Alberto Cammozzo

Università degli Studi di Padova

Corso di laurea triennale in *Diritto dell'Economia*

Insegnamento di *Informatica Giuridica*

A.A. 2015/2016

11, 12, 18 e 19 maggio

12 maggio

5/ ***Lawful Interception*** e “Trojan di Stato”

6/ Telefonia Cellulare: SS7, Stingray

7/ **Cifratura** dei dati

8/ vari tipi di **Censura** online e il caso **Wikileaks**. Aggiramento con TOR, VPN. **Darkweb, deepweb.**

12 maggio

5/ ***Lawful Interception*** e “captatore informatico”

6/ Telefonia Cellulare: SS7, Stingray

7/ **Cifratura** dei dati

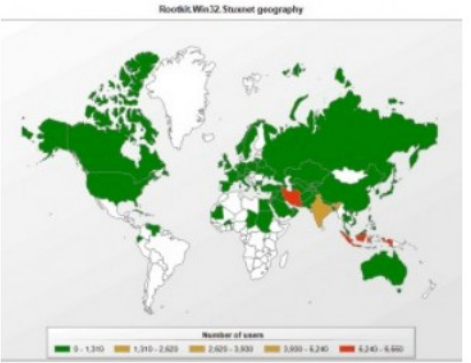
8/ vari tipi di **Censura** online e il caso **Wikileaks**. Aggiramento con TOR, VPN. **Darkweb, deepweb.**

Quando il virus informatico diventa un affare di Stato

Cresce esponenzialmente nel mondo il mercato dei software nocivi venduti ai governi per tenere sotto controllo gruppi antagonisti e criminali, ma il pericolo che questi programmi si trasformino in armi di repressione è dietro l'angolo. E' la guerra sporca del terzo millennio. Ecco perché

di MATTEO CAMPOFIORITO

Lo leggo dopo



SORVEGLIARE e punire. I governi mondiali sembrano aver scoperto che il controllo delle voci contrarie o eversive non passa solo dalle intercettazioni telefoniche. Le comunicazioni dei gruppi "antagonisti" sono sempre più digitali: email, Skype, social network, questi sono i mezzi che vengono usati più spesso. Ecco perché i governi hanno bisogno di metterli sotto controllo ricorrendo anche a strumenti illeciti come i "trojan", software nocivi usati fino a poco tempo fa solo da hacker "black hat", i cattivi della Rete insomma.

APPROFONDIMENTI

ARTICOLO
Cina, torna libero Wang Xiaoning il dissidente tradito da Yahoo!

La lista dei paesi che hanno scelto la guerra cibernetica con armi non convenzionali si allunga di giorno in giorno. Gli **Stati Uniti** sono stati (probabilmente) i precursori di una tendenza arrivando a creare la prima arma di distruzione di massa informatica, il virus Stuxnet che ha avuto l'obiettivo di colpire e rendere inagibili le centrali nucleari iraniane. Probabilmente anche altri virus come "Flame", "Duqu" e il recente "Gauss" (fresca scoperta della società di antivirus Kaspersky), potrebbero essere frutto di una joint-venture informatica tra Stati Uniti e Israele contro i nemici comuni in Medio Oriente. E stando alle ultime rivelazioni del blogger Richard Silverstein, **Israele** potrebbe presto andare oltre portando una massiccia offensiva cibernetica contro l'Iran, paralizzandone le comunicazioni informatiche.

Ad oggi, **Germania**, **Egitto**, **Siria**, **Bahrain** e **Marocco** hanno fatto ricorso a strumenti informatici "poco ortodossi" per sorvegliare (e punire) criminali, gruppi poco graditi o voci antagoniste ai governi in carica. Tra tutti i paesi citati solo la Germania ha pubblicamente ammesso di aver usato un trojan per infettare i computer di gruppi criminali e poterne fermare i traffici. I casi più interessanti però riguardano il Bahrain e il Marocco, gli ultimi due paesi ad essere stati "pizzicati" (anche se non vi è nessuna conferma ufficiale da parte di entrambi) ad usare software per il controllo remoto.

