永遠走在最前面
Always Ahead

網路攻擊防禦機制經驗分享

Cyber Security Experience Sharing

中華電信數據通信分公司
林奕翔

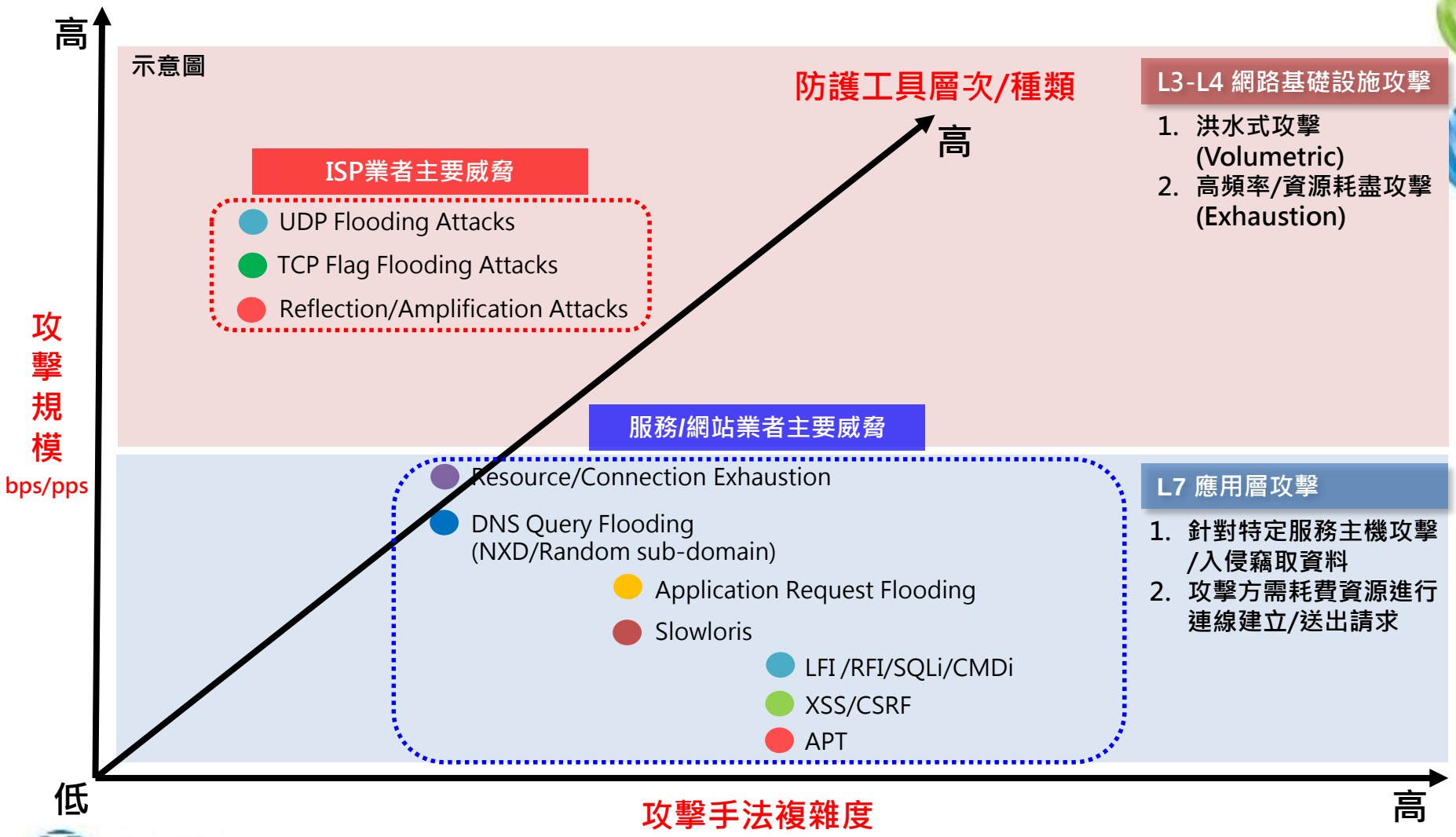
