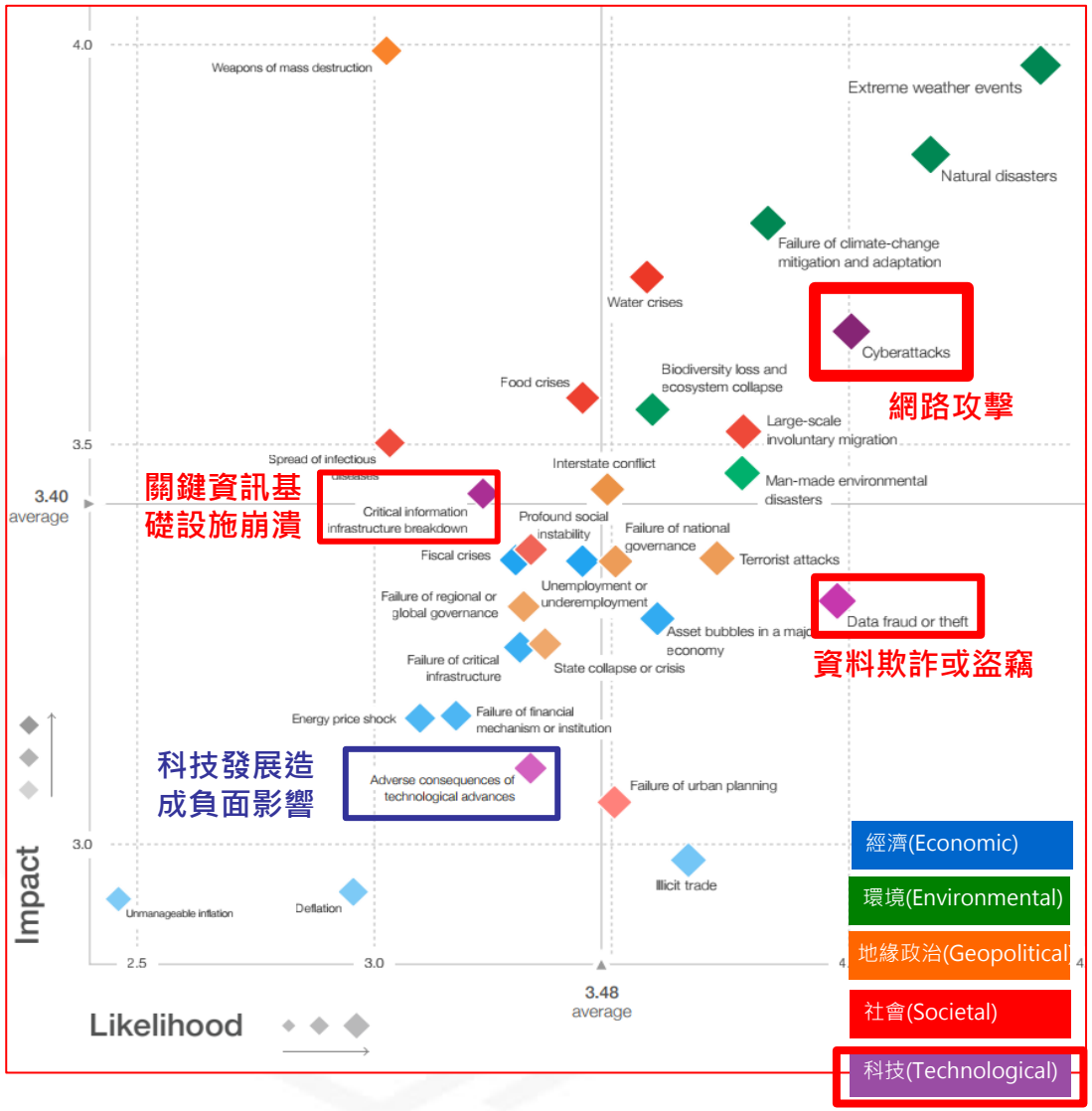
從全球數位領土之防禦
談我國資安聯防機制之規劃

行政院國家資通安全會報技術服務中心

吳啟文主任

107年3月30日

世界經濟論壇2018全球風險調查報告



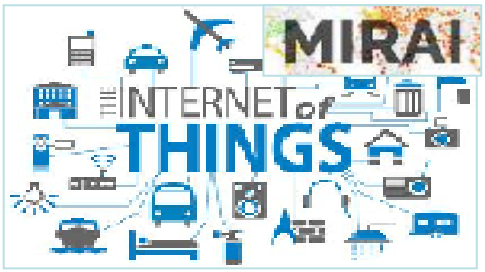
10大可能風險

1. 極端氣侯
2. 自然災害
3. 網路攻擊(同時為第6大影響風險、2017年排名第6)
4. 資料欺詐或盜竊(2017年排名第5)
5. 氣候變化調節與適應機制失效
6. 大規模非自願移民
7. 人為環境災害
8. 恐怖攻擊
9. 非法貿易
10. 主要經濟體的資產泡沫化

