

Cybersecurity

Part 1 – overview and state activities

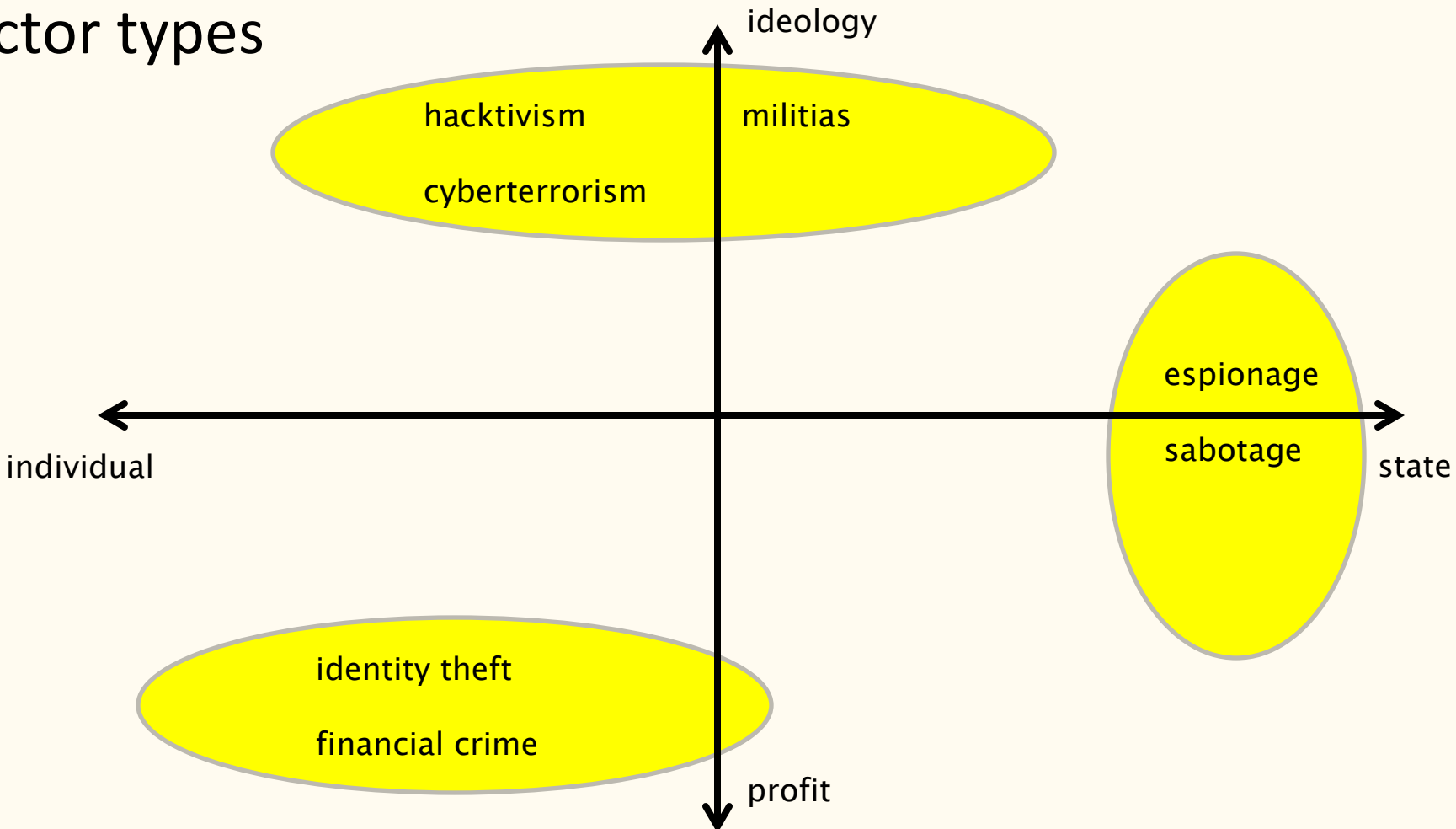
Cybersecurity is hard

—

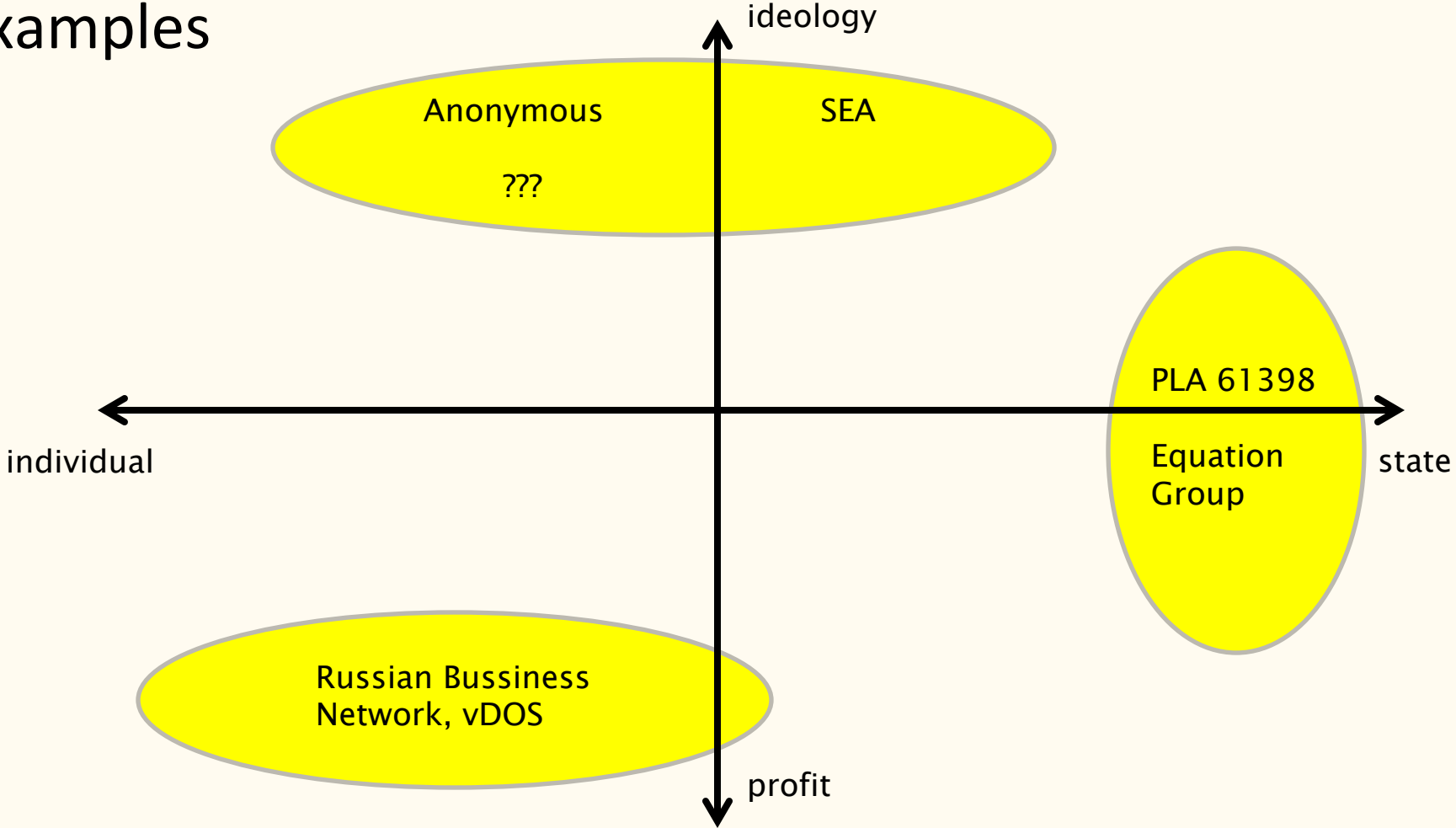
Characteristics to note when attack occurs

- 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?