2018年06月22日

中華電信
Chunghwa Telecom

大綱

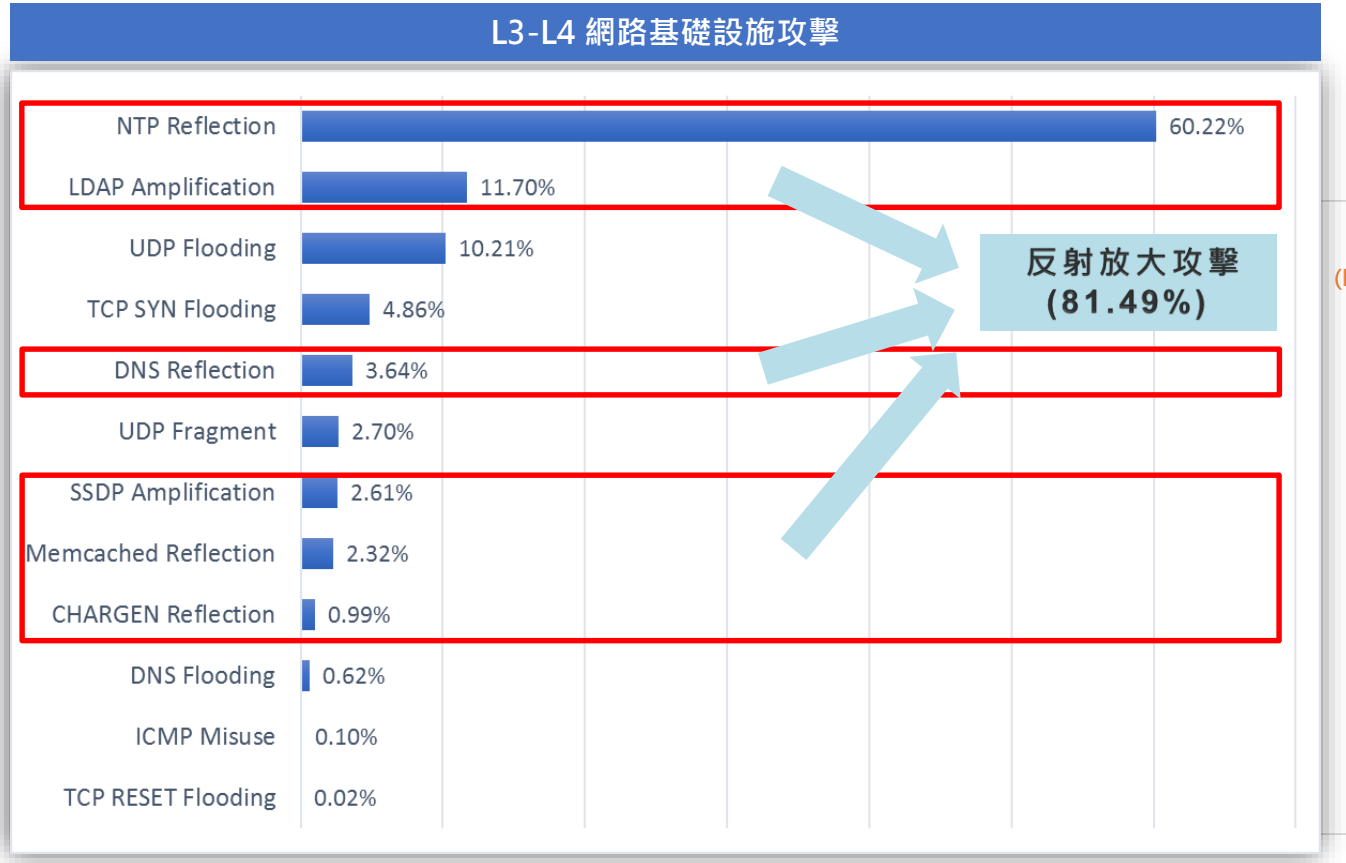
- 網路攻擊事件手法/分類
- DDoS事件觀察
- 多層次資安防護機制
- 資安防護週期

