. 花蓮縣

臺中市政府
1. 彰化縣
2. 南投縣

臺南市政府
1. 嘉義縣
2. 嘉義市
3. 雲林縣

高雄市政府
1. 屏東縣
2. 臺東縣
3. 澎湖縣

# 推升資安產業自主能量

## 1.推升資安產值

1) 107年資安產值439.4億，108年產值成長至493.4億，108年產值年成長率達12.2%，推估109年資安產業可望超過550億以上。
2) 打造台灣自主研發資安解決方案整合服務上架平台，促成51家、76項次國內資安自主產品或服務上架，打造國產最大資安商城。

## 2.發展資安產業標準環境

1) 建立物聯網資安檢測標準與檢測制度，完成7項物聯網標準，其中網路攝影機資安已納入國家標準，累計成立9家網路攝影機合格資安檢測實驗室，1家智慧巴士合格資安檢測實驗室以及2家智慧路燈資安檢測實驗室，已輔導36款合格網路攝影機產品，1款智慧站牌及1款車載機合格產品通過實驗室檢測。
2) 成立國際資安工作小組，成員包括台積電、日月光、趨勢科技等，共同撰擬SEMI國際資安標準草案。

## 3.扶植新創公司

1) 扶植新創公司累計達 22家 ，如白帽駭客社群產業化或帶動大企業進行投資。
2) 結合臺灣資安大會於南港展覽館2館舉辦「2020臺灣資安館」，並以2大特區進行展示，包括智慧臺灣安全展(四大主題：製造、醫療、工控與物聯網產業資安標準)及臺灣自主研發特展。其中臺灣自主研發特展，集結具備國內自主資安產品能量的廠商與單位共36家、40個攤位，共同打造臺灣資安品牌形象。

# 孕育優質資安人才

## 1 在職資安人才培訓—106年至108年累計培訓2,316名資安人才

- 針對待業者開設中長期養成班，培訓產業新進資安人才並媒合就業，以補充在職資安人力缺口，106-108年產業資安人才培訓累計達 2,316人次 。
- 109年短期資安人才累計開訓11班220人次、關鍵基礎設施資安人才累計開訓6班133人次、長期資安人才訓練課程3班次累計開訓3班69人次。

## 2 在學資安人才培育—推動4所大專院校成立5個資安碩士(學程)班

- 推動4所大專院校自108年起成立5個資安碩士(學程)班，逐步建置系統性資安人才培育體系
- 透過資安扎根、跨域教學、實務實戰、導師輔導及國際合作等策略，建立高中職及大專院校系統化培育資安專業人才之機制，為我國孕育優質在學資安人才。

## 3 高階資安人才養成3年培育774名資安碩博士生

- TWISC中心聯盟向下成立7個TWISC資安特色中心，累計培育資安碩博士生774名，截至109 年 8 月底已發表289篇期刊及研討會論文，執行96件產學合作，並移轉15項資安技術。

## 4 舉辦 HITCON CTF國際資安競賽，104年至108年吸引約6,500隊參與

- 本競賽已連續5年成為美國 DEFCON CTF種子資格賽，104年至108年吸引約6,500隊參與
- HITCON X Balsn 聯隊取得2020年DEFCON國際資安總決賽第3名。

# 大綱

- 國際資安威脅及政策趨勢
  - 國際資安威脅
  - 國際資安政策趨勢
- 第5期國家資通安全發展方案成效
- 問題評析
  - 分析SWOT及應對策略
- 下期方案藍圖
  - 願景、目標、策略、具體措施
- 宣導事項

# SWOT分析

## 優勢

1、資安為我國重點政策且積極推動
2、訂定資通安全管理法與子法、制定產業標準與檢測規範，完備法律基礎與相關制度配套
3、我國ICT產業供應鏈與工控電腦產品出口優勢
4、我國資訊相關人才素質佳，高階駭客人才藏富於民

## 劣勢

1、資安法規尚難全面擴及，企業及國民資安意識仍待提升
2、國家整體資安聯防機制仍待深廣化
3、國內資安產業規模較小、產值較低
4、欠缺前瞻研究、實戰及關鍵基礎設施等資安人才

## 機會

1、我國具有全球重要的資安戰略位置
2、網路犯罪偵查及資安防禦機制等已具一定能量，提升國際合作意願
3、政府資通訊環境逐步集中，有助強化防護
4、5G、物聯網(IoT)、AI及產業創新等資安防護需求日益提升

## 威脅

1、政經情勢特殊，面臨國家級組織駭客威脅
2、新型態資安威脅不斷推陳出新，主動防禦機制仍有不足
3、關鍵基礎設施及供應鏈資安風險日益增加，缺乏公私協同合作機制
4、我國資安業者面臨國際大廠強大競爭壓力

**資料來源：**資安會報第31-34次委員會議紀錄、立法院審查行政院(院本部)107-109年度預算案決議事項分辦表、資安產業發展行動計畫(107-114年)、108年度資安旗艦計畫(3/4)暨前瞻基礎建設計畫執行情形訪視報告、108年9月17-18日下階段國家資通安全發展方案芻議專家座談會、108年12月13-14日資安策略會議、108年資安政策白皮書

# TOWS分析矩陣

◎建構智慧國家安全環境(S1+S2+S3+O4)

◎提升科技偵查能量防制新型網路犯罪(S1+S4+O2)

◎制敵機先阻絕攻擊於邊境(S1+O2+O3)

◎賡續推動政府資訊(安)集中共享(W2+O3)

◎擴大國際參與及深化跨國情資分享(W2+O2)

◎擴增高教資安師資員額與教學資源(W4+O1+O4)

◎挹注資源投入高等資安科研(W4+O1+O2+O4)

