RSAC Studio

Connect to Protect

A Futurist´s look at Nation-State Cyber-Espionage

Vicente Diaz
Principal Security Analyst
Kaspersky Lab
@trompi

#RSAC

The rules driving evolution

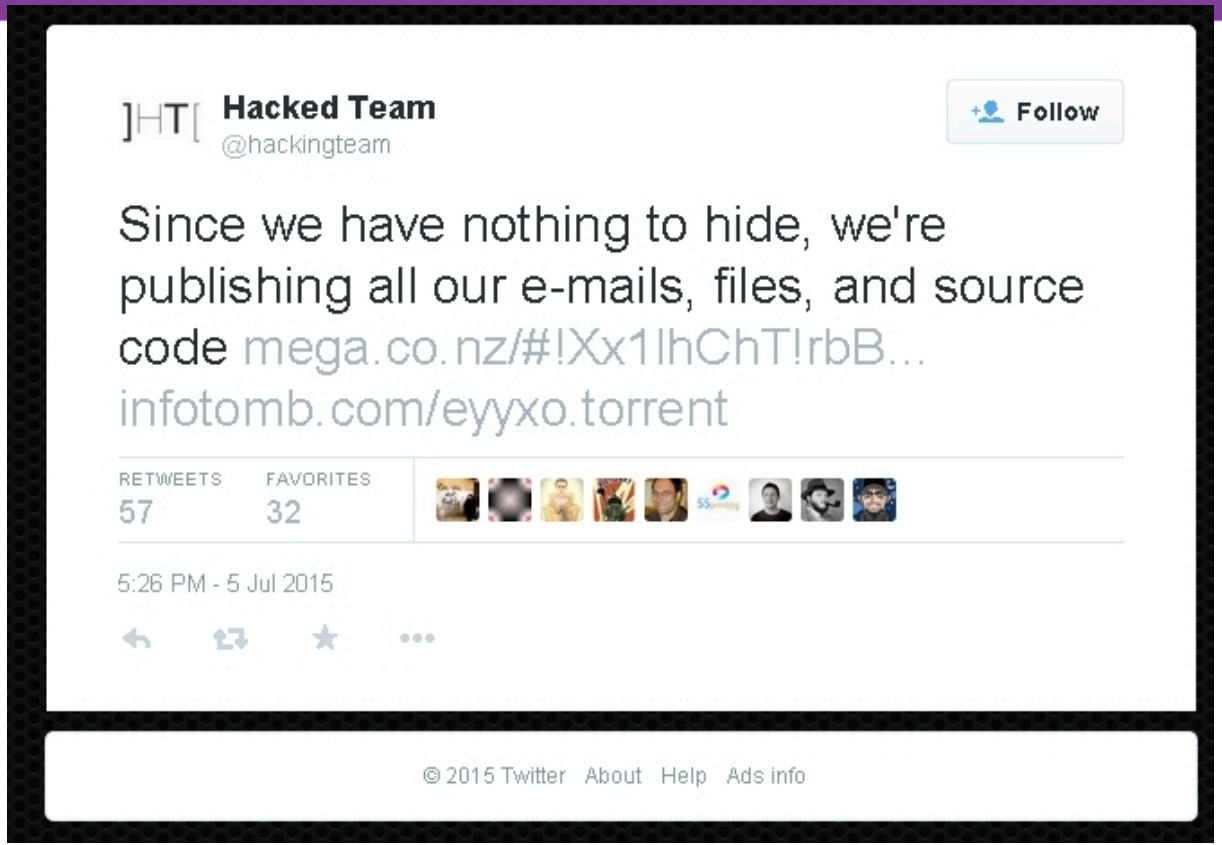
Where do we come from?

- Obviously, all countries pushed to develop their capabilities.
- According to their capabilities, we can make 3 categories.

Category 1 - “Unlimited” resources

Category 2 - “Middle class”

Category 3 – Externalize capabilities



What happens when you get public?

- Public level: Public scrutiny´s power depends on **democracy**´s health. May affect legislation and future capabilities.
- Operational level:
  - Operation burst – but maybe amortized
  - Operational changes and continue as usual
  - Do nothing
- **Diplomatic** level: Obvious consequences.

Lessons learned

- Avoid attribution (but get the job done)

Where are we now?

