


聯網車輛之風險監管-美國作法

 楊至善 高級法律研究員
stli 資策會科技法律研究所
113.09

1. 聯網車輛之定義
2. 聯網車輛帶來的國安風險
3. 美國對聯網車輛風險之防範措施

1. 聯網車輛之定義 (1/3)

「聯網車輛¹」相當於裝著輪子的智慧型手機

未來絕大部分車輛都會是「聯網車輛」

通訊技術

專用短程
通訊
DSRC²

蜂巢式
網路

衛星通訊

其他無線
通訊頻段

應用功能

車輛定位

連接智慧
交通系統

附加服務

無線更新

遠端存取/
操控



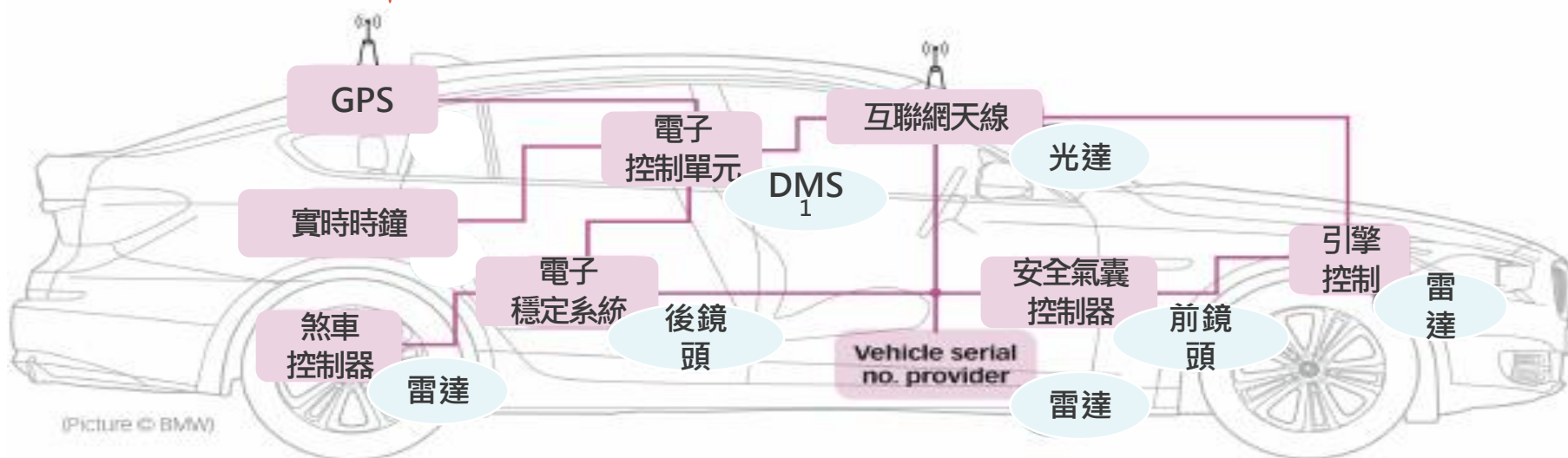
¹ 聯網車輛 Connected Vehicles, CV

² 專用短程通訊 Dedicated Short Range Communications, DSRC

1. 聯網車輛之定義 (2/3)

傳統車輛：引擎、輪子、方向盤

現代車輛：車載電腦、感測器、聯網設備、軟體定義



大量即時資料

現代車輛透過許多感測器大量蒐集車輛內、外部及時資料

特點

對內連結個人裝置

車用系統可連接、存取個人裝置，取得個人資料

對外連結基礎設施

連結網際網路、交通基礎設施、能源基礎設施

¹ 駕駛人監控系統 Driver Monitoring System, DMS

1. 聯網車輛之定義 (3/3)