SO進攻策略　WO轉進策略

ST迴避策略　WT避險策略

◎強化供應鏈安全管理(S2+S3+S4+T3)

◎建立各領域公私協同治理運作機制(S2+S4+T3)

◎公私合作深化平時情資交流與應變演練(S2+S4+T2+T3)

◎輔導企業強化數位轉型之資安防護能量(W1+W2+T1)

◎培育頂尖資安實戰及跨域人才(W4+T1+T2)

◎增強人員資安意識與能力建構(W1+T2+T3)

# 大綱

- 國際資安威脅及政策趨勢
  - 國際資安威脅
  - 國際資安政策趨勢
- 第5期國家資通安全發展方案成效
- 問題評析
  - 分析SWOT及應對策略
- 下期方案藍圖
  - 願景、目標、策略、具體措施
- 宣導事項

# 資安卓越產業

1090821向院長報告核定

## 主軸

## 強化新興領域防護

### 各核心產業導入資安開發新領域資安國際解決方案 5案

#### 研發5G、半導體等前瞻技術

- 以科專計畫研發IC設計檢測、5G等防護技術與AI輔助偵防【經濟部、科技部】
- 建立5G網路及軟體資通安全管理、檢測機制【通傳會】

#### 開發AIoT及醫療等新興領域解決方案

推動跨域聯防計畫，由資安業者與5G、物聯網及醫療等新興產業組成團隊，開發防護產品【經濟部】

## 打造高階實戰場域

### 國際攻防場域及高階資安人才基地

#### 成立資安攻防及跨國合作機構

- 進行國防、國安所需前瞻資安研究【院資安處】
- 建置4座關鍵基礎設施模擬場域，進行攻防演練【院資安處】
- 與歐美如柏克萊大學、NATO聯合網路防禦中心等機構合作【院資安處】

#### 完善資安高教環境

透過資安師資擴增計畫，增加80名師資及加碼薪資補助【教育部】

# 第六期國家資通安全發展方案草案

**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<br>培植自主創研能量 | 推動公私協同治理<br>提升關鍵設施韌性 | 善用智慧前瞻科技<br>主動抵禦潛在威脅 | 建構安全智慧聯網<br>提升民間防護能量 |
|---|---|---|---|

**具體措施**

| | | | |
|---|---|---|---|
| 1. 擴增高教資安師資員額與教學資源<br>2. 挹注資源投入高等資安科研<br>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<br>2. 增強人員資安意識與能力建構<br>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<br>2. 擴大國際參與及深化跨國情資分享<br>3. 制敵機先阻絕攻擊於邊境<br>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<br>2. 強化供應鏈安全管理<br>3. 建構智慧國家安全環境 |

# 策略一

# 吸納全球高階人才
# 培植自主創研能量

# 策略—推動架構

**目標**

**成為亞太高階資安人才及技術創新基地**

**策略**

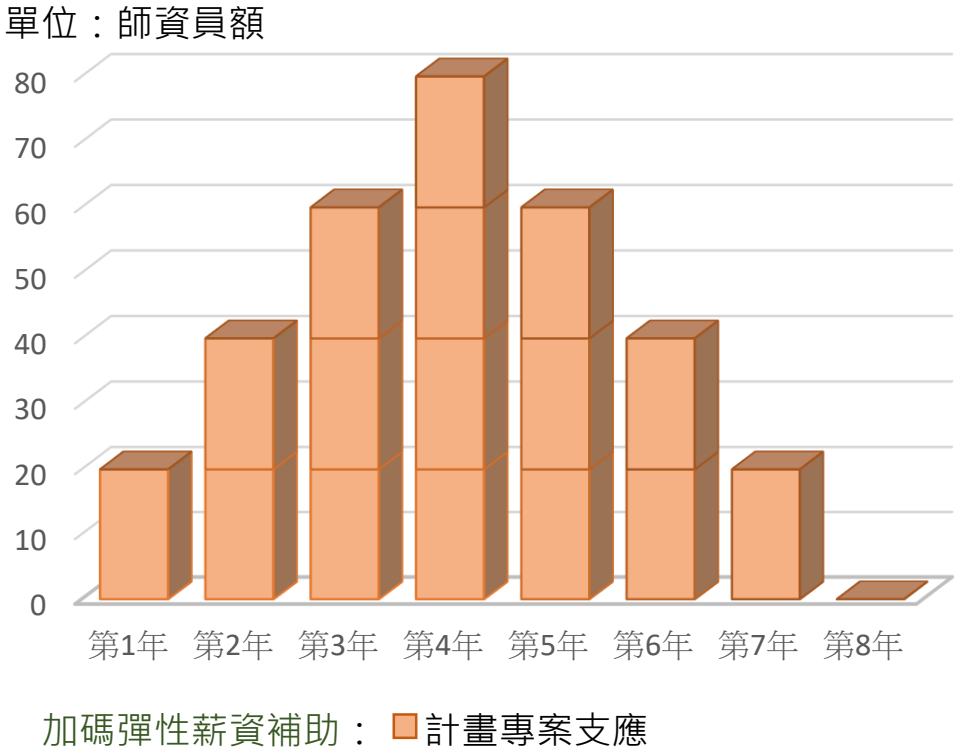
**措施**

| 驅動資安師資生態系統 | 設立資安卓越中心 | 拓展資安教學實習場域 |
| --- | --- | --- |
| 擴增資安師資員額 | 推動資安前瞻研究 | 大學區網中心 |
| 延攬國際頂尖師資 | 培育資安高端人才 | 大型攻防演練場域 |
| 培養資安種子師資 | 深化國際合作交流 | 政府開放場域 |