Intercettazioni: Cassazione, sì a virus spia ma solo in indagini per mafia e terrorismo

Lo schema di come avvengono le comunicazioni via smartphone

Ammesso con dei limiti l'uso della captazione. Ma per il deputato e pioniere di Internet, Stefano Quintarelli, "c'è un vuoto normativo che va colmato. I trojan, totalmente invisibili, mettono a rischio la privacy: consentono di conoscere i segreti più intimi delle persone". Depositato alla Camera un progetto di legge. Non si può più parlare di "ascolti" in senso tradizionale

di ALBERTO CUSTODERO

CORTE SUPREMA DI CASSAZIONE

SEZIONI UNITE PENALI

INFORMAZIONE PROVVISORIA N° 15

C.C.	**28 aprile 2016**
Presidente:	**CANZIO**
Relatore:	**ROMIS**
Estensore:	**ROMIS**
Ricorrente:	**SCURATO**
N.R.G.:	**6889/2016**

P.G.: ROSSI (Conf.)

Questione controversa:
Se - anche nei luoghi di privata dimora *ex* art. 614 cod. pen., pure non singolarmente individuati e anche se ivi non si stia svolgendo l'attività criminosa - sia consentita l'intercettazione di conversazioni o comunicazioni tra presenti, mediante l'installazione di un "captatore informatico" in dispositivi elettronici portatili (ad es., *personal computer, tablet, smartphone* ecc.).

Soluzione adottata:
Affermativa, limitatamente a procedimenti relativi a delitti di criminalità organizzata, anche terroristica (a norma dell'art. 13 d.l. n. 152 del 1991), intendendosi per tali quelli elencati nell'art. 51, commi 3-*bis* e 3-*quater*, cod. proc. pen., nonché quelli comunque facenti capo a un'associazione per delinquere, con esclusione del mero concorso di persone nel reato.

Intercettazioni col trojan, parziale sì della Cassazione

Via libera della Corte a intercettazioni ambientali via captatore informatico criminalità organizzata e terrorismo

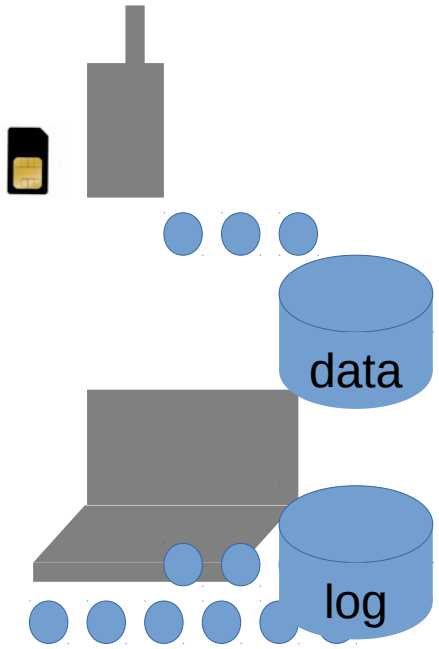
CAROLA FREDIANI 29/04/2016

Non è esattamente uno sdoganamento, ma come tale potrebbe essere interpretato. Ieri le sezioni unite della Cassazione hanno dato un via libera, per quanto circoscritto a un preciso ambito di utilizzo, all'uso di trojan (o captatori informatici) su dispositivi portatili - come pc, tablet e cellulari. Il caso specifico

VIDEO CONSIGLIAT
Galimberti li
Formigoni: "
checca è un
Kakebo. Il lib
casa. Il meto
per imparare

Acquisizione
di prove informatiche (digital evidence)

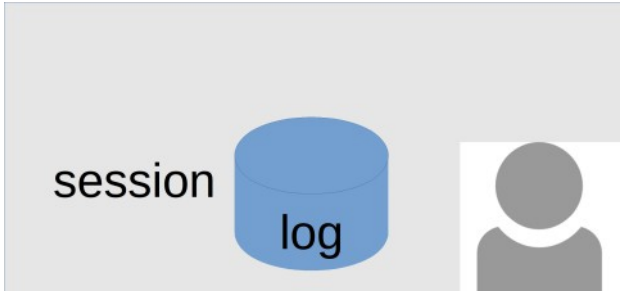
- Acquisizione/Sequestro di **dati conservati** (*retained data*)
- **Intercettazione** di dati in transito (*real time data interception*)
- **Captazione** dei dati all'origine (*remote access search*) “perquisizione” con un “virus” (NIT – *network investigation toolkit*) da installare presso un bersaglio ignaro