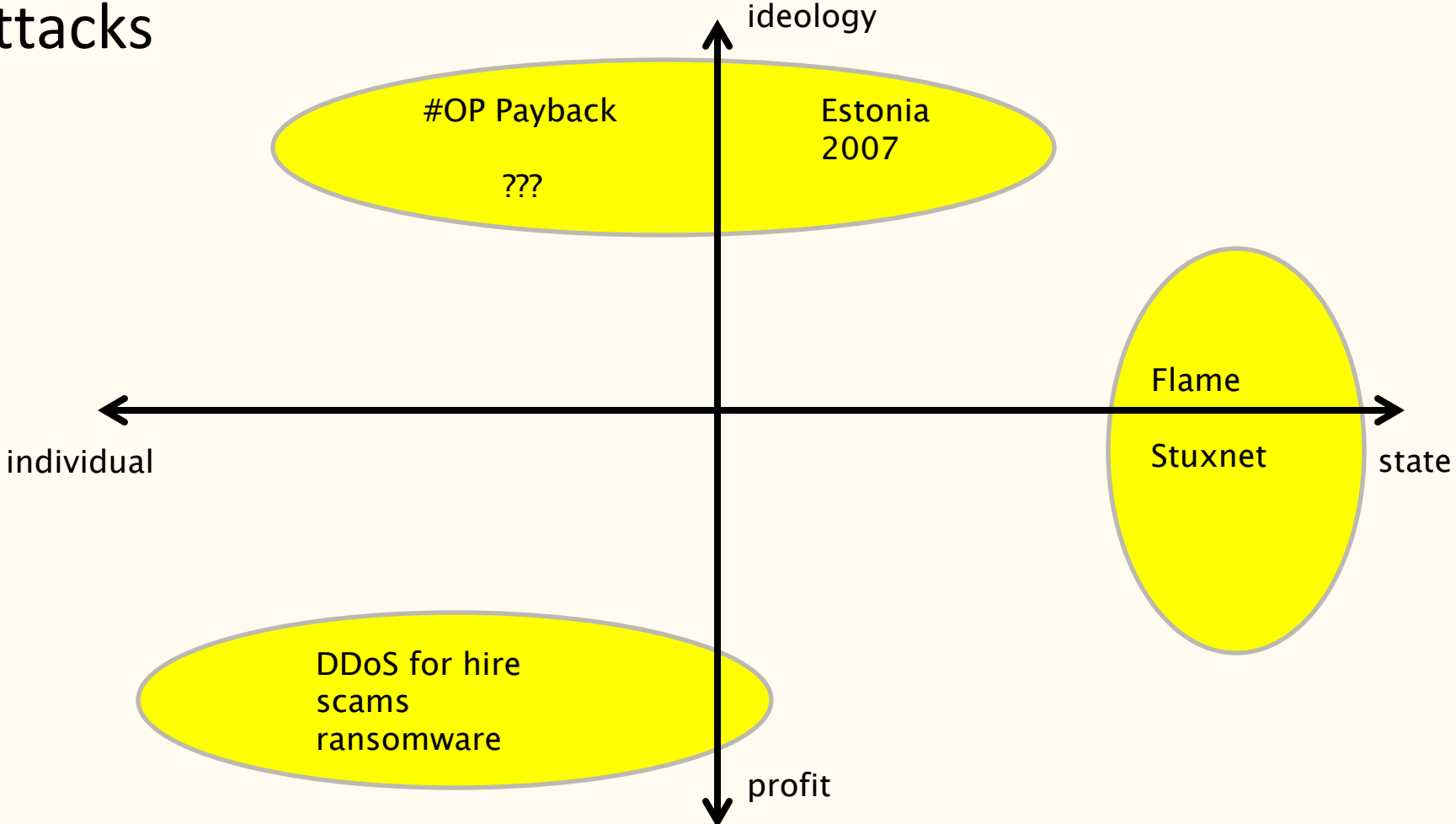
Actor types



Examples



Attacks



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

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

- examples?

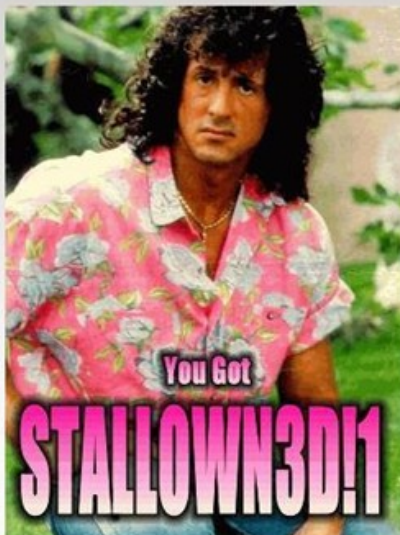
Key distinctions

- 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

This page has been Hacked!



XSS Defacement

">

Invalid list name.

Low Orbit Ion Cannon



newfag/LOIC

p.s cocks

Manual Mode (for pussies) **FUCKING HIVE MIND**

IRC server: Port: Channel: Connected!

1. Select your target

URL:

IP:

2. Ready?

Selected target

85.116.9.83

3. Attack options

Timeout: HTTP Subsite: Append random chars to the URL

Port: Method: Threads: Wait for reply

TCP / UDP message:

Speed slider: <= faster | Speed | slower =>

Attack status

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



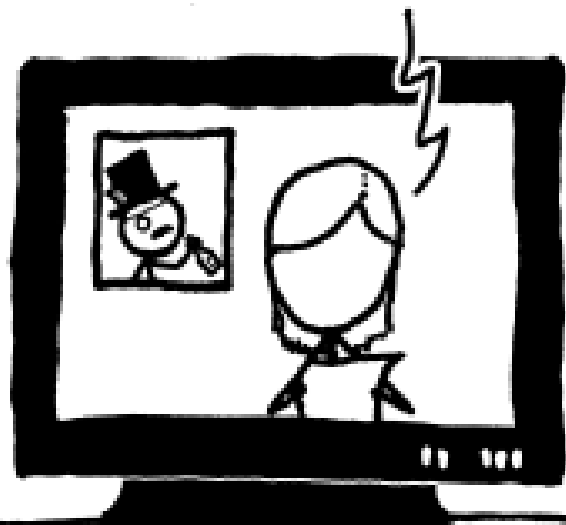
The connection has timed out

The server at www.cia.gov is taking too long to respond.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

Try Again

HACKERS BRIEFLY TOOK
DOWN THE WEBSITE OF
THE CIA YESTERDAY...



WHAT PEOPLE HEAR:

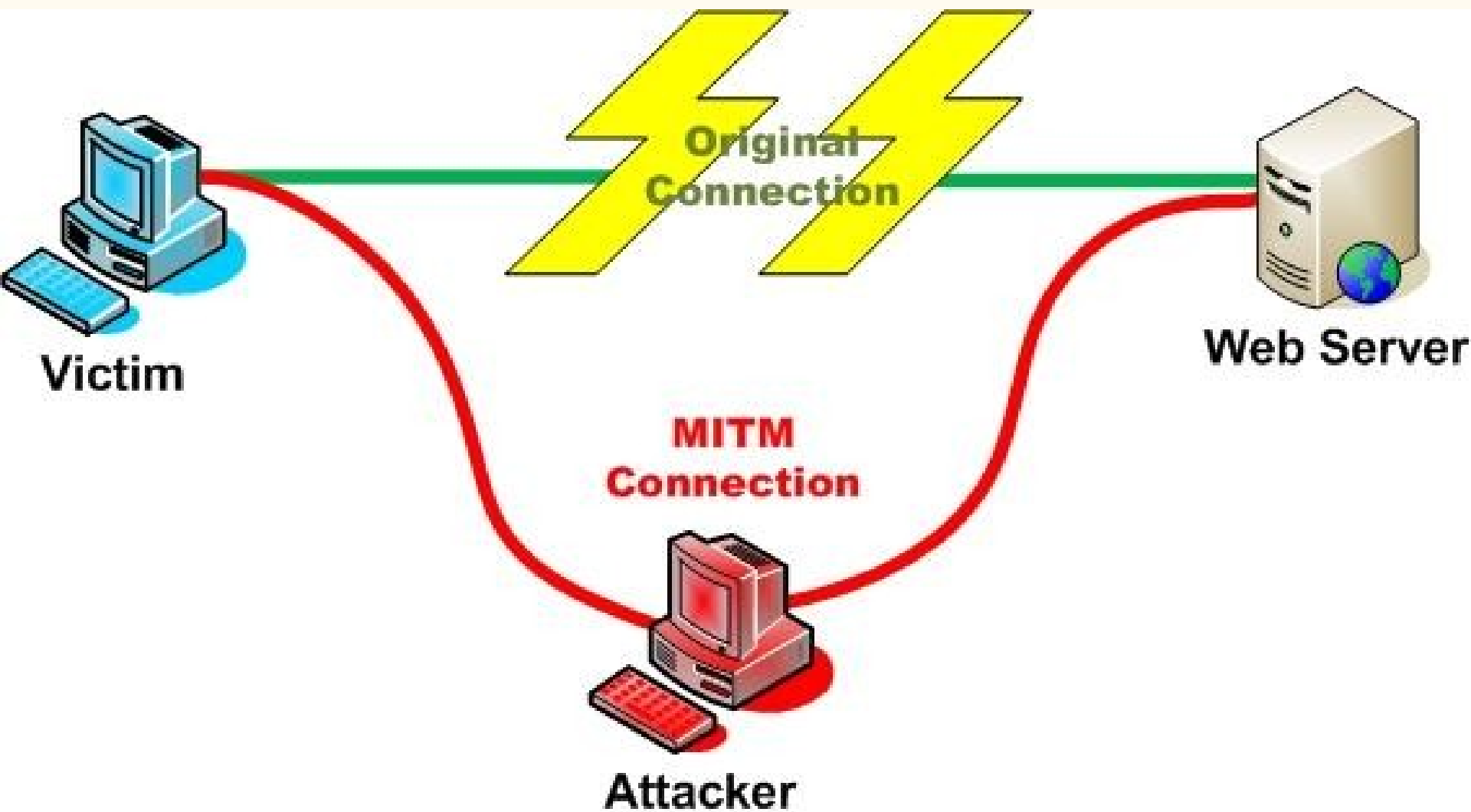
SOMEONE HACKED
INTO THE COMPUTERS
OF THE *CIA!!*



WHAT COMPUTER
EXPERTS HEAR:

SOMEONE TORE DOWN
A POSTER HUNG UP
BY THE *CIA!!*





MOVIE HACKING...

IF I CAN JUST OVERTHROW 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?



Gmail



Important: Your Password will expire in 1 day(s)



Inbox x



MyUniversity

12:18 PM (50 minutes ago) ☆



to me ▾

Dear network user,

This email is meant to inform you that your MyUniversity network password will expire in 24 hours.

Please follow the link below to update your password

myuniversity.edu/renewal





MY UNIVERSITY

Thank you
MyUniversity Network Security Staff



Salif Issa salifissa70@gmail.com via yahoo.com
to ▾

Tue, 22 Oct, 13:17   



This message seems dangerous

Similar messages were used to steal people's personal information. Avoid clicking links, downloading attachments or replying with personal information.

Looks safe



Dear Friend,

I am a banker by profession from Burkina-Faso in West Africa and currently holding the post of Manager of bill and exchange at the foreign remittance department of a Bank located Burkina Faso. I have the opportunity of transferring the abandon funds (\$31.5 Million USD) of one of my banks client who died along with his entire family on 6th December 2003 in a plane crash.

Since we got information about his death, we have been expecting his next of kin to come over and claim his money because we cannot release it unless somebody applies for as next of kin or relation to the deceased as indicated in our banking guidelines but unfortunately we learnt that all his supposed next of kin or relation died alongside with him at the plane crash leaving nobody behind for the claim.

The Banking law and guideline here stipulates that if such money remained unclaimed after Eight to Nine years an above, the money will be transferred into the Bank treasury as unclaimed fund. I agree that 40 % of this money will be for you as foreign partner in respect to the provision of a foreign account, and while 60 % would be for me.

There after I will visit your country for disbursement according to the percentages indicated. Therefore to enable the immediate transfer of this fund to you as arranged, you must apply first to the bank as relations or next of kin of the deceased indicating your bank name, your bank account number, your private telephone and fax number for easy and effective communication and location where the money will be remitted. Upon receipt of your reply, I will send to you by fax or email the text of the application. I will not fail to bring to your notice that this transaction is hitch free and that you should not entertain any atom of fear as all required arrangements have been made for the transfer.

I will not fail to bring to your notice this transaction is hitch-free and that you should not entertain any atom of fear as all required Arrangements have been made for the transfer, please treat this business with utmost confidentiality and you should contact me immediately as soon as you receive this letter.

Please make sure you keep this transaction as your top secret and make it confidential till we receive the fund into the account that you will provide to the Bank. Dont disclose it to any body, because the secrecy of this transaction is as well as the success of it.

I am waiting to hear from you urgently. Please reply me on this my private E-MAIL contact only; (issas2392@gmail.com)

Your full name.....

Home address:.....

Your country.....

Your city.....

Telephone.....

Occupation:.....

Age:.....

SEX:.....

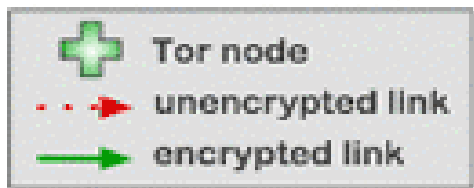
I expect your urgent response with much anticipation!!!!!!!

yours faithfully,

Mr Salif Issa.

	PIN	Freq
#1	1234	10.713%
#2	1111	6.016%
#3	0000	1.881%
#4	1212	1.197%
#5	7777	0.745%
#6	1004	0.616%
#7	2000	0.613%
#8	4444	0.526%
#9	2222	0.516%
#10	6969	0.512%
#11	9999	0.451%
#12	3333	0.419%
#13	5555	0.395%
#14	6666	0.391%
#15	1122	0.366%
#16	1313	0.304%
#17	8888	0.303%
#18	4321	0.293%
#19	2001	0.290%

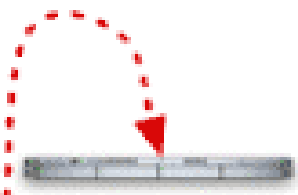
How Tor Works: 3



Alice



Step 3: If at a later time, the user visits another site, Alice's tor client selects a second random path. Again, **green links** are encrypted, **red links** are in the clear.