# 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

# 1-① 專案增加師資員額




- 仿矽導計畫增加師資員額
- 共增聘80名編制內專任教師，分4年補齊
- 加碼彈性薪資補助

邀請國內外國際一流資安競賽團隊、業師、學界和社群知名人士，並提供優渥薪資待遇，以延攬頂尖高階研究人員擔任資安師資，鼓勵大專校院與國內外產業及學研機構競逐優秀資安人才，以利學校培育資安專業人才並維持教學品質。

1. 以4年為期，每年以核撥15名預算員額為上限，4年累計60名。
2. 大學每提撥1名預算員額，教育部搭配提供3名預算員額。
3. 另為賦予學校彈性，學校提撥員額第1年得以專案教師替代。
4. 先借後還，於第5~8年起逐年平均歸還員額。
5. 加碼彈薪補助，政府補助每名師資，每年最高以120萬元為度。

# 1-② 開放學術區域網路中心、政府網路等場域供實習、實戰用

## 學術場域

### 資安實務課程搭配區網中心以奠基資安基礎

- 透過大學區網中心與大學資安實驗室，提供「教學實驗主題」與「實習場域(實體/虛擬)模式」及「結合大學資安系所教研課程」三面向，將區網或實驗室網路擬真情境，融入教學實習並進行研析或攻防演練，養成資安實務人才。(第1年建置2所區網中心為資安教學實習場域，後續評估擴大)

## 政府場域

### 開放政府網路或應用系統場域以培育實戰人才

- 提升GSN骨幹網路惡意行為資料分析能量，並開放為研訓場域
- 建立政府開放場域營運制度及威脅情資分析索引系統，
- 建置政府開放場域可模擬機關網路環境與應用系統之實驗場域

# 2-① 發展國家任務導向型及關鍵(核心)資安型前瞻研究

- 國家任務導向型研究
  - 以提供政府機關短中期所需之應用技術研究為主，包括技術面(如主動式防禦技術、惡意攻擊溯源追蹤、弱點挖掘自動化、駐外館處之安全網路通訊技術、5G政府網路之資安防護架構等)及政策面(如跨國網路戰之國際法規研究、平戰轉移等)議題。
- 關鍵(核心)研究
  - 屬長期性基礎型研究，以發展國防、國安之關鍵技術及研究為主，如量子與後量子密碼技術，人工智慧資安攻防技術、暗網攻防技術、零時差弱點研究及解決方案(含關鍵基礎設施系統)等。

# 2-② 深耕學術型資安研究

- 開發軟體資安技術(Security in Air)
  - 針對 5G(B5G)、CI、IoT 與 AI 等相關應用潛在威脅，開發對應前瞻資安防護
  - 開發先進資安技術與防護機制，培育資安研發人才，建立資安研發自主能量
  - 研發成果擴散產業界，帶動國內資安產業發展
  - 建立資安技術自主創新，提高資安研發人才供給， 帶動資安產業升級，推動資安產業聚落與生態系的形成與發展
- 開發硬體資安晶片(Security on Chip)
  - 即時掌握最新國際規範並參與國際競賽及提案
  - 透過 PUF 技術以加強晶片安全防護
  - 開發基於安全設計的 EDA 工具與環境
  - 針對各式旁通道攻擊提出防禦機制
  - 應用國際開源的晶片安全框架技術
- 每年預計開發10項資安技術或機制

# 2-③ 跨國人才交流與研究合作

- 強化與先進國家資安研發機構合作關係，合作對象以美國、歐洲及澳洲等國家級或以資安著名之研究機構為合作對象，每年對接1家國外技術或研究機構，跨國人才交流至少達15人次，初期不排除以鎖定資安重點學校，後續逐步擴展至國家實驗室或標準制定機構等方式辦理
- 積極展現臺灣資安實力，提升我國資安領域能 見度，掌握國內外資安技術發展趨勢與領先地位，於111年起參與國際組織進行資安標準制定、112年起辦理大型國際學術會議發表研究成果
- 培育具有國際視野與研發技術之高階人才為目標，並積極推動科技外交，經營跨國人才培育的合作夥伴關係。

# 3-① 培育在學、在職及政府資安人才

- 在學資安人才：透過實務課程、導師輔導及國際合作等策略，連結產業實務場域，每年至少發展1門跨域資安實務課程，且養成資安實務人才達1,000人次。
- 在職資安人才：每年選取2項主軸產業，結合產業、公協會等單位，持續推動短中長期培訓課程，培養具備相關資安專業訓練及應用之人才，加速產業提升資安人才能量。
- 政府資安人才：前3年每年完成2個資安職能構面訓練課程開發，預計累計完成6個構面，精進政府資安職能培訓框及資安職能藍圖。另建立調訓機制，培訓政府機關專職人力，4年累計完成200人次以上。

# 3-② 培育實戰型之頂尖資安人才

- 擇優挑選產學政軍之人才進行培訓，透過「以戰代訓」之理念，定期密集針對不同模擬場域進行實戰演練，提升學員實戰經驗，完訓獲得較優渥之就業機會，並做為國家緊急需調用人力之後盾，長期招收對象將擴及亞太地區。
- 結合關鍵基礎設施場域建置，開發相關實戰訓練教材，前2年建立「引進國外頂尖資安實戰課程機制」，第3年建立自主頂尖資安實戰課程。
- 邀請國內資安國際競賽得獎團隊培訓國內實戰人才，前2年至少100人次，後2年至少250人次。

# 策略二

# 推動公私協同治理
# 提升關鍵設施韌性

# 策略二推動架構

**行政院資通安全處**


1. 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
2. 建構工控領域資安治理成熟度
3. 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. 建立公私合作推動機制
2. 制定資安防護基準及資安防護規範
3. 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. 落實執行資安防護基準及資安防護規範