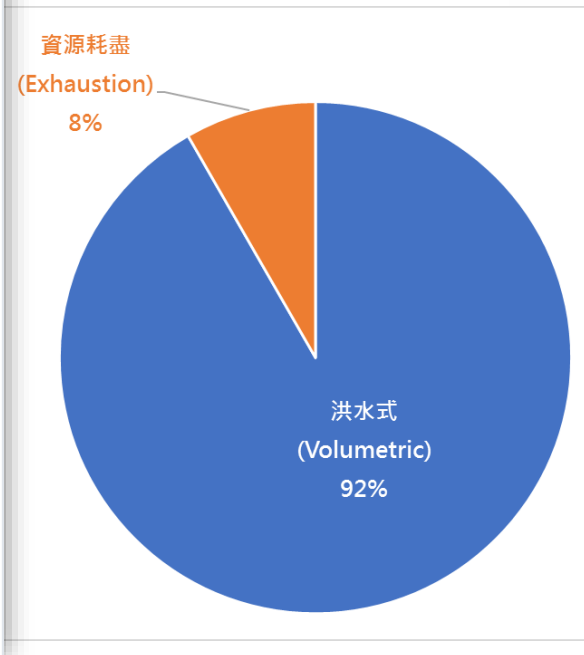
網路攻擊事件手法/分類



中華電信 Chunghwa Telecom

DDoS事件觀察

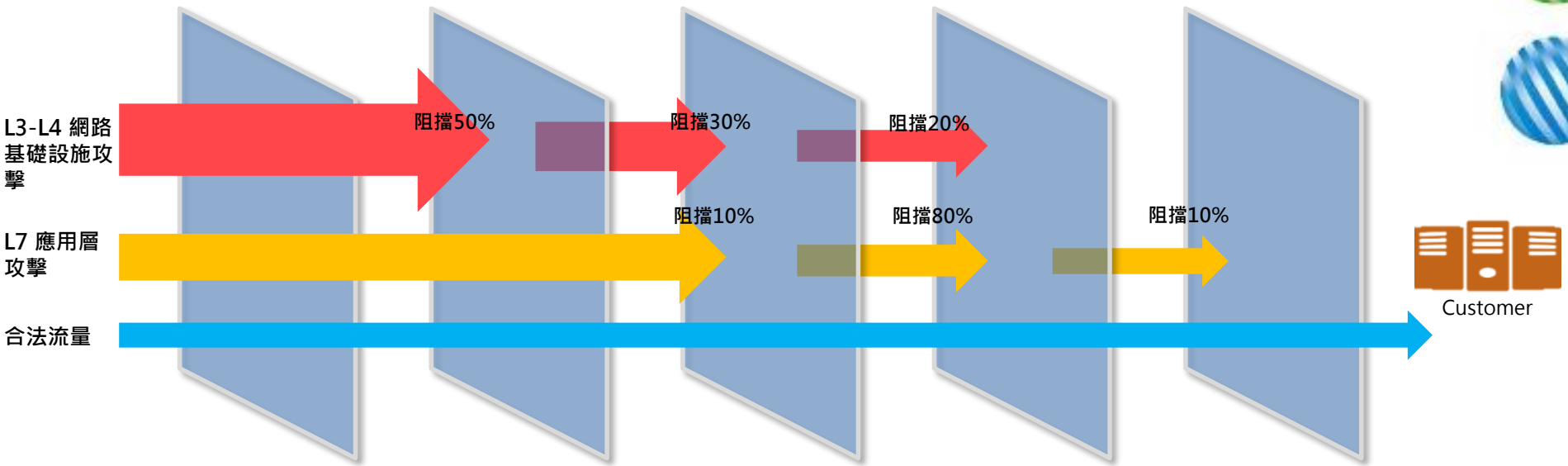




中華電信
Chunghwa Telecom

多層次資安防護機制(1/2)