全球資安威脅趨勢

進階持續威脅攻擊竊取機密資料

分散式阻斷服務攻擊癱瘓網路運作



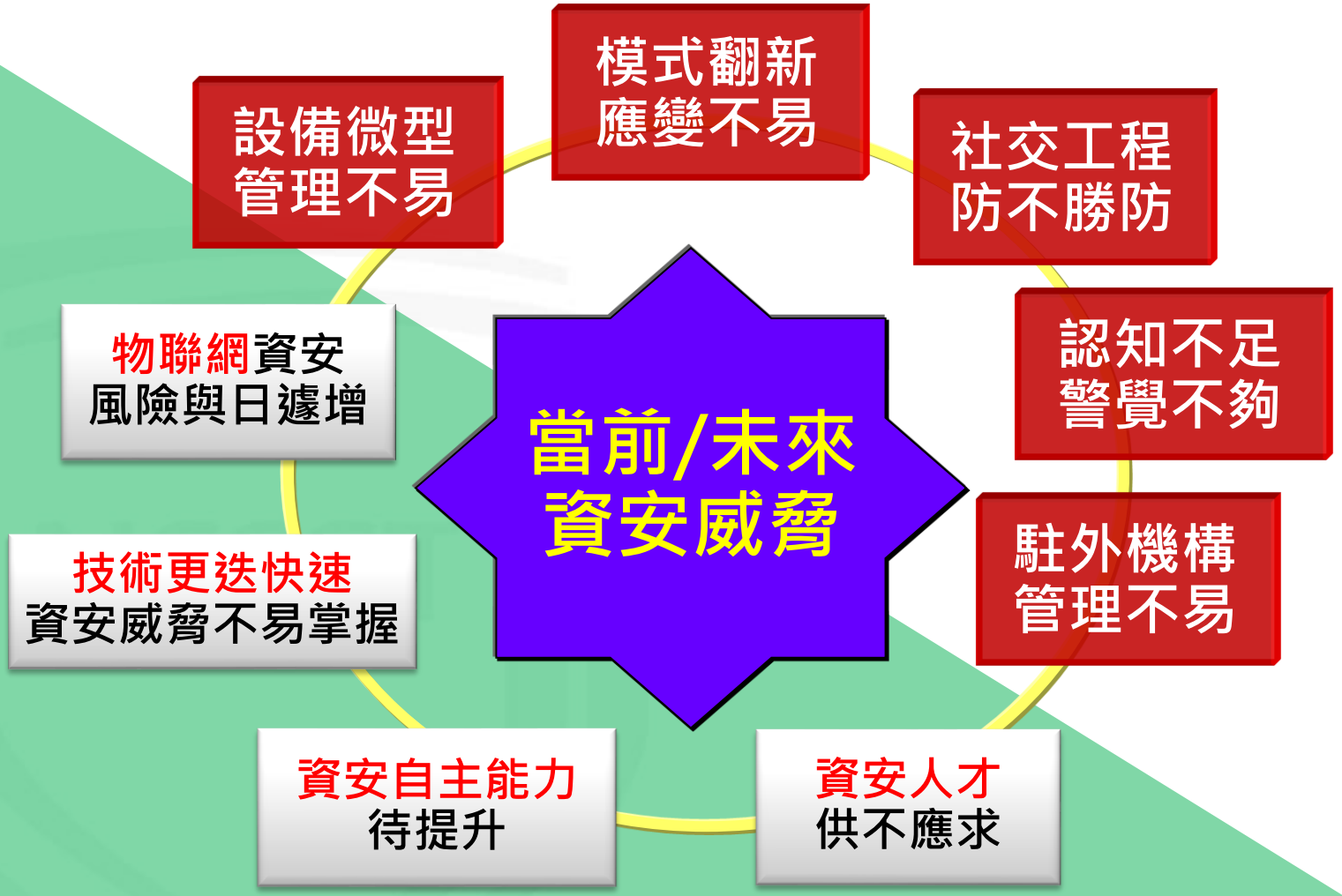
物聯網設備資安弱點威脅升高

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

政府資安威脅趨勢


當前/未來
資安威脅
模式翻新
應變不易
社交工程
防不勝防
認知不足
警覺不夠
駐外機構
管理不易
資安人才
供不應求
資安自主能力
待提升
技術更迭快速
資安威脅不易掌握
物聯網資安
風險與日遽增
設備微型
管理不易