# 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 公私合作共同制定及推動資安防護規範
   - 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

# 1. 建立各領域公私協同治理運作機制

① 公私合作共同制定及推動資安防護規範：

- 各關鍵基礎設施主管機關依據領域獨特性訂定資安防護規範(或遵循資通安全法之資通系統防護基準)，並推動資安等級A、B級之關鍵基礎設施提供者(CI)提供者逐年導入並落實辦理

② 推動落實關鍵基礎設施資安防護基準：

- 各關鍵基礎設施主管機關每年檢視一定比例之CI提供者有無落實相關應辦事項及防護基準，並稽核資安維護計畫實施情形

③ 建構工控領域資安治理成熟度：

- 行政院院資安處訂定工控領域資安治理成熟度評估機制相關標準文件，同時辦理教育訓練及持續宣傳，持續擴大推動範圍，預計4年後推動所有A級CI提供者工控資安治理成熟度達第3級以上(部分CI領域可視實際情況調整推動數量)

④ 推動國家層級資安風險評估：

- 行政院院資安處將訂定國家層級資安風險評估機制相關標準文件，預計3年內擇取數個A或B級以上CI提供者，導入國家層級資安風險評估機制，第4年彙整各CI領域評估結果，完成我國資安風險地圖

# 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：

- 推動CI提供者設置資通安全長，由機關(構)首長指派副首長或適當人員兼任，負責推動及監督機關(構)內資通安全相關事務；並研議建立領域專家資料庫，包含退休人員及廠商等
- 各領域CI主管機關逐步規劃資安職能訓練課程並培訓其人員，針對課程及訓練內容應加強實務操作，如針對資安事件進行根因分析並研析適切應變策略

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：

- 行政院資安處協調相關機關並遴選模擬場域範疇，規劃每年建置一套CI模擬場域，主要用以納入資安情境進行教學訓練、辦理國內大型攻防演練、結合國際資安攻防競賽等，並設置攻防技術檢測實驗室，每年培訓學員達20人次

# 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)：

- 評估政府領域資安監控成效，提升政府領域資安監控有效性
- 訂定符合國際最新標準之通報單交換格式，將資安事件資訊快速轉化應用分享，縮短通報應變處理與情資整合時效
- 各CI主管機關提升情資分享(ISAC)、通報應變(CERT)、資安監控(SOC)之會員數量及精進情資分享/事件聯防/事件關聯之機制，提升其質化及量化效益，並強化橫向分享交流

② 定期於場域進行公私聯合攻防演練：

- 各領域中央目的事業主管機關應每年至少遴選1個CI提供者辦理進行攻防演練，或是結合國土辦所辦理之演練
- 將熟悉機關網路環境之廠商，納入機關網路攻防演練團隊之可行性，以強化演練成效