透過多元技術互聯，帶來安全、疏運、智慧服務等優點

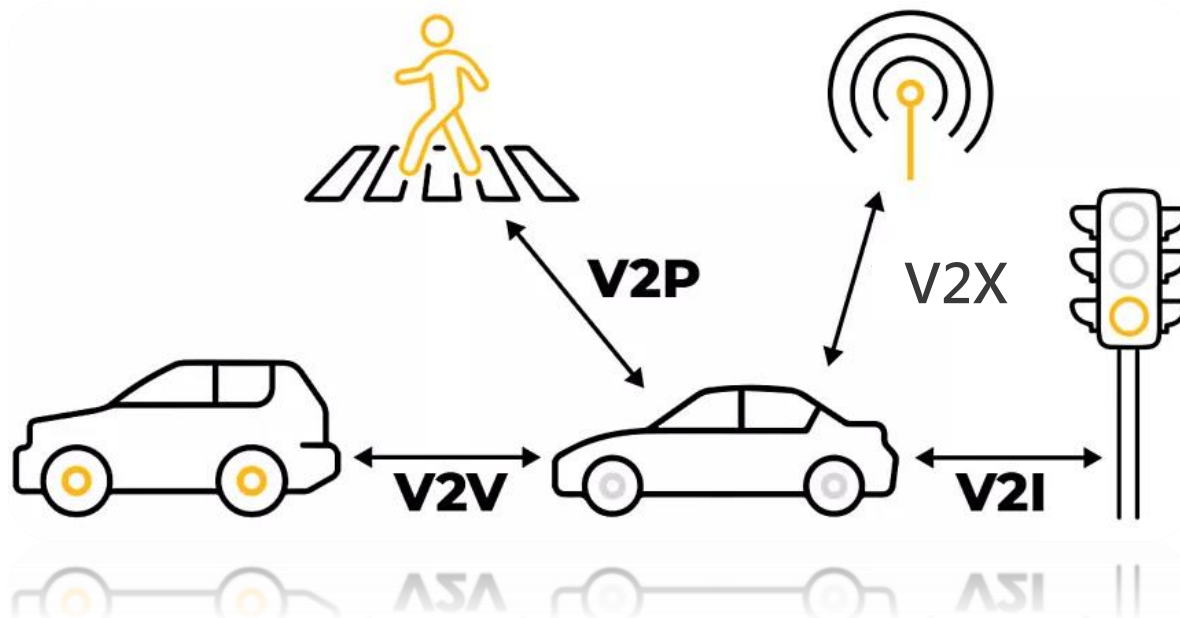
互聯類型

V2V 車對車互聯

V2I 車對基礎設施互聯

V2P 車對個人裝置互聯

V2X 車對網際網路互聯



優點

提升道路安全 製造透視效果，及時同步資訊，保障用路人（尤其弱勢用路人）之安全

舒緩交通壅塞 共享路況資訊、執行列隊行駛、避免多餘的停煞，間接達到節省能源效果

提供多元服務 分享天災警告、連結智慧設施，建構多元服務應用潛力

2. 聯網車輛帶來的國安風險

車輛聯網也帶來安全風險，部分國家已採取管制措施

風險

更多攻擊面向

更密集的網路連結可能提供攻擊面向 (vectors) 與弱點

海外連接與後門

車聯網資料可能直接傳輸至海外伺服器。軟體可能被安裝「後門」

內含機敏資料

車輛所蒐集之資料可能包含關鍵戰略設施等國安機敏資料

資料量龐大

聯網車輛透過感測器蒐集大量即時資料，帶有戰略價值

3. 美國聯網車輛監管政策發展 (1/4)

美國政府不分黨派，合力遏止國安機敏資料遭外國竊取

- 2019.5.15 (川普) 行政命令13873-確保資通訊技術及服務 (ICTS¹) 供應鏈的安全
- 2021.6.9 (拜登) 行政命令14034-保護美國人敏感資料免受境外敵對勢力侵害
- 2024.2.28 (拜登) 行政命令14117-防止特定國家存取大量敏感個人與政府相關資料
- 2024.3.1 (商務部) 法規制定預告-確保資通訊技術及服務供應鏈的安全：聯網車輛
(Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles)
- 2024.6.13 (眾議院) 聯網車輛國家安全審查法案
(Connected Vehicle National Security Review Act) **尚未通過**
- 2024.9.26 (商務部) 法規預告-確保資通訊技術及服務供應鏈的安全：聯網車輛

¹ 資通訊技術及服務 Information and Communications Technology and Services, ICTS

3. 美國聯網車輛監管政策發展 (2/4)

五大因素，判定中國為風險最高之境外敵對勢力

《中華人民共和國國家情報法》授權情報官員
控制私人企業之設施，包含通訊設備

《中華人民共和國
數據安全法》規定
基於國安需求，國
家得取得所有私人
資料

統計顯示中國對美
國進行網路攻擊次
數最多、範圍最廣



《中華人民共和國國家
安全法》邀由個人及企
業須向安全及軍事機關
提供「所有必要之協助」

《中華人民共和國公司
法》規定公司內部應設
立黨組織、執行黨的活
動，並為黨組織的活動
提供必要條件。

3. 美國聯網車輛監管政策發展 (3/4)

