# 從塔林手冊2.0版觀點看跨境數據取證之合法性

2018.7.13

智慧財產法院 / 蔡志宏

# Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations

Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence

# Cyber is complex……

- Par 8. The Experts noted that it sometimes may be impossible or difficult to reliably identify the State in which the digital evidence or other data subject to extraterritorial enforcement jurisdiction resides.
- They agreed that international law does not address this situation with clarity.
- Par 12. Experts acknowledged that determining whether enforcement jurisdiction is territorial or extraterritorial can be complex in the cyber context.

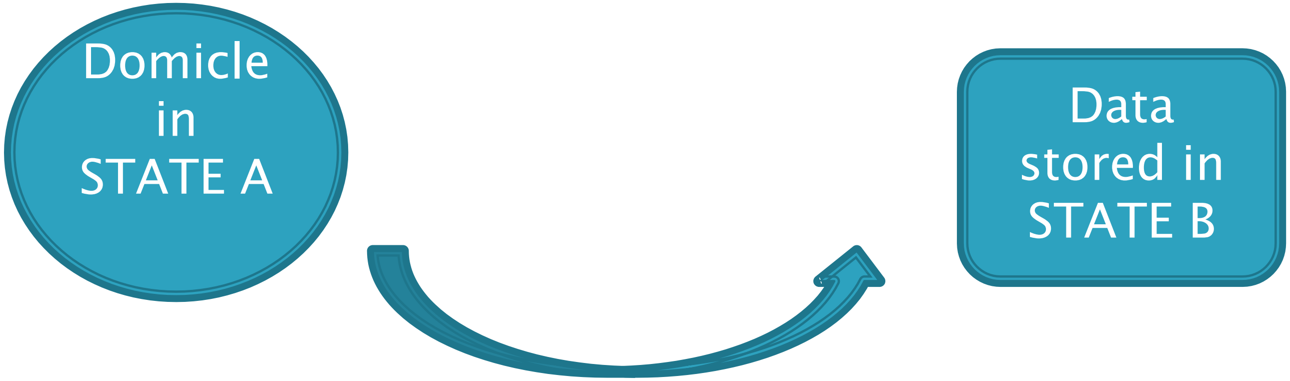
# Rule 11

- Extraterritorial enforce jurisdiction (EEJ)
- A State may only exercise EEJ in relation to persons, objects and cyber activities on the basis of authority under international law, or valid consent by the respect State.
- Par. 14 – Data that is stored on a private computer abroad, even if connected to the Internet, that is not meant to accessible.
- If a law enforcement agency(LEA) hacks to into a suspected criminal's computer located in another State, it is exercising EEJ.

- Par. 15
- LEA directly contact private foreign hosting service providers to obtain extraterritorial data.
- There are splitting comments on this issue.
- Some have the view: the data is not public available, consent is required.
- Some thought: mere request not accompanied by compulsion to comply is not exercising EEJ.

- Par 16.
- Mere fact that a person or private entity of its nationality does not alone afford  that State the legal authority to exercise EEJ with respect to that data.
- However, the State may exercise EJ over the individuals or private entities themselves if they are located in the State.