③ 辦理關鍵基礎設施跨領域攻防演練：

- 行政院院資安處規劃，每兩年辦理一次跨領域關鍵基礎設施資安防護演練，建立跨領域規模之資安事件處理作業流程、通報應變程序及聯防機制

# 策略三

# 善用智慧前瞻科技
# 主動抵禦潛在威脅

# 策略三推動架構

## 網路攻擊狙殺鏈(Cyber Kill Chain )

攻擊階段

**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。

防禦策略

**推動政府大內網及資安防護向上集中**

**建立資訊系統弱點之主動發掘、通報及修補機制**

**整合國內外情資來源，並深化國際合作**

**發展主動式防禦技術，完善GSN防禦深廣度**

**提升科技偵查能量防制新型網路犯罪**

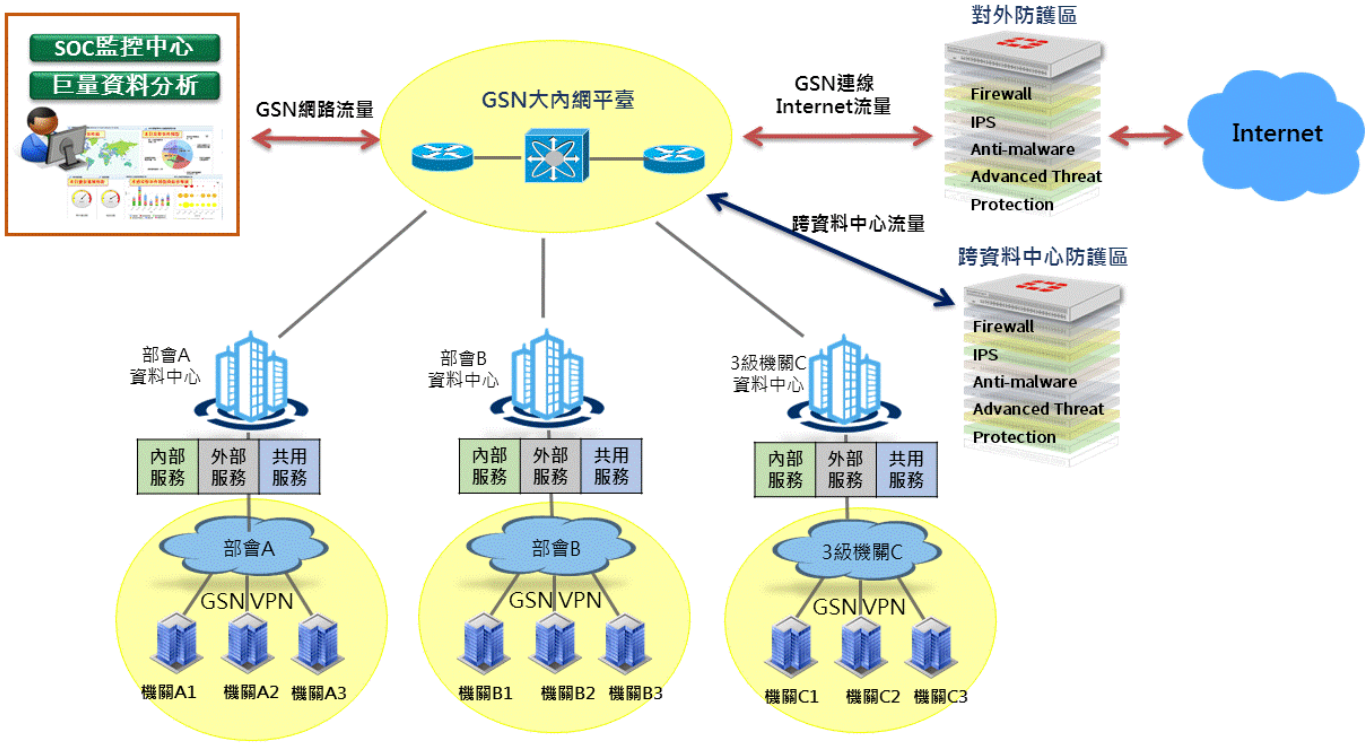
強化新型網路犯罪偵防能量、提升資安事件溯源追蹤能力、加強跨境網路犯罪偵查機制。

# 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 建立資訊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

# 1-① 推動政府大內網及資安防護向上集中

- 提供全GSN機房具備SDN網路架構，並完成所有中央2、3級機關網路集中出口。
- 完成惡意郵件與網路威脅誘捕向上集中偵蒐機制規劃，接續每年推動2個機關導入，配合資訊資源向上集中，強化政府大內網之主動防禦能量，及時阻擋惡意攻擊。



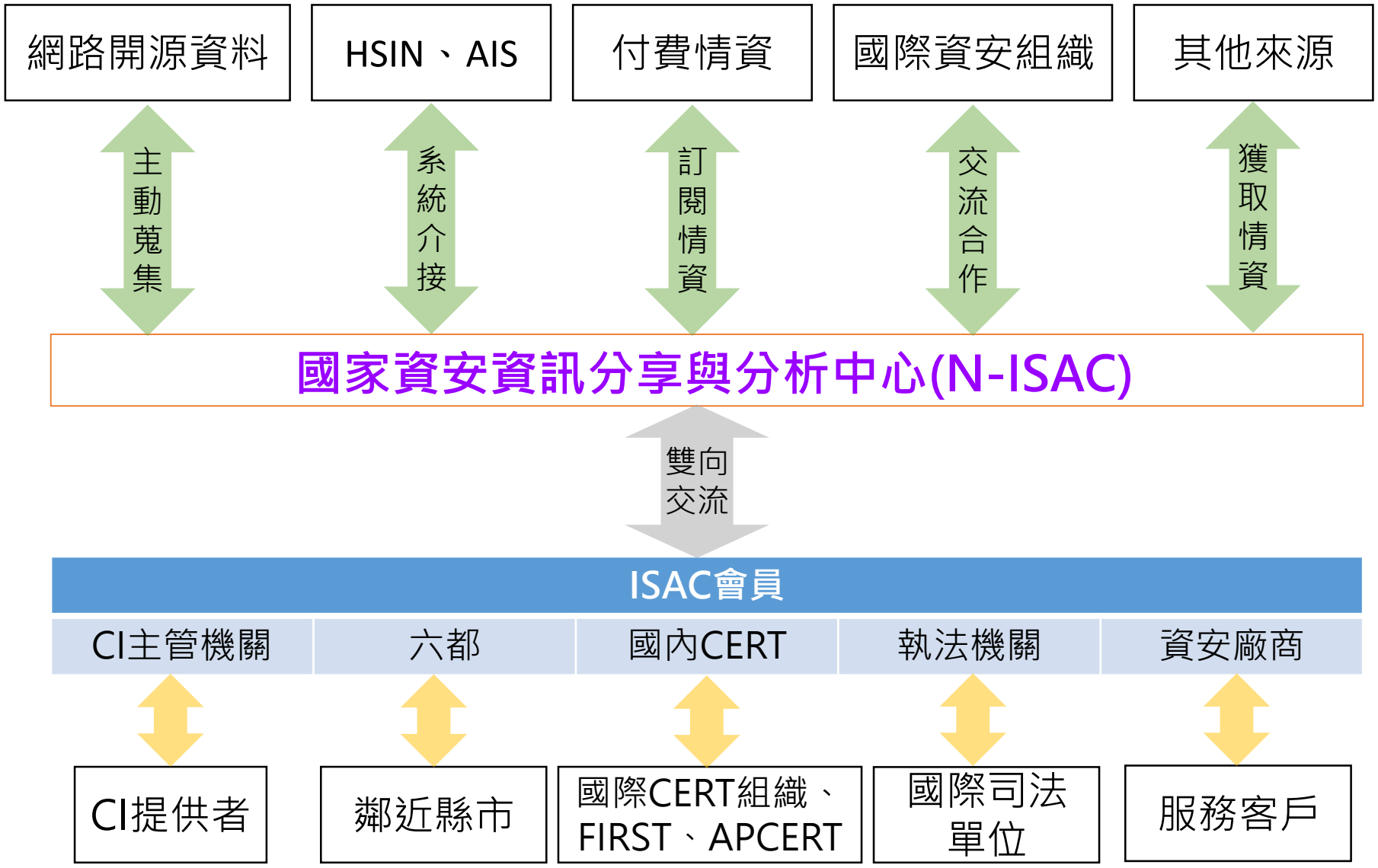
# 1-② 建立資訊系統弱點之主動發掘、通報及修補機制

- 結合資訊資產管理與弱點管理，掌握整體風險情勢，降低重大弱點爆發時可能造成之損害，逐年導入公務機關及CI提供者，預計完成C級以上機關全數導入
  - 定期蒐集主機與電腦所使用之資訊資產項目及版本，建立資訊資產清冊，以達降低風險與管控成本等目標
  - 將資訊資產清單與弱點資料庫比對，以掌握所使用之資訊資產是否存在已公開揭露之弱點資訊