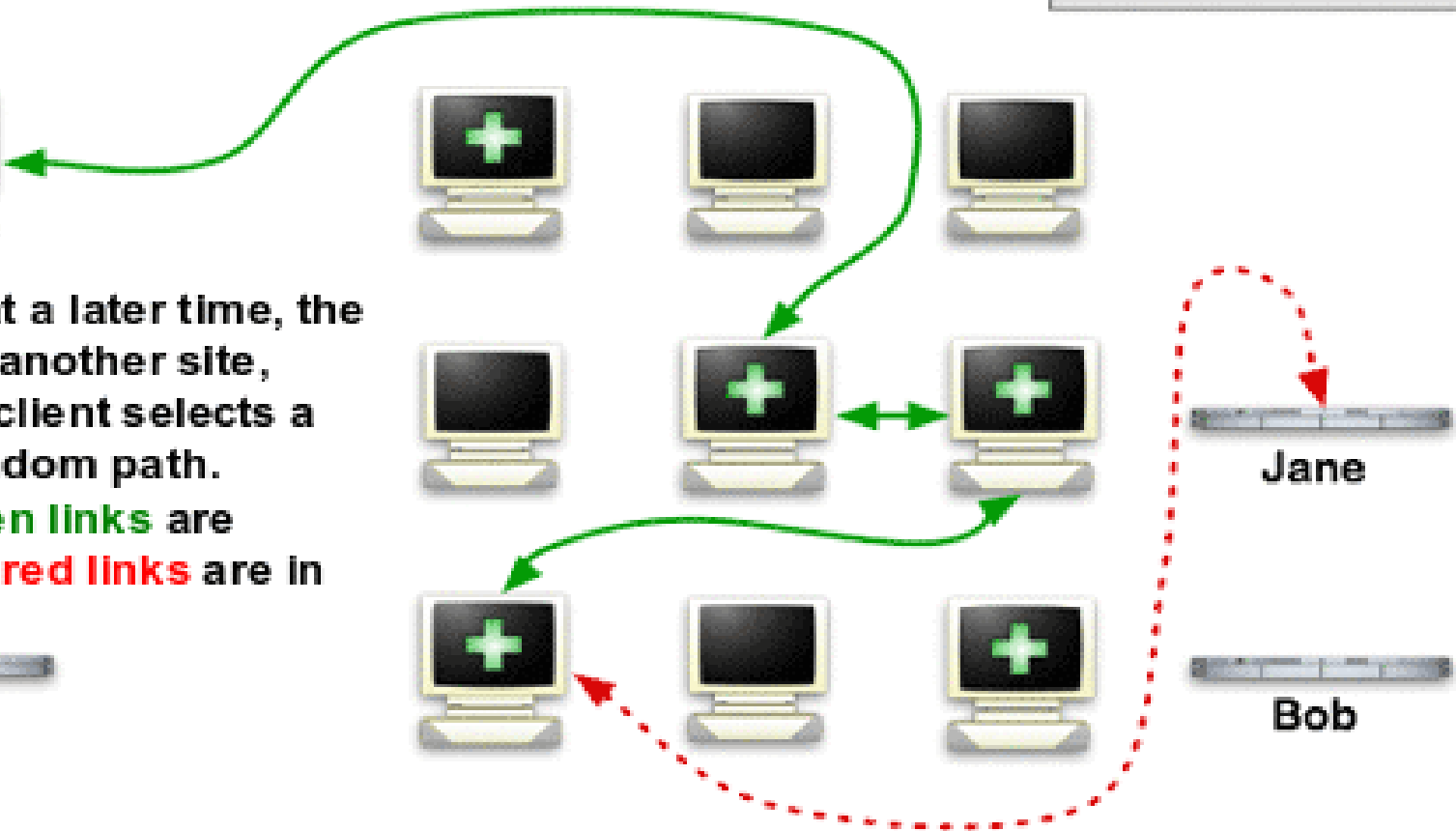
Jane



Dave



Bob



Biometrics

Physiological

face



fingerprint



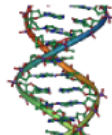
hand



iris



DNA



Behavioral

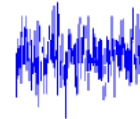
keystroke

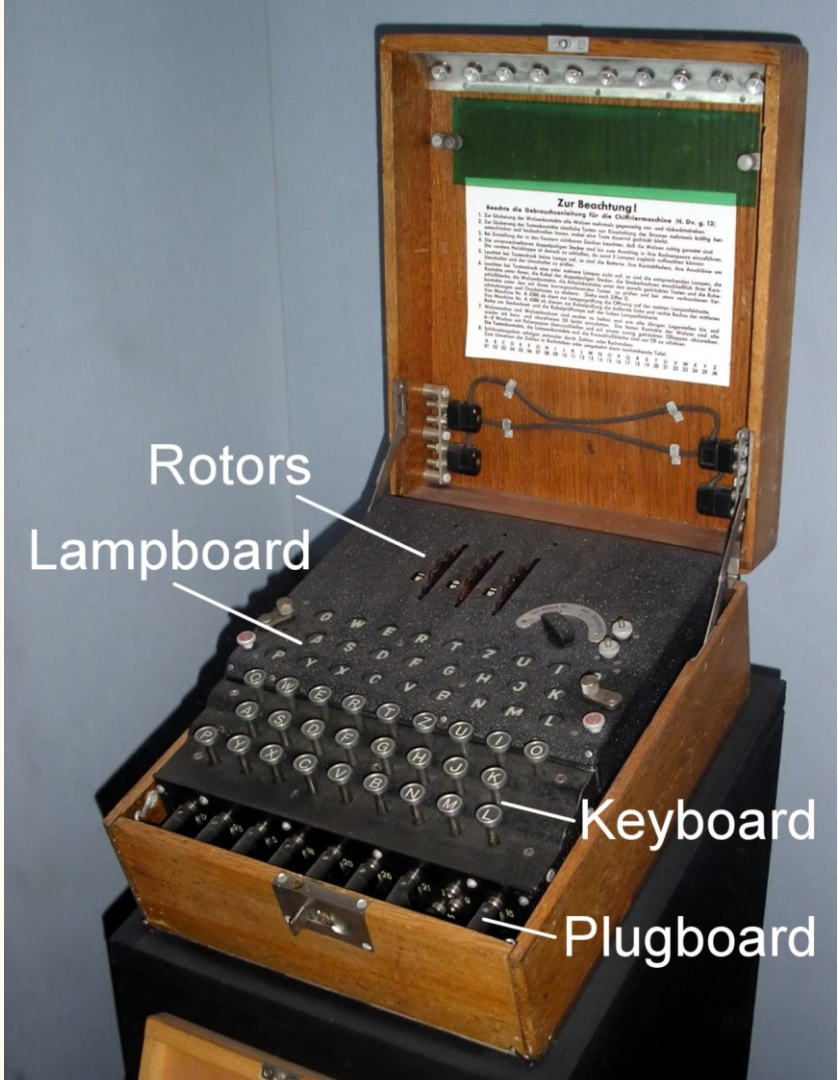


signature



voice





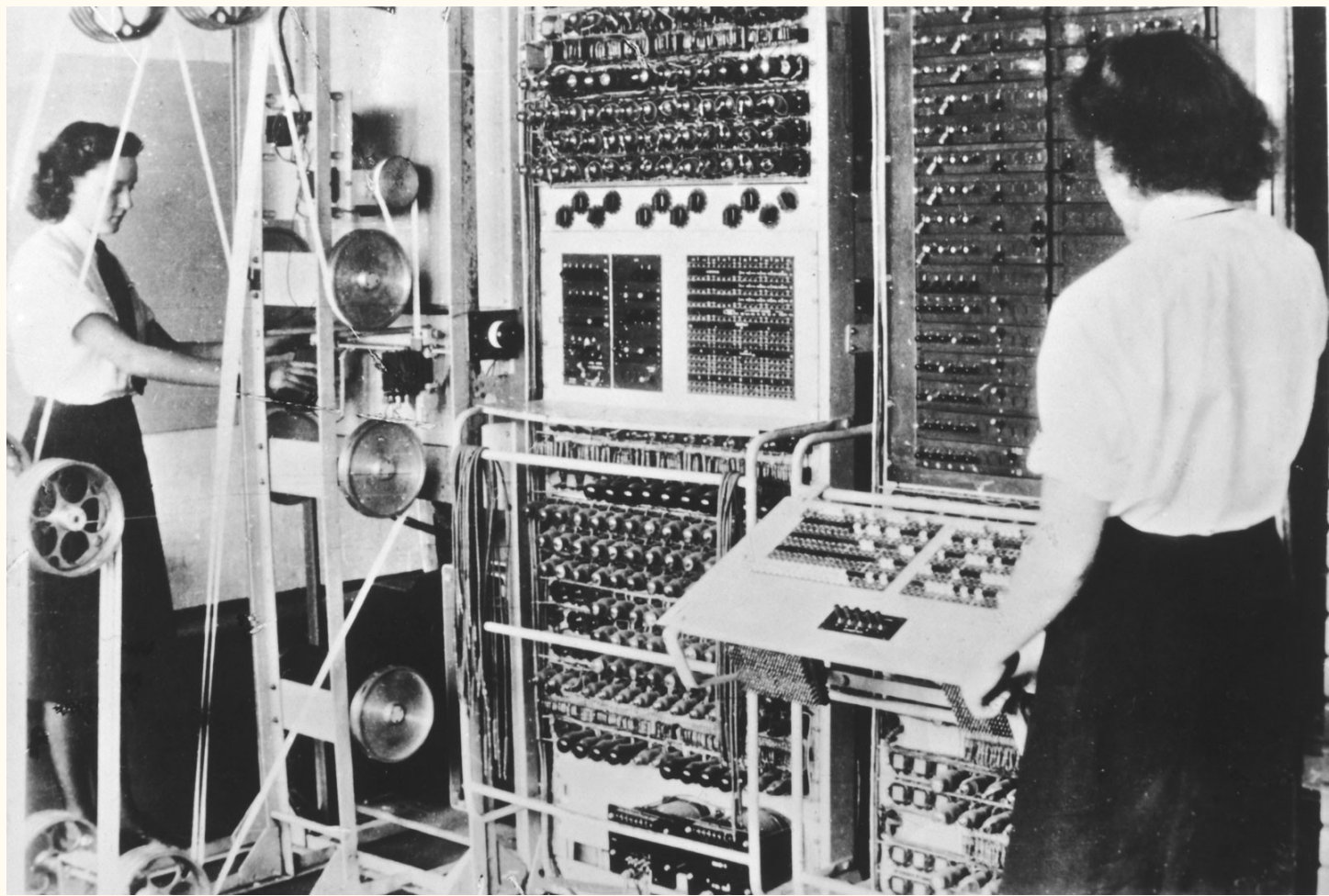
Zur Beachtung!

- Beachte die Gebrauchsanleitung für die Schlüsselmaschine SK, Dr. g. 132.
1. Die Schlüsselmaschine ist ein wertvolles Instrument, das strengstens vor Feindhänden zu schützen ist. Die Schlüsselmaschine ist ein wertvolles Instrument, das strengstens vor Feindhänden zu schützen ist.
 2. Die Schlüsselmaschine ist ein wertvolles Instrument, das strengstens vor Feindhänden zu schützen ist.
 3. Die Schlüsselmaschine ist ein wertvolles Instrument, das strengstens vor Feindhänden zu schützen ist.
 4. Die Schlüsselmaschine ist ein wertvolles Instrument, das strengstens vor Feindhänden zu schützen ist.
 5. Die Schlüsselmaschine ist ein wertvolles Instrument, das strengstens vor Feindhänden zu schützen ist.
 6. Die Schlüsselmaschine ist ein wertvolles Instrument, das strengstens vor Feindhänden zu schützen ist.
 7. Die Schlüsselmaschine ist ein wertvolles Instrument, das strengstens vor Feindhänden zu schützen ist.
 8. Die Schlüsselmaschine ist ein wertvolles Instrument, das strengstens vor Feindhänden zu schützen ist.
 9. Die Schlüsselmaschine ist ein wertvolles Instrument, das strengstens vor Feindhänden zu schützen ist.
 10. Die Schlüsselmaschine ist ein wertvolles Instrument, das strengstens vor Feindhänden zu schützen ist.

Rotors
Lampboard

Keyboard

Plugboard



Examples of steganography

Example 1: Coded message

Apparently neutral's protest is thoroughly discounted and ignored.

Isman hard hit. Blockade issue affects pretext for embargo on byproducts, ejecting suets and vegetable oils.

Take second letter of each word to get message:

Pershing sails from NY June 1

Example 2: Coded images: Least Significant Bits (LSB) insertion

Original image



Altered image



Areas where binary code of pixel has been altered

Binary code from original image pixel 1

10000000 10100100 10110101 10110101 11110011 10110111 11100111 10110011 00110000

Changes made on altered image pixel 1

10000001 10100100 10110100 10110100 11110010 10110110 11100110 10110011 00110011

Read last digit:

1000001 which is ASCII binary code for A

1 2 3 4

Fox

Hash
function

DFCD3454

The red fox
runs across
the ice

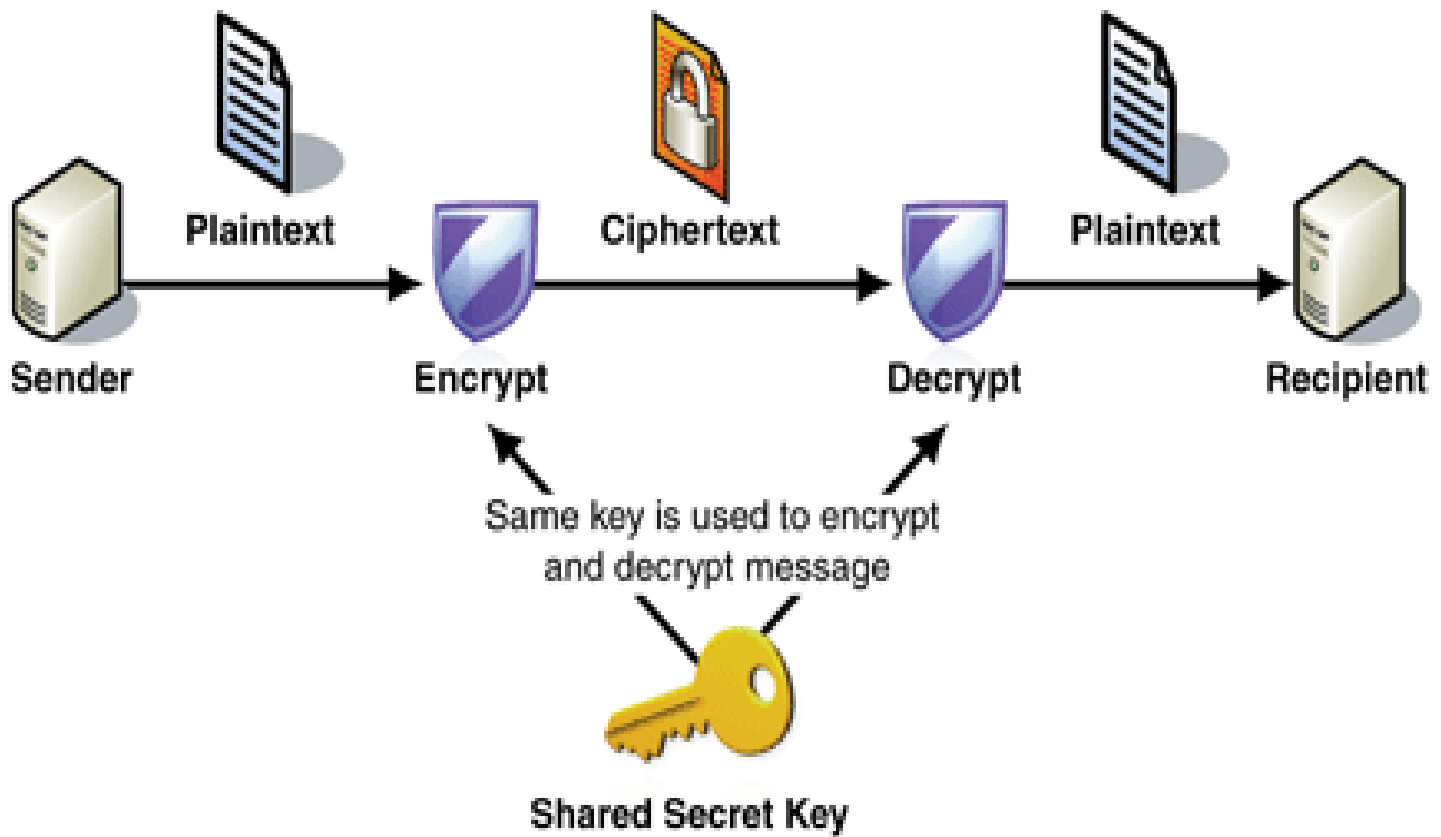
Hash
function

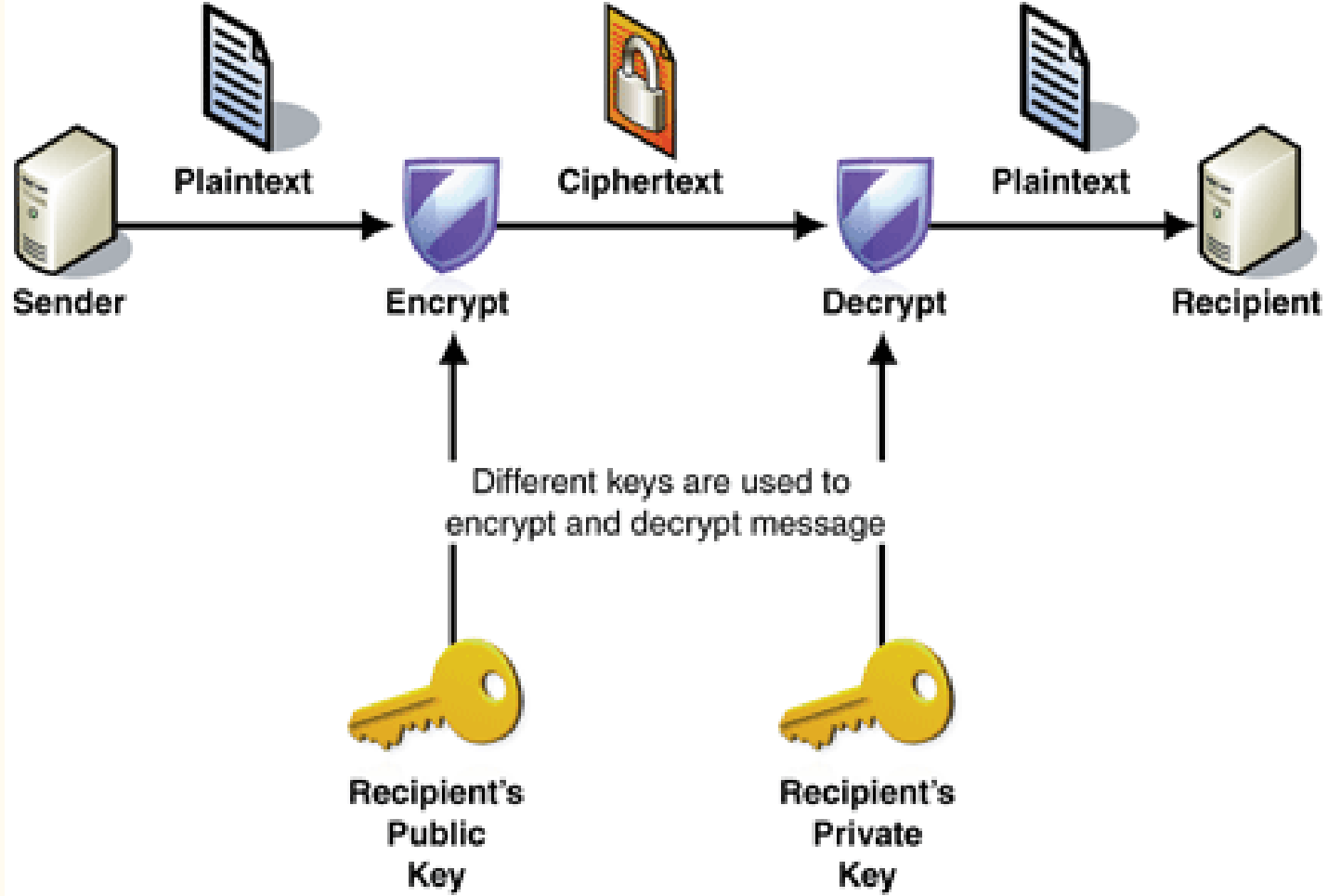
52ED879E

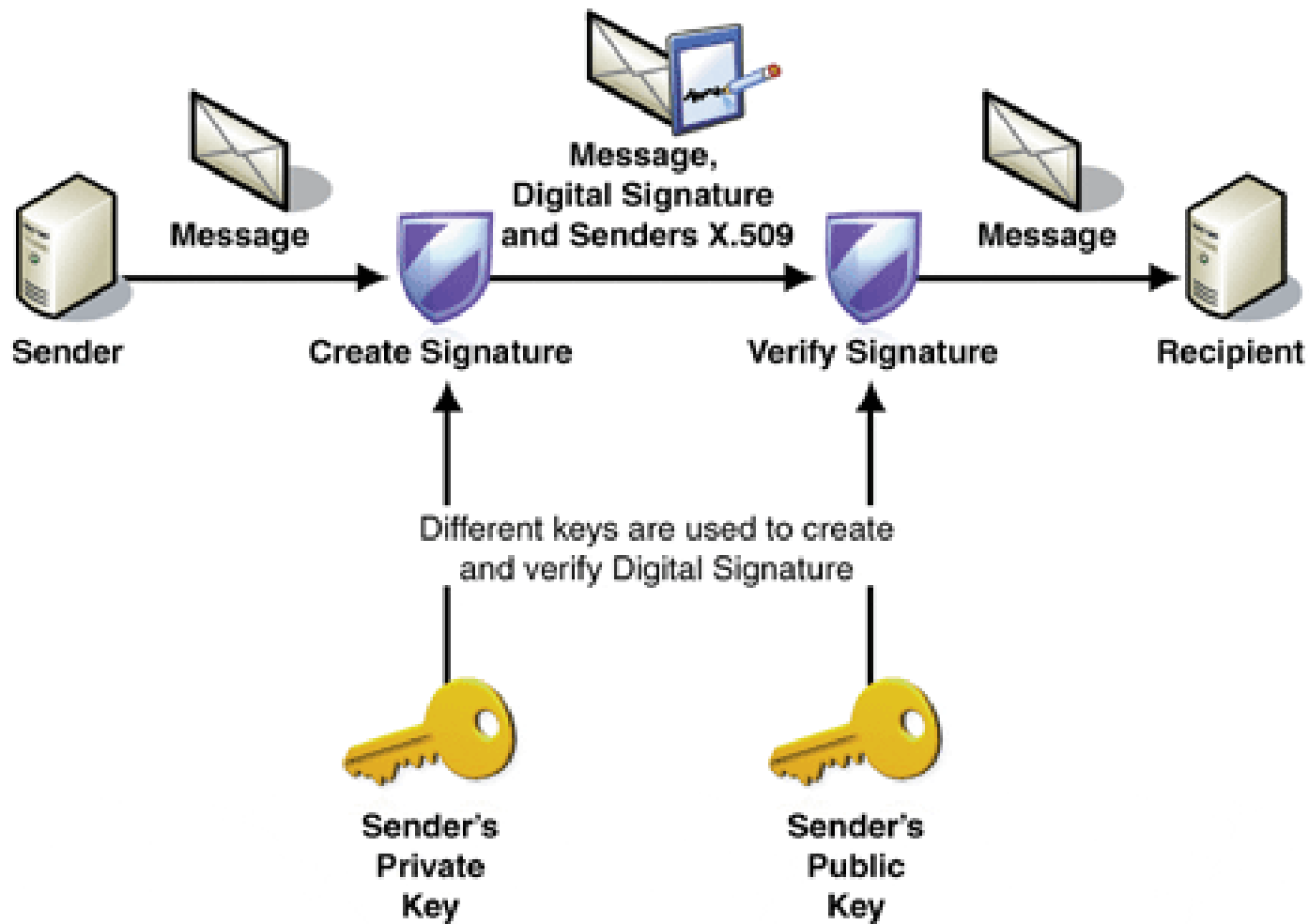
The red fox
walks across
the ice

Hash
function

46042841







Cybersecurity

State activities and APTs

Espionage

- attack on confidentiality
- Flame, Red October

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

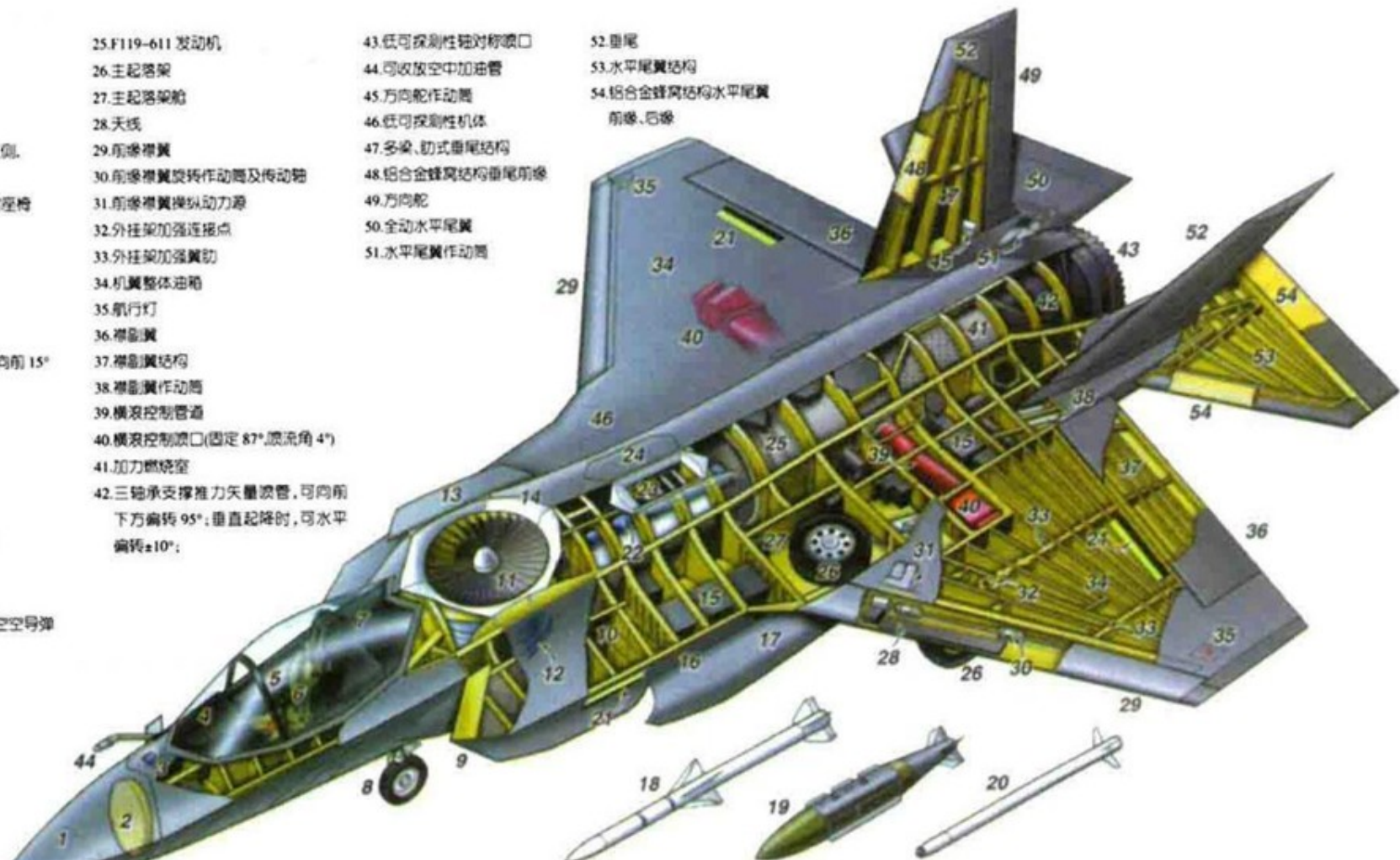
- <https://apt.securelist.com/#secondPage>

- 1.雷达罩
- 2.主空电回路多功能雷达
- 3.红外传感器
- 4.夜视仪光电罩
- 5.雷达右侧操纵台,油门在左侧,操纵杆在右侧
- 6.马丁·贝利 MK16 轻型弹射座椅
- 7.弹射器打开的座舱盖
- 8.起落架
- 9.燃油进气口
- 10.钛合金复合材料进气道
- 11.二阶三反转升力风扇
- 12.升力风扇进气口,偏转角从前向 15° 到向后 30°
- 13.升力风扇双叶舱盖
- 14.升力风扇进气口
- 15.各型通用系统
- 16.三发发动机左右各一个
- 17.三发发动机盖
- 18. AIM-120 中程空空导弹
- 19. AIM-132 先进远程格斗空空导弹
- 20.瞄准吊钩
- 21.二次泵传动轴
- 22.燃油进气口
- 23.燃油进气口油门

- 24. F119-611 发动机
- 25. 主起落架
- 26. 主起落架舱