示意圖



異常流量分析

- 自動偵測
- 封包內容合法性
- 流量使用異常性

ISP間的合作

- 情資交換
- RTBH
- Blackhole

網路端防護

- Flowspec
- Black list/ ACL
- White list
- 特區管制

資安防護設備

- 清洗中心
- IPS
- WAF
- NGFW

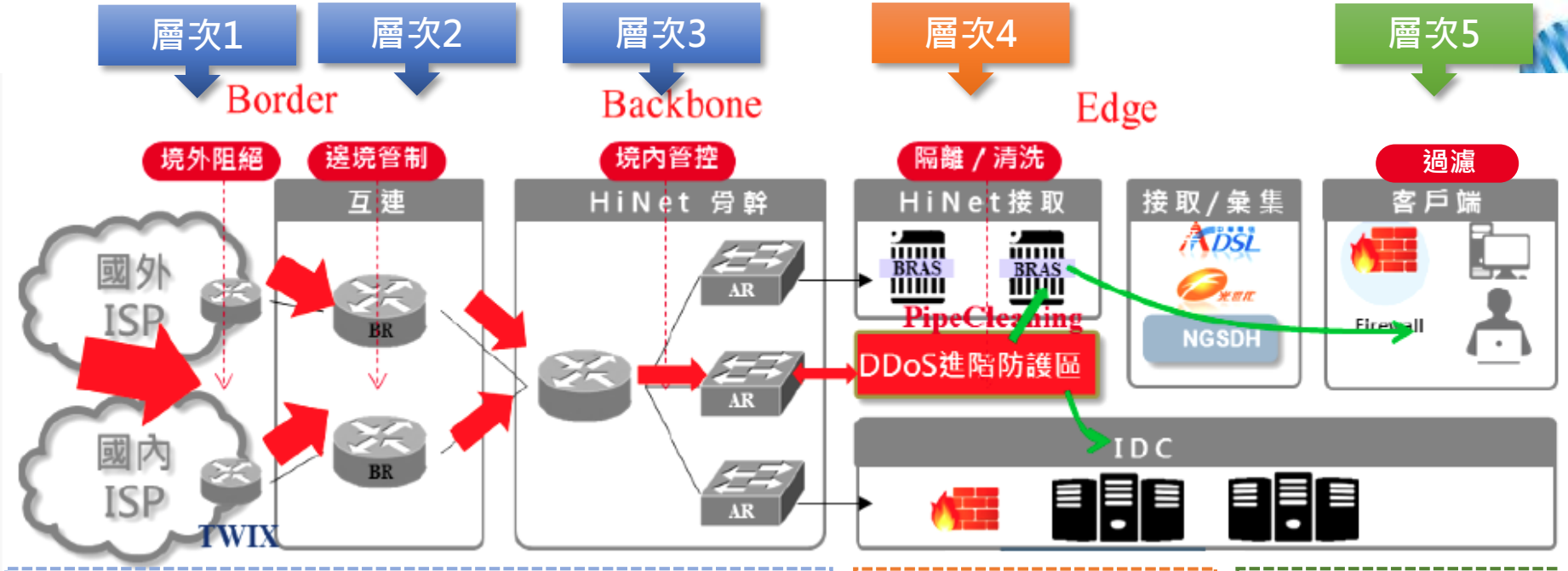
終端防護

- EDR
- 防毒/防駭軟體
- Threat Intelligence
- 定期更新

參考資料來源：IPServerOne/NEXUSGUARD

多層次資安防護機制(2/2)

- 多層次縱深防護架構：阻擋/隔離/清洗/過濾



若遭受大規模DDoS滿頻攻擊，透過Border網路的境外阻絕和邊境管制，將攻擊封包阻擋在境外，如果攻擊進入骨幹(Backbone)，將再進一步阻擋與限頻，免於網路癱瘓的威脅