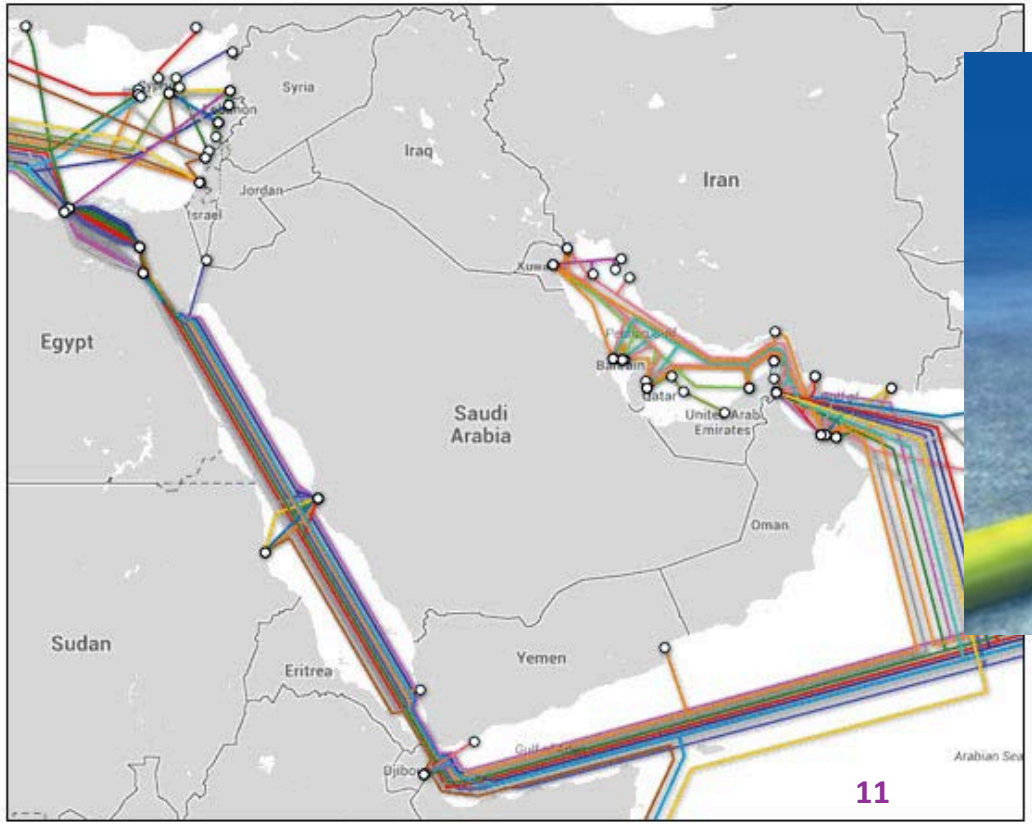
- Top players have:
  - Legislation control
  - Infrastructure control
  - Relationships with partners/companies

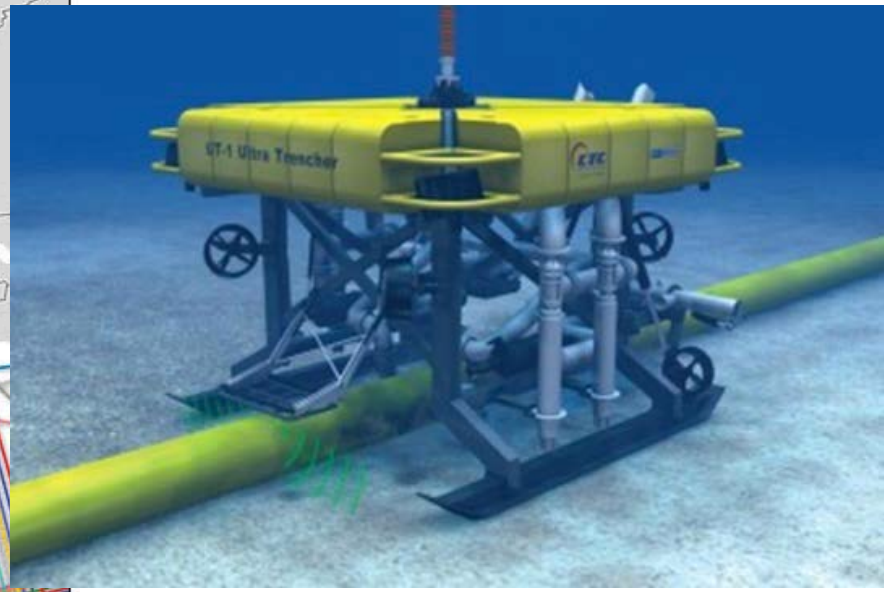
Only one barrier left

Boiten argued the prime minister may try and persuade services that use end-to-end encryption, such as Apple and WhatsApp, to introduce government backdoors to give UK spies access to private communications.

Actually, where is the data now?

Undersea Fiber-Optic Cables in the Middle East





Who can do that?

- Nobody trusts other´s infrastructure → Internet Balkanization

What will we see in the future?

- Besides espionage, control of adversary´s critical systems
- “Middle class Stuxnet”

BlackEnergy Involved in Targeted Attack Against Boryspil Airport, Says Ukraine

Future cyberespionage

- “Middle class” operations are enough when you control the infrastructure

Future cyberespionage

- Assume unlimited supply of 0 days

HACKERS CLAIM MILLION-DOLLAR BOUNTY FOR IOS ZERO DAY ATTACK

Future cyberespionage

- Get control of non-controlled infrastructure attacking network devices, firmware, rogue hardware, etc. Regin and Equation as early adopters.

Either way, the malware investigators at Belgacom never got a chance to study the routers. After the infection of the Cisco routers was found, the company issued an order that no one could tamper with them. Belgacom bosses insisted that only employees from Cisco could handle the routers, which caused unease among some of the investigators.

Future cyberespionage

- Exfiltration through non monitored protocols and devices.

Future and present cold war

U.S. Charges Chinese Government Officials With Cyber Espionage

Future and present cold war

Obama: U.S. and China Reach Cyber-Espionage 'Common Understanding'

The future brings us

- Keep sophistication as low as possible to avoid attribution
- Fight for infrastructure control
- Cyber diplomacy and alliances
- “IoT” infections over “computers”

A Futurist´s look at Nation-State Cyber-Espionage