# 2-① 發展主動式防禦前瞻研究及技術應用

- 國際間近年持續發展主動式防禦，同時研究開發網路攻擊的偵測及分析，譬如誘使攻擊者入侵模擬政府機關或企業等組織之網路，以掌握攻擊活動狀況。
  - 完成自動開源情資搜集分析技術，建置異質來源威脅特徵情資之知識圖譜。
  - 建立可行動型情資萃取雛形系統，整合靜態特徵分析、動態行為分析、威脅誘捕(Honeypot)分析技術等主要情資
  - 導入至少1個場域建立示範應用，並發展異質場域智能聯防技術，支援重點領域(如：政府、醫療、金融等)至少2家廠商，建立主動式防禦資安解決方案。
  - 研發技術扶植自主研發產品，帶動國內資安/系統整合廠商，達到至少10億元產值；並建立1套AI Security協作產業標準。

# 2-② 整合國內外情資來源，並深化國際合作(1/2)



# 2-② 整合國內外情資來源，並深化國際合作(2/2)

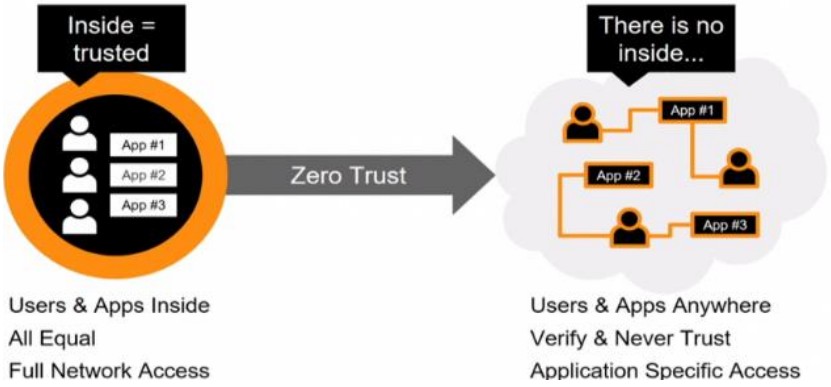
- 發展N-ISAC成為國內最大情資綜整平臺，並整合國內外情資來源，提升威脅情蒐與主動偵測能量：
  - 完成國際情資交換格式STIX 2.1與MITRE ATT&CK框架導入規劃 ，並協助國內各領域ISAC完成系統與資料轉換。
  - 比對分析國內外資安情資與威脅，並提供2種「開放情資」予學研單位或國際資安組織參考
  - 持續擴展並深化情資內容，收容亞太區共通性資安情資；並強化國際情蒐合作，增加全球共通性資安情資
  - 分享威脅偵測與分析情資，產製事前重點防護指標，強化N-ISAC主動防禦與聯防機制

# 3-① 應用新興技術淬鍊有效情報，發展主動式防禦技術

- 以主動式防禦思維，透過情蒐研析、縱深防禦、主動防制及溯源阻斷等重點工作面向，強化相關技術研發與應用，以提升政府機關資安防護能力
  - 第1年完成主動式防制機制規劃，且每年實作驗證2套主動防禦情境，4年內累計完成8套主動防禦情境
  - 建立偵測規則部署與回傳機制，並每年選定2個機關試行導入偵測機制