利用專屬網路/資安設備，清洗或隔離攻擊訊務

過濾流量，阻擋網路入侵/病毒/惡意連線

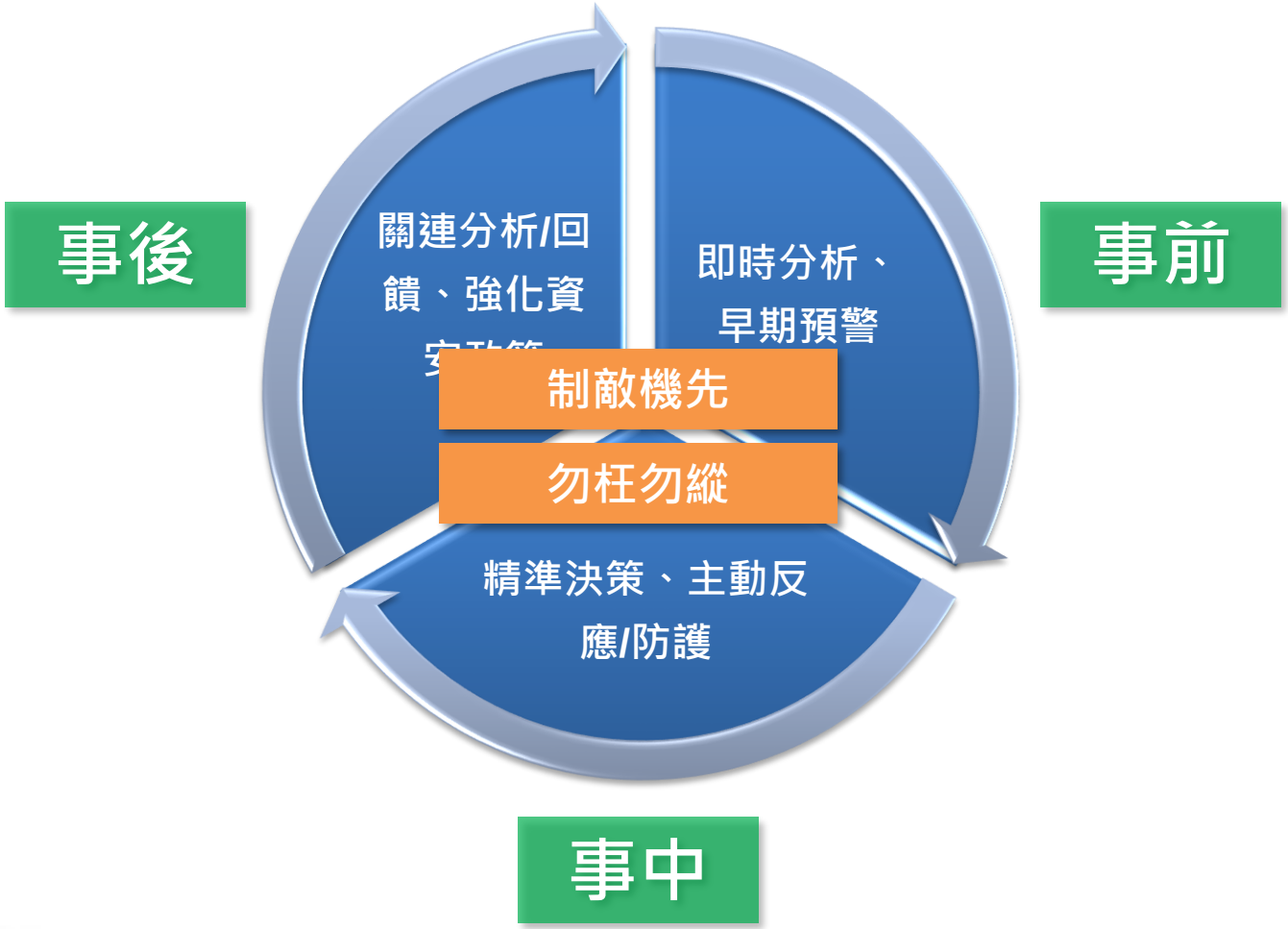
中華電信DDoS防護服務

HiNet新世代防火牆

HiNet SOC監控中心

HiNet入侵防護服務/企業防駭守門員

中華電信 Chunghwa Telecom

中華資安國際

資安防護週期