我國資安發展藍圖(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

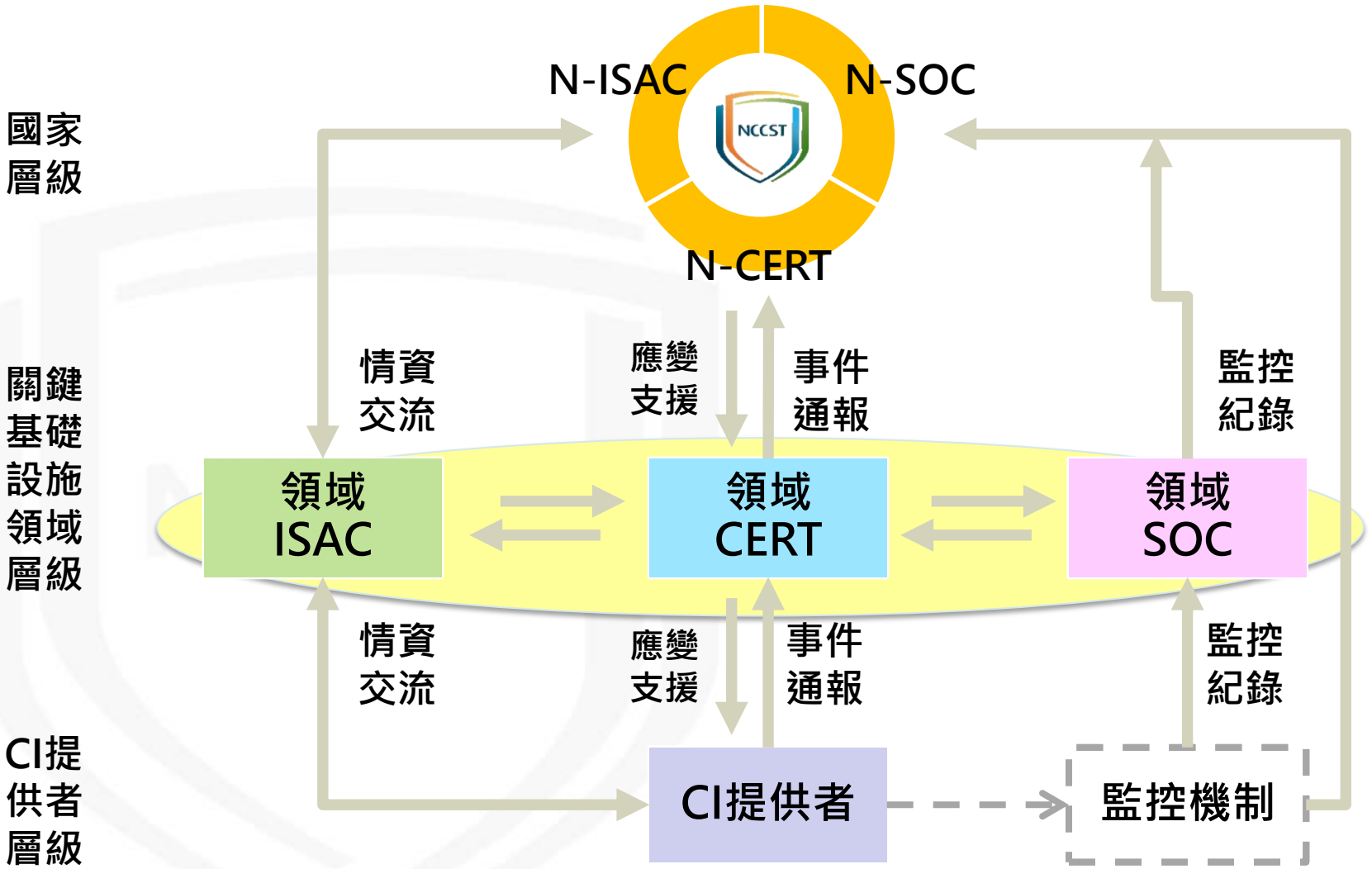
推動策略

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

CIIP防護運作架構


國家層級
關鍵基礎設施領域層級
CI提供者層級
N-ISAC
N-SOC
N-CERT
情資交流
應變支援