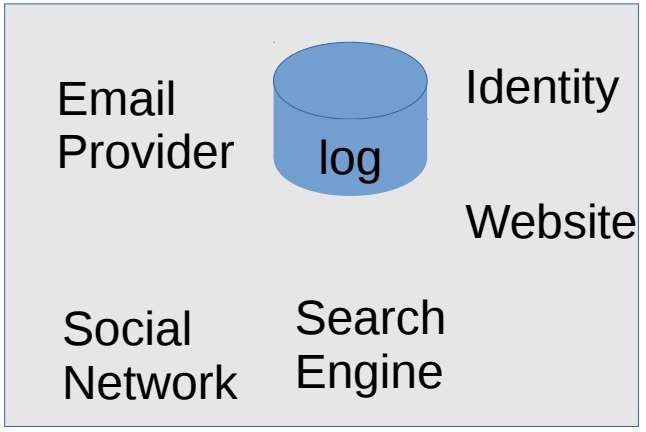
User/ Customer

ISP

Ad Exchange

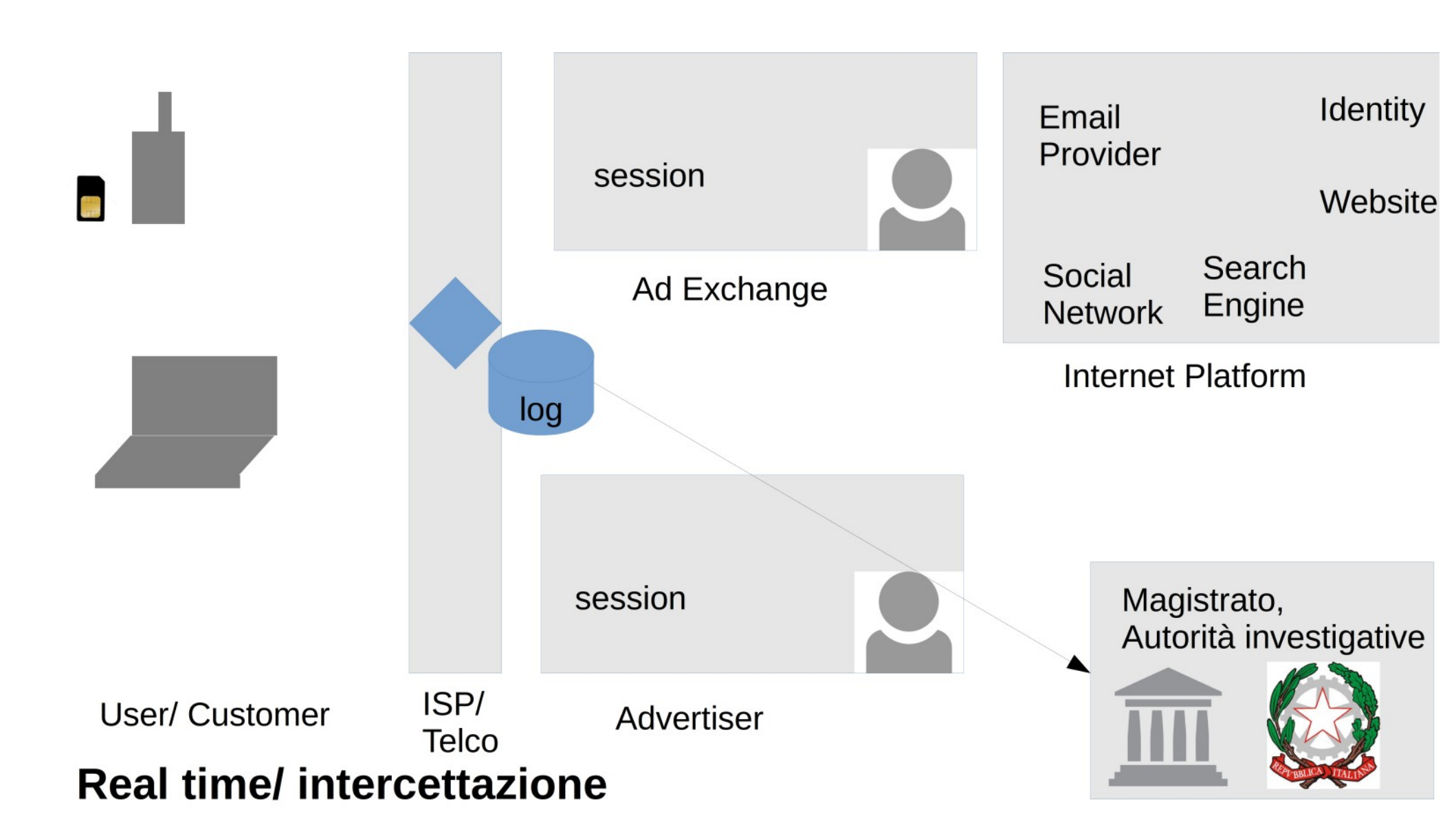


Advertiser

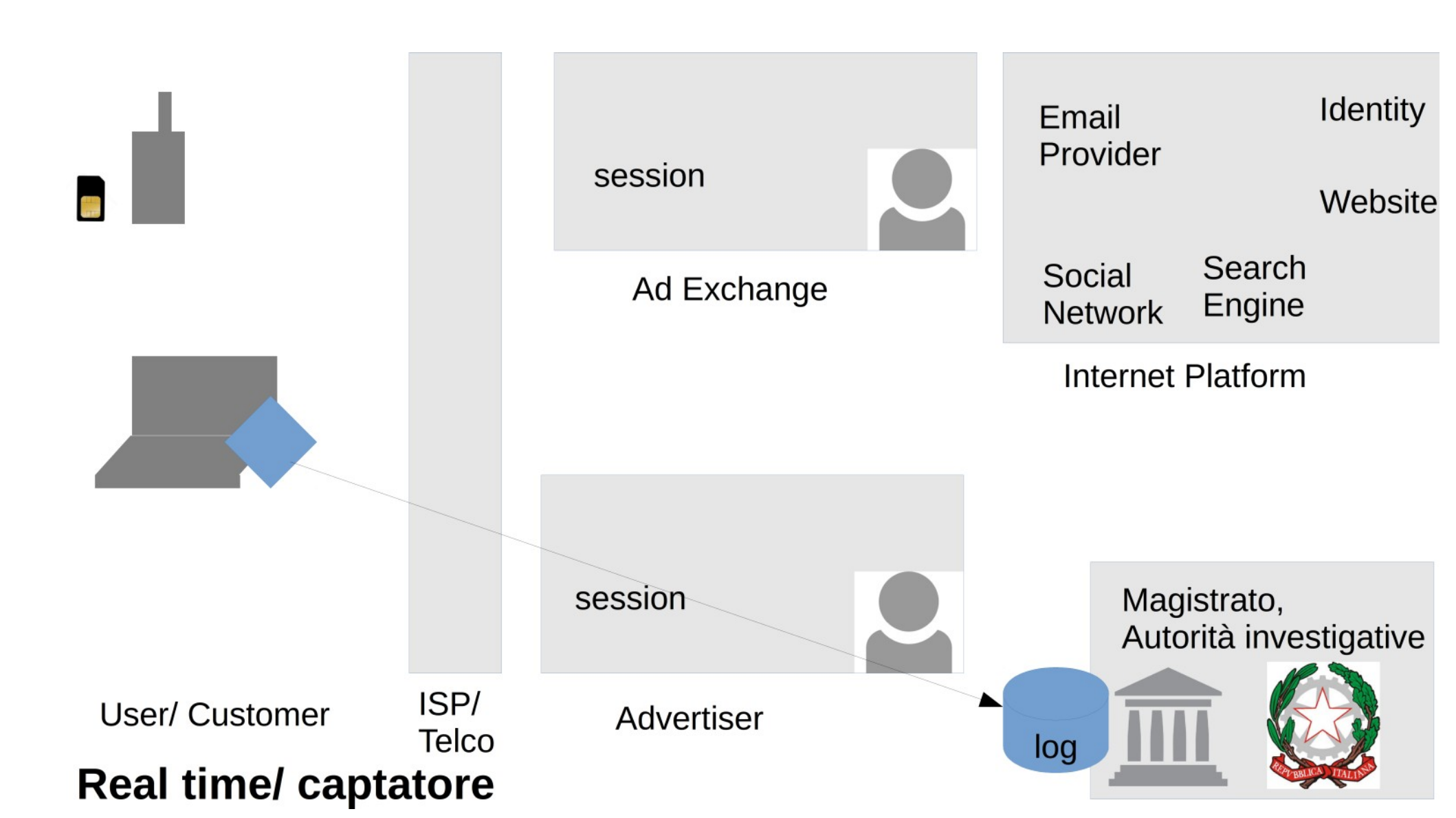


Internet Platform

Retained Data/ sequestro

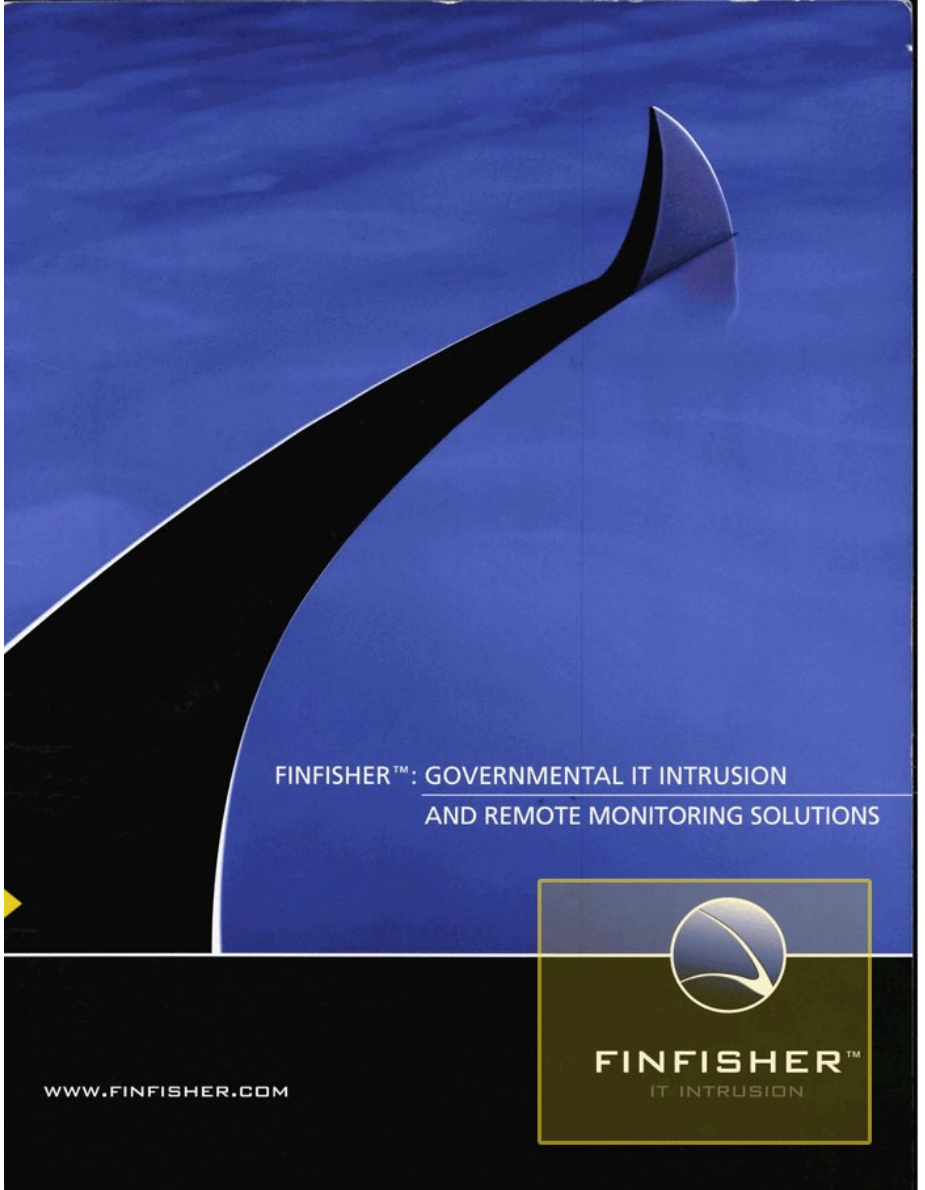


Real time/ intercettazione



Real time/ captatore

Può l'accusato essere ritenuto responsabile per il materiale contenuto in un computer la cui sicurezza è dimostrabilmente stata compromessa dal Network Investigation Toolkit (NIT)?



FINSPY

FinSpy is a field-proven Remote Monitoring Solution that enables Governments to face the current challenges of **monitoring Mobile and Security-Aware Targets** that regularly **change location**, use **encrypted and anonymous communication** channels and **reside in foreign countries**.