- 27. 天线
- 28. 前缘襟翼
- 29. 前缘襟翼旋转传动筒及传动轴
- 30. 前缘襟翼操纵动力源
- 31. 外挂架加强连接点
- 32. 外挂架加强翼肋
- 33. 机翼整体油箱
- 34. 航行灯
- 35. 襟副翼
- 36. 襟副翼结构
- 37. 襟副翼传动筒
- 38. 襟副翼控制管道
- 39. 横滚控制进气口(固定 87° 偏流角 4°)
- 40. 加力燃烧室
- 41. 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°;

- 42. 低可探测性轴对称喷口
- 43. 可收放空中加油管
- 44. 方向舵传动筒
- 45. 低可探测性机体
- 46. 多梁、肋式垂直尾翼结构
- 47. 铝合金蜂窝结构垂直尾翼前缘、后缘
- 48. 铝合金蜂窝结构水平尾翼前缘、后缘
- 49. 方向舵
- 50. 全动水平尾翼
- 51. 水平尾翼传动筒

- 52. 垂直尾翼
- 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

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.

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.



Prime Minister David Cameron. Reuters/Darren Staples

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.

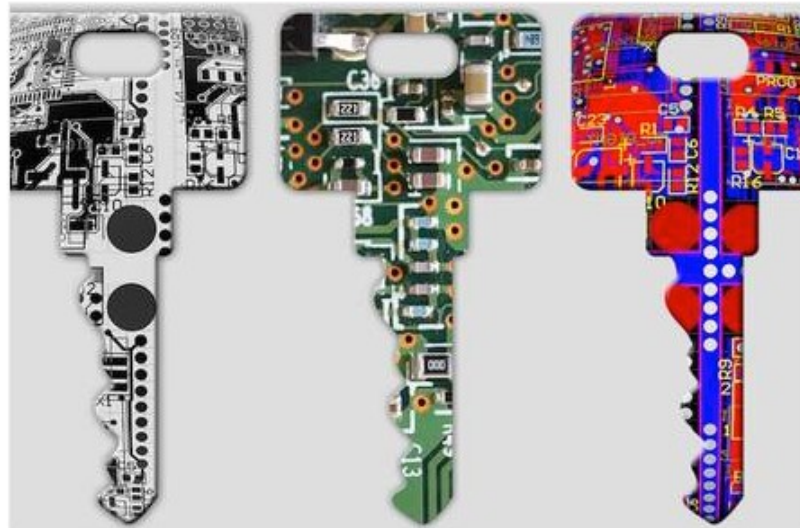
It's currently used in some of the most popular tech products in the world, including the iPhone, WhatsApp, and Facebook. But amid heightened terrorism fears, David Cameron is attempting to take action.