事件通報
監控紀錄
領域ISAC
領域CERT
領域SOC
情資交流
應變支援
事件通報
監控紀錄
CI提供者
監控機制

資安情資分享

- 鑒於國內外資安情資來源漸趨多元，跨領域情資日益增加，需建立更有效之**國家層級的N-ISAC**(National ISAC)運作機制，打造**資安情資聯防網路**

N-ISAC

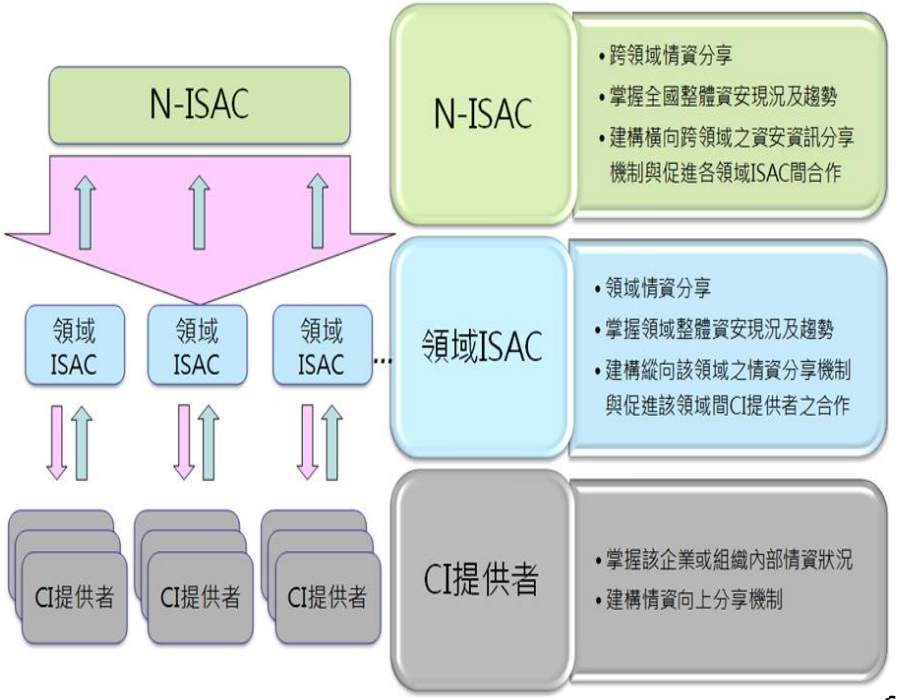
N-ISAC
(107年1月由G-ISAC升級)