Traditional Lawful Interception solutions **face new challenges** that can only be **solved using active systems** like FinSpy:

- Data not transmitted over any network
- Encrypted Communications
- Targets in foreign countries

FinSpy has been **proven successful** in operations around the world **for many years**, and valuable intelligence has been gathered about Target Individuals and Organizations.

When FinSpy is installed on a computer system it can be **remotely controlled and accessed** as soon as it is connected to the internet/network, **no matter where in the world** the Target System is based.

QUICK INFORMATION	
Usage:	· Strategic/Tactical Operations
Capabilities:	· Remote Computer Monitoring · Monitoring of Encrypted Communications
Content:	· Hardware/Software

Usage Example 1: Intelligence Agency

FinSpy was installed on several computer systems inside **Internet Cafes in critical areas** in order to monitor them for suspicious activity, especially **Skype communications** to foreign individuals. Using the Webcam, pictures of the Targets were taken while they were using the system.

Usage Example 2: Organized Crime

FinSpy was **covertly deployed on the Target Systems** of several members of an Organized Crime Group. Using the **country tracing and remote microphone** access, essential information could be gathered from **every meeting that was held** by this group.

Feature Overview

Target Computer – Example Features:

- Bypassing of 40 regularly tested Antivirus Systems
- **Covert Communication** with Headquarters
- Full **Skype Monitoring** (Calls, Chats, File Transfers, Video, Contact List)
- Recording of **common communications** like Email, Chats and Voice-over-IP
- **Live Surveillance** through Webcam and Microphone
- **Country Tracing** of Target
- **Silent extracting of Files** from Hard-Disk
- **Process-based Key-logger** for faster analysis
- **Live Remote Forensics** on Target System
- **Advanced Filters** to record only important information
- Supports most common Operating Systems (**Windows, Mac OSX** and **Linux**)