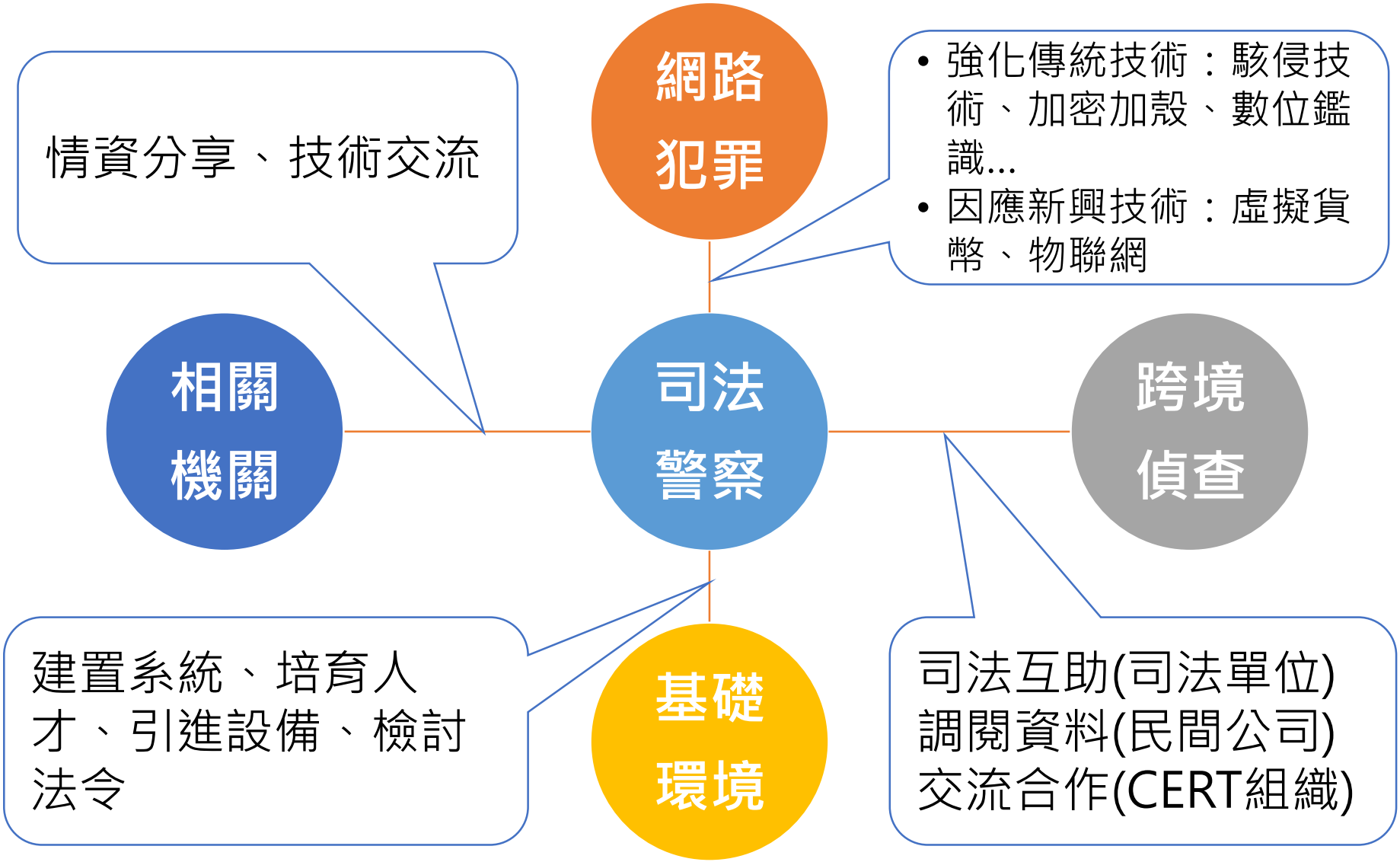
# 3-② 完善政府網際服務網防禦深廣度

- 政府網際服務網(GSN)
  - 強化外網惡意入侵偵測及區域聯防，並提升DNS抵禦攻擊之抗性，以確保DNS資料之「機密性」與「完整性」，及DNS持續「可用性」，全面強化GSN DNS防禦能力。
  - 提升GSN骨幹流量收容達40G，攻擊與受害指標行為可回溯1年，完成GSN骨幹網路威脅情資分析索引系統建置
- 發展零信任網路(zero trust network)
  - 第1年完成零信任網路與概念性驗證機制研究與部署機制，第2年起每年推動2個機關逐步導入零信任網路之身分鑑別、設備鑑別及信任推斷等機制




零信任網路為保護資料/應用存取，且任何資料存取永不信任且必須驗證

# 4. 提升科技偵查能量防制新型網路犯罪(1/2)



# 4. 提升科技偵查能量防制新型網路犯罪(2/2)

① 強化新型網路犯罪偵防能量：

- 分析IoT及中繼站駭侵行為攻擊態樣、防禦機制；加強犯罪偵查技能之實務訓練，提升整體偵防能量；建置資安事件調查模擬平臺，強化警調人員實戰能力。

② 提升資安事件溯源追蹤能力：

- 持續提升數位鑑識能量、強化情資分享及技術交流；分年推動南區建置鑑識實驗室，加速中南部單位取得數位鑑定報告時效，拓展資安鑑識能量；自主研發現場取證工具，並扶植國內廠商共同開發，提升國內鑑識工具研發能量；透過蒐集各單位所得國內情資，比對境外提供情資，找出策動攻擊之來源與駭客組織，以達溯源目的。

③ 加強跨境網路犯罪偵查機制：

- 積極參與各項司法機關、國際資安研討會、建立與國外企業調閱相關犯罪資料窗口，增進跨境網路犯罪偵查管道、技術並促進國際警政情資交換；開發主動式威脅端點獵蒐系統，機先發掘境內潛藏之惡意威脅端點。

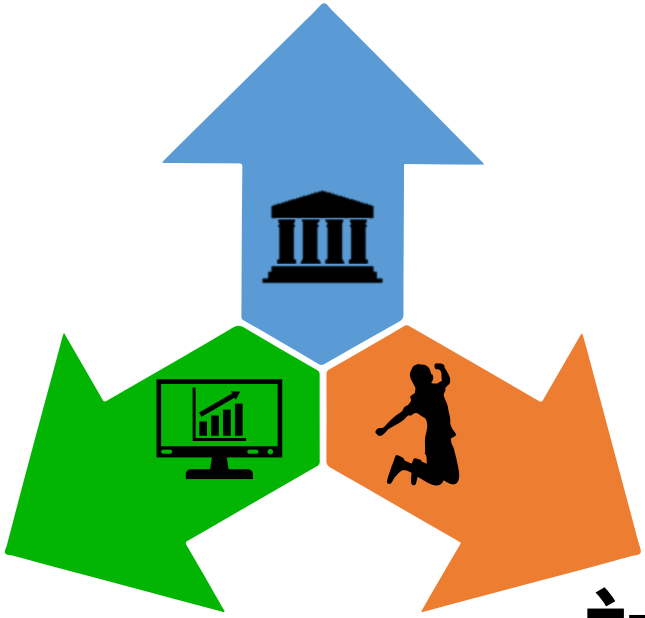
# 策略四

# 建構安全智慧聯網
# 提升民間防護能量

# 策略四推動架構

## 政府機關

落實資安相關法規及標準



## 民間企業

提升整體資安防護
能量及產品競爭力

## 社群個人

提供安全的智慧聯網之
軟硬體及通訊相關環境

# 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 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 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. 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

