# IT and the state

9. 10. 2019

Jakub Drmola

Modern technology and Conflicts

# In general

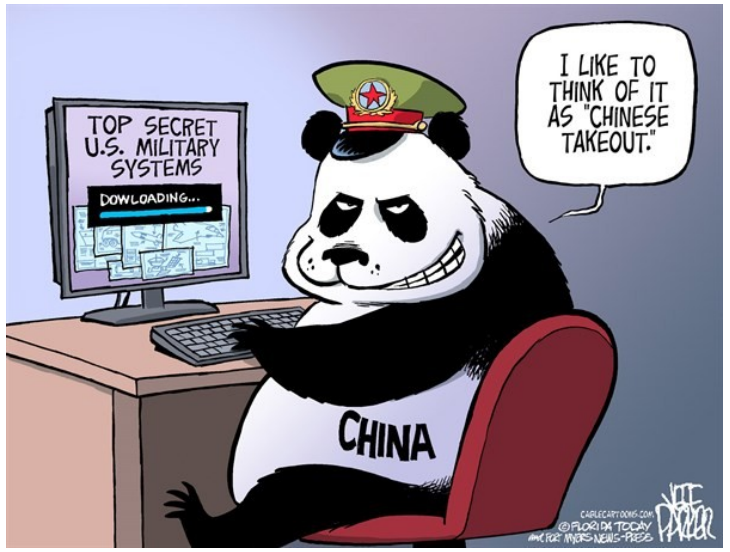
Specific

- Behavior
- Activities
- Purpose

Ideology

Hacktivism
Cyberterrorisms

Militia




Individuals

State

Espionage
Sabotage

Financial crime
Stolen identity

Profit

# Triad of cyber security

CIA

- Confidentiality
- Integrity
- Availability

# Main state activities in cyberspace

- Espionage
- Sabotage
- Censure
- Information war/propaganda
- Demonstration of power
- Support of conventional attack

# Cyber espionage vs. Sabotage

Espionage

- Obtaining strategically sensitive or strategically important information from individuals or organizations by using or targeting IT means. It is used most often in the context of obtaining a political, economic or military supremacy.

Sabotage

- Deliberate action aimed at weakening a polity or corporation through subversion, obstruction, disruption or destruction. In a workplace setting, sabotage is the conscious withdrawal of efficiency generally directed at causing some change in workplace conditions.

# Cases

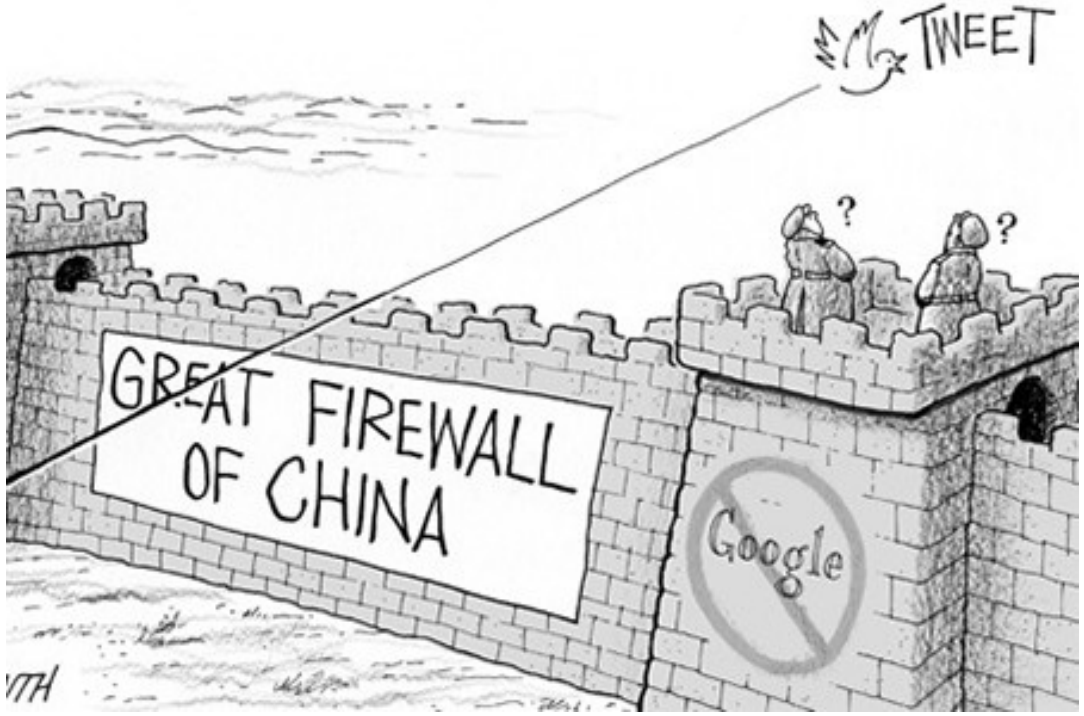
Saudi Aramco
roducing Operations

25.F119-611 发动机
26.主起落架
27.主起落架舱
28.天线
29.前缘襟翼
30.前缘襟翼旋转作动筒及传动轴
31.前缘襟翼操纵动力源
32.外挂架加强连接点
33.外挂架加强翼肋
34.机翼整体油箱
35.航行灯
36.襟副翼
37.襟副翼结构
38.襟副翼作动筒
39.横滚控制管道
40.横滚控制喷口(固定 87°,喷流角 4°)
41.加力燃烧室
42.三轴承支撑推力矢量喷管，可向前下方偏转 95°；垂直起降时，可水平偏转±10°；
43.低可探测性轴对称喷口
44.可收放空中加油管
45.方向舵作动筒
46.低可探测性机体
47.多梁、肋式垂尾结构
48.铝合金蜂窝结构垂尾前缘
49.方向舵
50.全动水平尾翼
51.水平尾翼作动筒
52.垂尾
53.水平尾翼结构
54.铝合金蜂窝结构水平尾翼前缘、后缘
爱空军 www.jAirForce.com

DO WE HAVE A BACKUP?
Stuxnet VIRUS
Int'l Herald Tribune

# Censorship

- Commonly linked with non-democratic regimes
- Halal internet vs. forbidden applications
- Different methods of circumvention



# Surveillance

- Repressive or suppressive
- For law enforcement

- Potential targets:
  - Criminals, terrorists
  - Dissidents, journalists
  - Minorities, foreigners

# Demonstration of power

Estonia (2007) and Latvia (2008)

- Similar modus operandi (DDoS, defacement and malware)
- Russian Federation – absence of direct evidence

Estonia - due to the removal of the bronze statue of an unknown Soviet soldier

- for RF symbol of freedom vs. symbol of occupation

Latvia – main reasons: law about non-acceptance Nazi and Soviet symbols, planning of American antimissile defense

# Support conventional attack

**Georgia (2008)**

- In the background of a five-day war
- Target: destroying of active communication and information
- Methods: defacement, DoS, DDoS, malware
- Patriotic hacking (nationalistic mode in society)
- Russian Business Network
- Attacks also on RF

# Information war/ propaganda

# Demystification ???

**1982: trans-siberian sabotage**

**2000s: shot mafia boss**

**2008: Lodz trams**

**2014: steel mill hack**