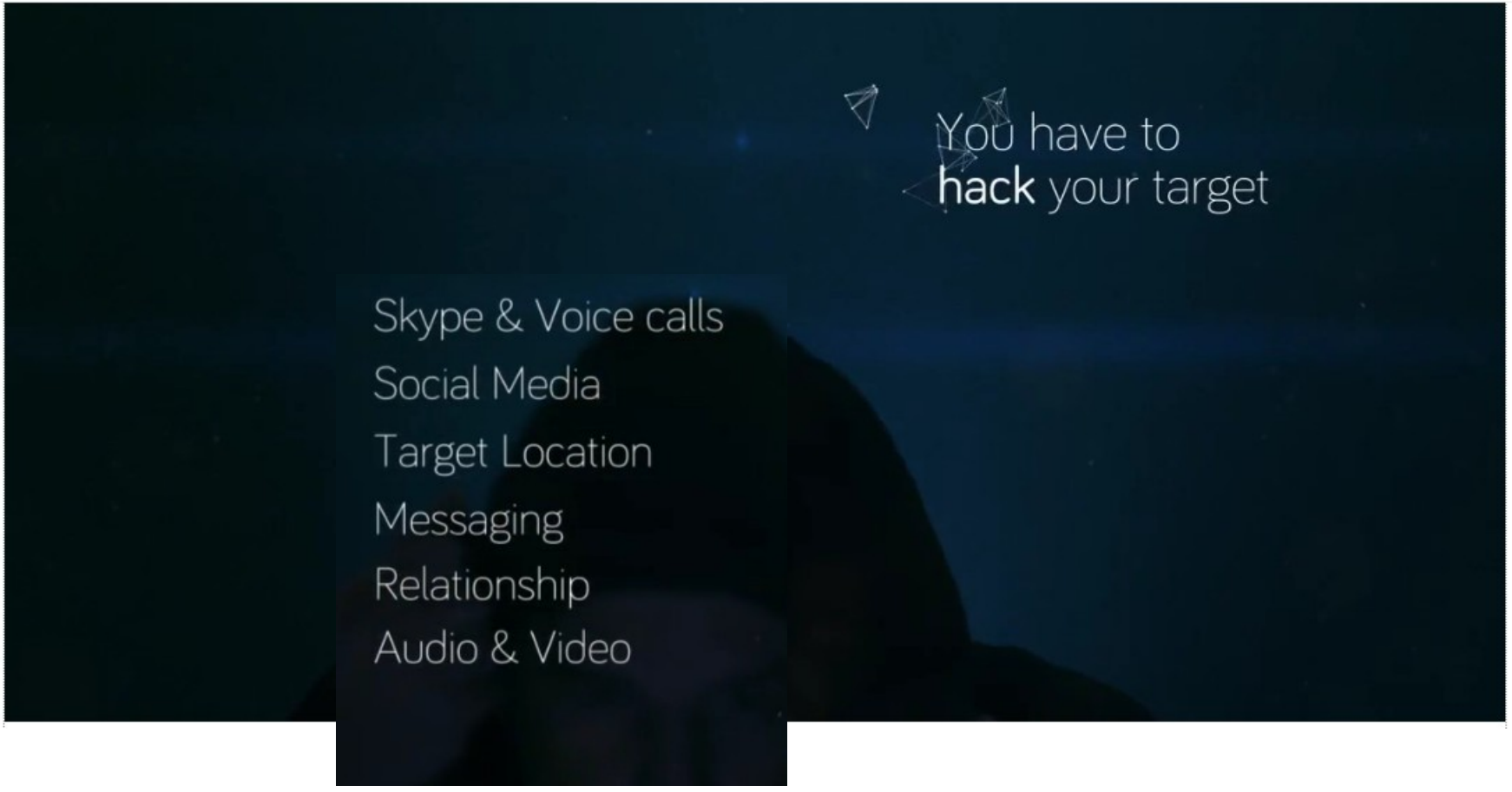
Headquarters – Example Features:

- Evidence Protection (Valid Evidence according to **European Standards**)
- **User-Management** according to Security Clearances
- Hidden from Public through **Anonymizing Proxies**
- Can be **fully integrated** with Law Enforcement Monitoring Functionality

For a full feature list, please refer to the Product Specifications.

FINFISHER™
IT INTRUSION
WWW.FINFISHER.COM

We believe that fighting crime should be easy: we provide effective, easy-to-use offensive technology to the worldwide law enforcement and intelligence communities.


You have to
hack your target
Skype & Voice calls
Social Media
Target Location
Messaging
Relationship
Audio & Video