# 1-① 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

- 由行政院資安處定期檢視「資通安全管理法」及其子法內容，並與公務機關、特定非公務機關及利害關係人等共同檢討法規內容，適時調整以切合我國資安現況及發展所需。
- 每年持續檢視資通安全管理法納管機關之資通安全維護計畫實施情形，並透過稽核進行實地瞭解。
- 適時給予獎勵誘因及折衷懲處措施，落實資安法推動。
- 持續蒐集國際資安相關法規及標準，掌握國際資安發展情勢，確保我國資安能量與國際趨勢同步。

# 1-② 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

- 優化TWCERT/CC資安情資系統及服務，深化我國企業資安事件諮詢及協處服務，每年受理並審核國內企業產品資安漏洞通報10個。
- 建置民間企業之資安情資分享平台，逐年擴大與國內中小企業介接，即時交換資安威脅情資。
- 鼓勵電商(網路零售業者)參與TWCERT/CC，每年輔導至少10家高風險網路零售業者導入資安防護措施，舉辦網路零售資安推廣活動2場，
- 擴大資訊安全宣導，提升民間資安防護能量及意識。

# 2-① 強化委外供應鏈風險管理

- 行政院資安處將協助及輔導各機關辦理委外作業時，加強對委外廠商的管理，具體作法為：
  - 因應新興科技及國際資安威脅情勢，每年完成2份委外管理相關參考文件之檢視或增修訂。
  - 每年遴選10個機關進行實地輔導，落實委外作業安全管理。
  - 每年遴選至少20個以上機關辦理資安稽核，加強檢視委外管理制度。
- 由行政院資安處強化委外資訊服務廠商資安管理能量。

# 2-② 聚焦資通訊晶片產品安全性

- 研發半導體及資通訊供應鏈在製程前後階段之晶片檢測技術，並技術轉移國內廠商，帶動設備與其供應鏈國產化發展
  - 制定晶片安全檢測規範1份及晶片安全相關指引10份
  - 研發晶片資安檢測工具(如惡意邏輯威脅、旁側道攻擊檢測與模糊測試等)，並協助國內晶片業者進行晶片安全檢測工具場域實證，以解決晶片潛藏資安風險問題
  - 成立國際認可晶片資安檢測實驗室，補強國內晶片檢測技術缺口與檢測環境生態系，減少國內產品外銷的資安合規障礙
  - 提供國際物聯網平台安全標準(PSA或SESIP)等測試服務，達成產品國內檢測，檢測結果受國際承認至少1案

# 3-①健全新世代行動通訊技術網路安全

- **法規標準**：建置5G SA網路及MEC系統、5WWC及非公眾網路架構、5G端到端之控制面控制信令與用戶面資料傳輸、5G與低軌道衛星通訊匯流之資通安全檢測實驗室與監理能量，以修訂「5G資通安全維護計畫」稽核計畫及標準作業程序文件，將其納入資安防護範圍。
- **技術研發**：建立兩大平台，5G「軟體整合開發暨運作程序(DevOps)」及「軟體系統」資通安全分析及檢測平台)，透過5G網路軟體系統及應用程式安全性研析，提供業者相關評估、測試及驗證服務。
- **場域實證**：引導建構5G垂直應用發展環境，前2年推動智慧教育、公共安全或其他垂直場域實證，後2年研析國內外發展智慧工廠、智慧醫療等相關政策、案例與數位轉型議題。

# 3-② 推動物聯網合規驗證及場域實證

- **法規標準：**
  - 每年制(修)訂1項以上物聯網設備或通傳事業使用之資通設備資安檢測產業標準或技術規範(通傳會)。
  - 協助國內法人及資通訊廠商參與5G、IOT、車聯網及其資安相關國際標準制定，每年提出2件技術貢獻爭取納入國際標準，並與NIST進行標準資訊交流，促進我國資安技術與國際接軌(經濟部)。
- **場域實證：**每年建立1項指標應用示範展示場域，涵蓋至少2項次資安技術或產品應用，協助強化智慧聯網製造業之資安防護能力。
- **推動領域應用之資安解決方案**：加速物聯網資安解決方案落地與商用化，擴大產業資安應用規模，鎖定國內優勢產業(如半導體、物聯網)，並參考國際標準，據以推動具備國際競爭力之資安解決方案，及輸出國際市場。

# 大綱

- 國際資安威脅及政策趨勢
  - 國際資安威脅
  - 國際資安政策趨勢
- 第5期國家資通安全發展方案成效
- 問題評析
  - 分析SWOT及應對策略
- 下期方案藍圖
  - 願景、目標、策略、具體措施
- 宣導事項

# 宣導事項

- 本院資安處前於109年3月上旬調查7,292個公務機關有無使用或採購中國大陸廠牌資通訊設備，經統計分析各公務機關使用大陸設備之用途，可概分為智慧型手機、影像攝錄設備、無人機及網通設備4類。
- 各界都相當關心本案，為了降低機關資安風險，同時也為了避免外界疑慮，請各上級機關督促其所屬儘速汰換；另未達使用期限者，亦應儘速訂定汰換期程，在未汰換之前，應列冊管理，並禁止與公務網路環境介接，對於影像攝錄設備及無人機並應關閉對外連網功能。
- 另，本院資安處後續也會將前揭使用大陸設備之機關將優先納為稽核重點對象，並檢視其設備汰除及管理情形，請各(中央及地方)機關應依資通安全管理法規定稽核所屬機關，並將所屬機關使用大陸設備情形納為稽核重點。


# 資安是持續精進的風險管理