「受監管之ICTS交易」須符合四要件 - 行政命令13873

1 ▶ 對象

受境外敵對勢力所擁有、控制、或受其司法管轄或指示的人員或組織，包含合夥企業、協會、信託、合資企業、公司、團體、子團體或其他組織；以及任何危害美國國家安全、關鍵基礎設施安全或美國人民安全的外國人士或地區。

2 ▶ 產品

設計、開發、製造或提供的聯網車輛資訊和通訊技術或服務。

3 ▶ 活動

取得、進口、轉讓、安裝、交易、使用，或託管服務、資料傳輸、軟體更新、維修

4 ▶ 不當風險

- (A) 對美國境內資通訊技術或服務的設計、完整性、製造、生產、配送、安裝、操作或維護造成不當的破壞或難以回復之風險；
- (B) 對美國關鍵基礎設施的安全或韌性，或對美國數位經濟造成災難性之影響；
- (C) 對美國國家安全或美國人民的安全構成其他不可接受的風險。

3. 美國聯網車輛監管政策發展 (4/4)

商務部對「受監管之ICTS交易」之監管手段 - 行政命令13873

介入調查

要求相關人士提供資訊、簽署切結、搜查文件、舉行聽證、傳喚及詰問證人等。

第1步

暫停交易

商務部可要求在調查期間先暫停相關聯網車輛ICTS交易活動。

第2步

風險緩和

可自制定風險緩和措施、協調或強制相對人接受特定條件，包括但不限於符合特定網路安全標準、禁止使用特定的軟硬體零件等。

第3步

禁止交易

若安全風險無法降低至可接受範圍，商務部可禁止聯網車輛ICTS的取得、進口、轉讓、安裝、交易或使用。

第4步

3. 商務部之法規預告 (1/2)

商務部依據法規制定預告收到之反饋做出回應，並於法規預告繼續徵詢意見

1 聯網車輛 定義

法規制定預告

指具備車載網路軟硬體系統，並能透過DSRC、行動網路、衛星或其他無線頻譜技術，與任何其他網路或設備進行通訊之車輛。

法規預告

沿用上述定義，但限縮為使用於公共街道路或高速公路之車輛，而不包含僅於鐵路運行之車輛。

2 聯網車輛 供應鏈

法規制定預告

聯網車輛ICTS供應鏈之各階段（如設計、開發、製造）廠商？ICTS相關零件之設計、開發、製造地理位置為何？上述零件所指之軟體、硬體為何？受境外反對勢力指示者涉足ICTS供應鏈部門之情況？

法規預告

由法規制定預告之反饋意見可見供應鏈之複雜性，因此商務部尚未預計訂立盡職調查相關要求，並將制定延遲實施之時程表，給予產業緩衝時間調整現有供應鏈。

3. 商務部之法規預告 (2/2)

商務部依據法規制定預告收到之反饋做出回應，並於法規預告繼續徵詢意見

3

聯網車輛
ICTS

法規制定預告

網聯車輛不可或缺之資通訊技術包括6種系統：(1) 車載操作系統 (OS) ; (2) 遠端資訊處理系統 (Advanced Driver-Assistance System) ; (3) 駕駛輔助系統 (ADAS) ; (4) 自動駕駛系統 (ADS) ; (5) 衛星或蜂巢式通訊系統 (satellite or cellular telecommunications systems) ; (6) 電池管理系統 (BMS)

法規預告

反饋意見指出，原定之ICTS範圍過廣，為了兼顧產業發展與國家安全，應排除資訊洩漏風險較小之OS、ADAS、BMS。

4

聯網車輛
監管

法規制定預告

是否已有適合的產業標準、最佳實踐？是否應建立盡職調查、記錄保存等行政規範？是否應建立特許審查程序？

法規預告

反饋意見提供之產業標準、最佳實踐尚不足以完全降低風險，商務部預計將：(1) 設立監管諮詢機制；(2) 允許供應鏈廠商自行證明其符合法規；(3) 制定一般通用之審查程序。

- https://www.its.dot.gov/research_areas/pdf/WhitePaper_connected_vehicle.pdf
- <https://www.whitehouse.gov/briefing-room/statements-releases/2024/02/29/statement-from-president-biden-on-addressing-national-security-risks-to-the-u-s-auto-industry/>
- <https://stli.iii.org.tw/article-detail.aspx?no=64&tp=1&d=9173>
- <https://www.congress.gov/bill/118th-congress/house-bill/8741/text>