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

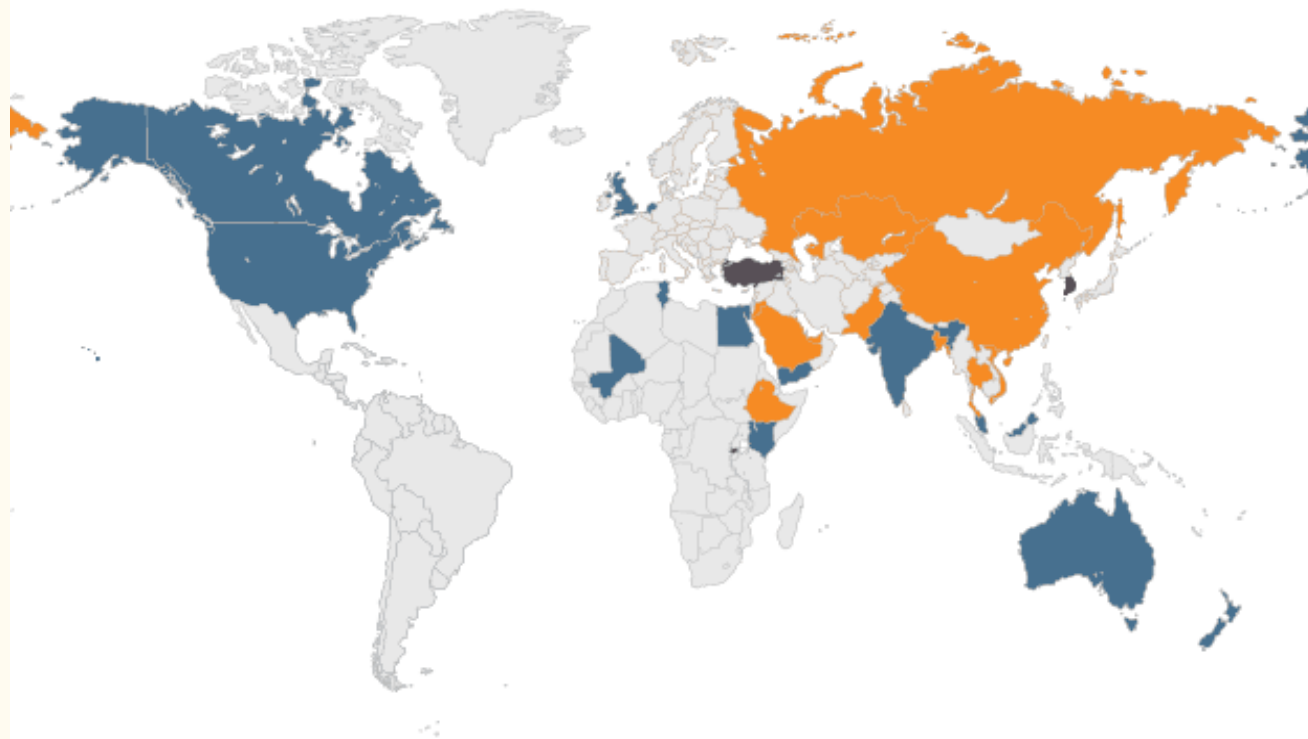


The deputy US Attorney General said he wants legislators to force technology companies to decrypt people's private conversations.

Censorship

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

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.

Sabotage

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

- still quite rare
- “kinetic barrier”



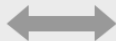
Error 522

Connection timed out

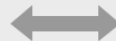


You

Browser
Working



CloudFlare
Working



www-local.projecthoneypot.org

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	-	ensorship
external	espionage	sabotage	suppression

CYBER WAR

THE NEXT THREAT TO
NATIONAL SECURITY AND
WHAT TO DO ABOUT IT

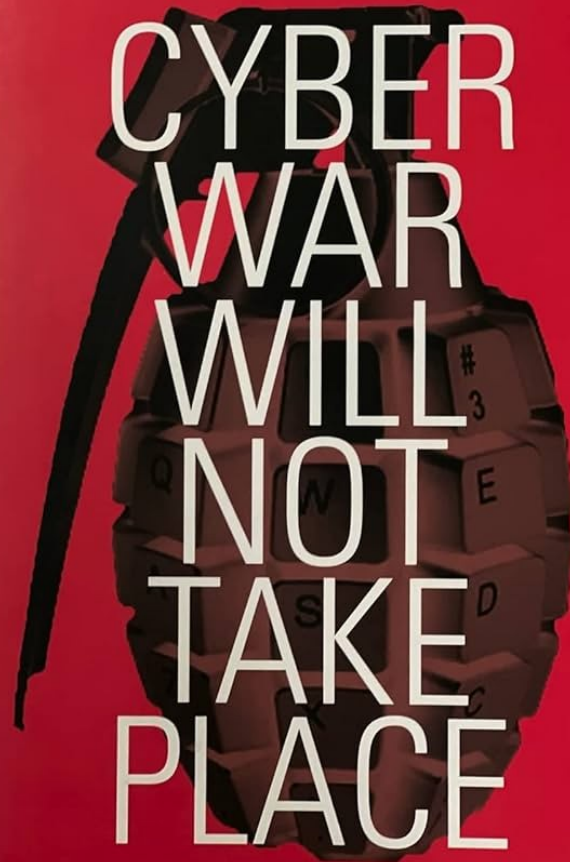
#1 BESTSELLING AUTHOR OF *AGAINST ALL ENEMIES*

**RICHARD A.
CLARKE** AND
ROBERT K.
KNAKE



THOMAS RID

CYBER
WAR
WILL
NOT
TAKE
PLACE



Cyberwar?

- Controversial concept
- A watered-down concept?
- A question of real impacts and severity
- "The use of computers and the Internet to wage war in cyberspace. A set of large-scale, often politically or strategically motivated, related and mutually provoked organised cyberattacks and counterattacks." (Jirásek, Novák and Požár 2013)

What is War?

e.g: At least 2 armed forces (at least one regular)

Organization in battle, organization of defense, strategically planned attacks

A certain level of continuity of armed operations

War from 1,000 casualties/calendar year

should cyberwar be a subset of this?

Violence?

- Clausewitz's concept of war?
- Is instrumental violence with a political aim present?
- "A war in which no one risked his life would be a tournament, a game..." (Huyghe 2011)
- Cyber attacks as a manifestation of secondary violence (RID 2013)

The attribution problem

- Cyberattacks are currently problematic to attribute to actors
- Attribution to State actors
- Rid: "History knows no unattributed wars"
- Gartzke: "Politically motivated conflict will be attributed"

Continuity

- War is not an isolated phenomenon!
- The requirement for a long-term organized strategy
- Is long-term cyber warfare possible?
- Is it possible to win a war through cyber means?

Cyber weapons?

- Not bullets and shrapnel, but ones and zeros
- Weapons of Mass Disruption
- (In)ability to cause permanent damage, to subjugate, to conquer?
- Limited capabilities by target type
- Gartzke's "perishable nature of CW"

Forms of cyber operations (E. Gartzke)

as a Substitute

- takes place instead of a conventional one

as a Complement

- in support and in conjunction of a conventional one

as an Independent tool

- to achieve completely separate results

Types of cyberattack (by T. Rid)

- Sabotage
- Espionage
- Subversion

is any of that war?

Cyberwar?

- So what is cyber warfare?
- Is it possible to win a war through cyber means?
- Are espionage and sabotage acts of war?