情報分享

國內八大CI領域

能源　政府機關　金融　高科技園區

交通　水資源　醫療　通訊傳播



N-ISAC公私協同合作

強化國內資安領域彼此鏈結與交流

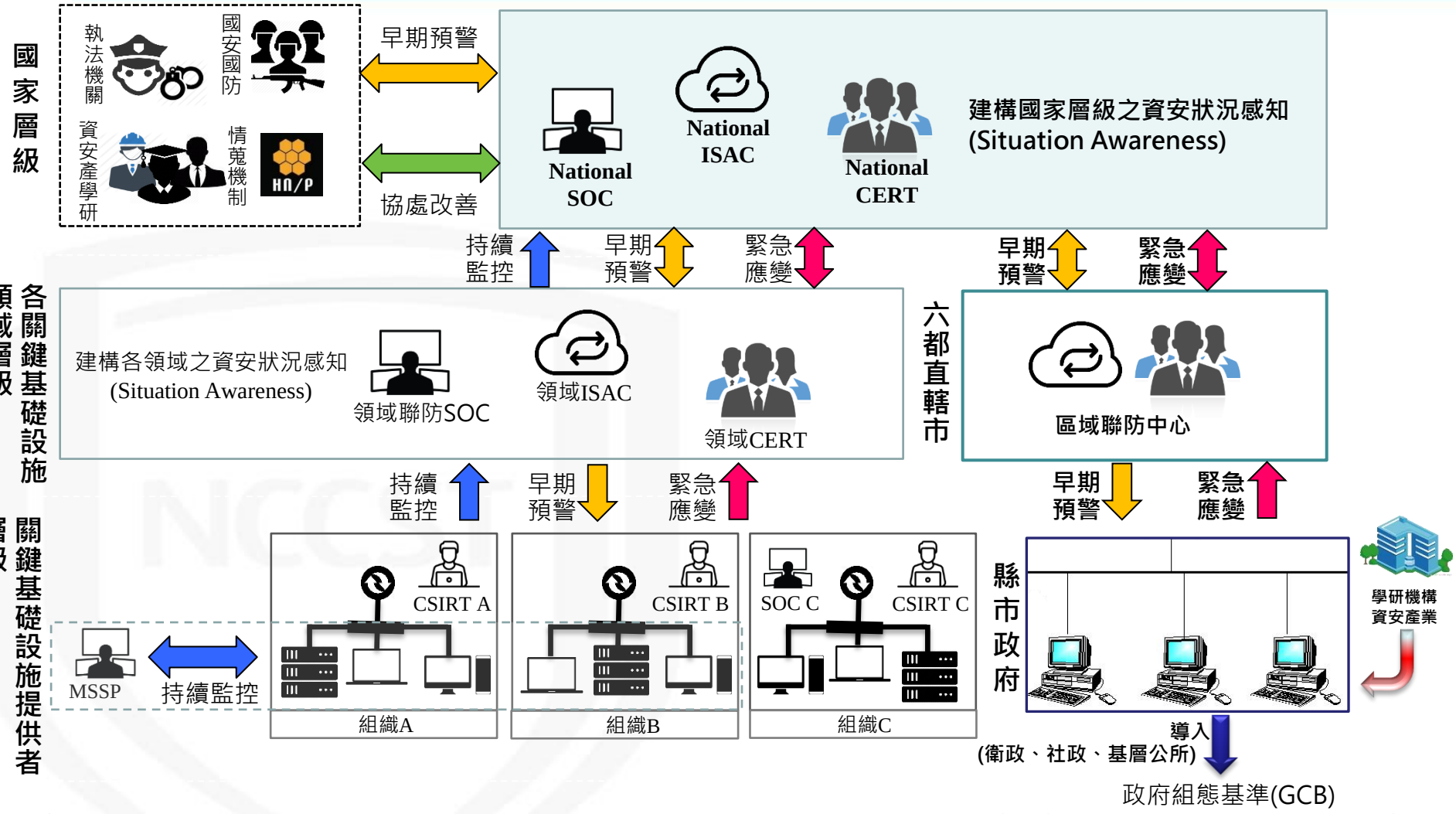
- 橫向情資分享與應變防禦
- 促進公私協同合作

即時傳遞情資訊息

- 資安威脅情資
- 中繼站阻擋名單
- IoT設備防護情資
- 工控設備防護情資
- 國際網路犯罪情資
- 安全防護參考文件

多元化情資來源

建構國家資安聯防體系


國家層級
執法機關
國安國防
資安產學研
情蒐機制
早期預警
協處改善
National SOC
National ISAC
National CERT
建構國家層級之資安狀況感知
(Situation Awareness)
持續監控
早期預警
緊急應變
早期預警
緊急應變
各關鍵基礎設施領域層級
建構各領域之資安狀況感知
(Situation Awareness)
領域聯防SOC
領域ISAC
領域CERT
六都直轄市
區域聯防中心
持續監控
早期預警
緊急應變
早期預警
緊急應變
關鍵基礎設施提供者層級
CSIRT A
CSIRT B
SOC C
CSIRT C
縣市政府
學研機構
資安產業
MSSP
持續監控
組織A
組織B
組織C
導入
(衛政、社政、基層公所)
政府組態基準(GCB)
資安旗艦建設：強化國家資安基礎建設
前瞻基礎建設：強化政府基層機關資安防護及區域聯防計畫

報告完畢
敬請指教