# Example



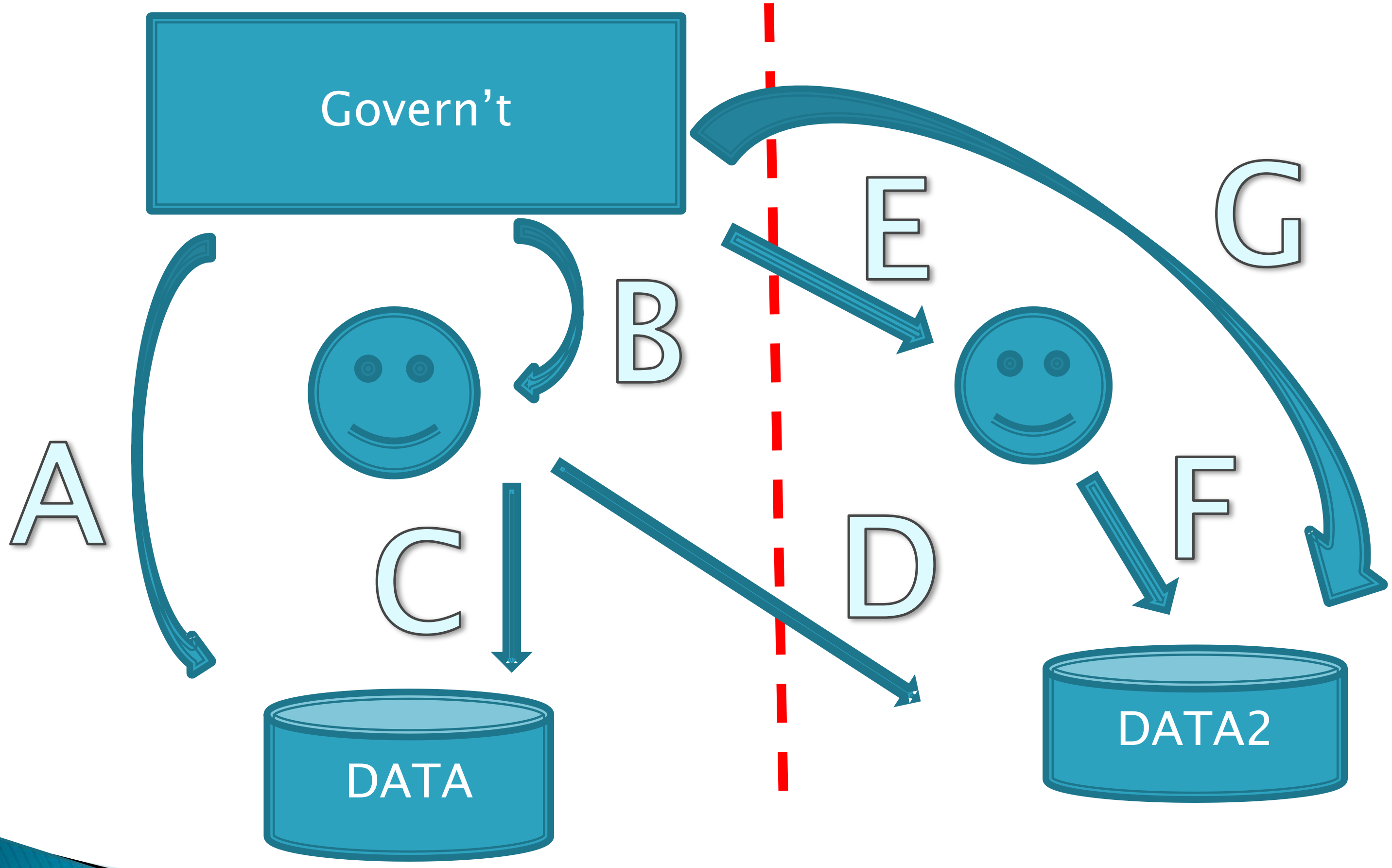
Domicle
in
STATE A

Data
stored in
STATE B

- The consent of State A is not enough to permit remote access by State C to the data in State B
- State A may exercise it jurisdiction over the entity and require it to provide the data to State C.

# 境內＆跨境取證示意圖

A: 境內搜索
BC: 境內提出命令
BD: 境外提出命令
EF：境外提出請求
G：境外搜索



# 境內＆跨境取證之國際法解析

- A：可以包括破解、侵入境內電腦
- BC：可以在資料持有人（包括所有人及保管人）抗拒時處罰，以強制提出
- BD：同BC，等同僅對境內行使管轄，但Data 2所在國可以為保護境內資料立法干預保管人提出資料。
- EF：單純請求者，仍有爭議；如伴隨強制力，即為境外行使管轄，應經Data 2所在國同意。
- G: 非經Data 2所在國同意，不得為之。
- 於境內反於Data 2所有人意願，取得帳號、密碼後所為之跨境取證，是否為境外搜索？

# Convention on Cybercrime Budapest, 23.Nov.2001

- A Party may, without the authorisation of another Party: access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

# Question and Comments?