Customer	Country	Area	Agency	Year First Sale	Annual Maintenance Fees	Total Client Revenues
Polizia Postale e delle Comunicazioni[46]	Italy	Europe	LEA	2004	€100,000	€808,833
Centro Nacional de Inteligencia[47]	Spain	Europe	Intelligence	2006	€52,000	€538,000
Infocomm Development Authority of Singapore	Singapore	APAC	Intelligence	2008	€89,000	€1,209,967
Information Office	Hungary	Europe	Intelligence	2008	€41,000	€885,000
CSDN	Morocco	MEA	Intelligence	2009	€140,000	€1,936,050
UPDF (Uganda Peoples Defense Force), ISO (Internal Security Organization), Office of the President	Uganda	Africa	Intelligence	2015	€831,000	€52,197,100
Italy - DA - Rental	Italy	Europe	Other	2009	€50,000	€628,250
Malaysian Anti-Corruption Commission	Malaysia	APAC	Intelligence	2009	€77,000	€789,123
PCM	Italy	Europe	Intelligence	2009	€90,000	€764,297
SSNS - Ungheria	Hungary	Europe	Intelligence	2009	€64,000	€1,011,000
CC - Italy	Italy	Europe	LEA	2010	€50,000	€497,349
Al Mukhabarat Al A'amah	Saudi Arabia	MEA	Intelligence	2010	€45,000	€600,000
IR Authorities (Condor)	Luxembourg	Europe	Other	2010	€45,000	€446,000
La Dependencia y/o CISEN[48]	Mexico	LATAM	Intelligence	2010	€130,000	€1,390,000
UZC[49]	Czech Republic	Europe	LEA	2010	€55,000	€689,779
Egypt - MOD[49]	Egypt	MEA	Other	2011	€70,000	€598,000
Federal Bureau of Investigation[50]	USA	North America	LEA	2011	€100,000	€697,710
Oman - Intelligence	Oman	MEA	Intelligence	2011	€30,000	€500,000
President Security[51][52]	Panama	LATAM	Intelligence	2011	€110,000	€750,000
Turkish National Police	Turkey	Europe	LEA	2011	€45,000	€440,000
UAE - MOI	UAE	MEA	LEA	2011	€90,000	€634,500
National Security Service[49]	Uzbekistan	Europe	Intelligence	2011	€50,000	€917,038
Department of Defense[50]	USA	North America	LEA	2011		€190,000
Bayelsa State Government	Nigeria	MEA	Intelligence	2012	€75,000	€450,000
Estado del Mexico	Mexico	LATAM	LEA	2012	€120,000	€783,000
Information Network Security Agency	Ethiopia	MEA	Intelligence	2012	€80,000	€750,000
State security (Falcon)	Luxemburg	Europe	Other	2012	€38,000	€316,000
Italy - DA - Rental	Italy	Europe	Other	2012	€60,000	€496,000
MAL - MI	Malaysia	APAC	Intelligence	2012	€77,000	€552,000
Direction générale de la surveillance du territoire	Morocco	MEA	Intelligence	2012	€160,000	€1,237,500
National Intelligence and Security Service[49]	Sudan	MEA	Intelligence	2012	€76,000	€960,000
Russia - KVANT[53]	Russia	Europe	Intelligence	2012	€72,000	€451,017
Saudi - GID	Saudi	MEA	LEA	2012	€114,000	€1,201,000
SIS of National Security Committee of the Republic of Kazakhstan[49]	Kazakhstan	Europe	Intelligence	2012	€140,000	€1,012,500

Content

This section includes the following topics:

]HackingTeam[

RCS 9

The hacking suite for governmental interception

Technician's Guide

THE WASSENAAR ARRANGEMENT

ON

EXPORT CONTROLS FOR CONVENTIONAL ARMS

AND

DUAL-USE GOODS AND TECHNOLOGIES

LIST OF DUAL-USE GOODS AND TECHNOLOGIES

AND

MUNITIONS LIST

* This Corrigendum is issued to correct 3.A.1.a. and 6.A.5.e.3.b.3. of the Dual-Use List.

The **Wassenaar Arrangement** has been established in order to contribute to regional and international security and stability, by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies, thus preventing destabilising accumulations.

http://www.wassenaar.org/about-us/

Dec 2013

DUAL-USE LIST - CATEGORY 5 – PART 1 – TELECOMMUNICATIONS

5. A. 1. j. IP network communications surveillance systems or equipment, and specially designed components therefor, having all of the following:

1. Performing all of the following on a carrier class IP network (e.g., national grade IP backbone):
   a. Analysis at the application layer (e.g., Layer 7 of Open Systems Interconnection (OSI) model (ISO/IEC 7498-1));
   b. Extraction of selected metadata and application content (e.g., voice, video, messages, attachments); and
   c. Indexing of extracted data; and

2. Being specially designed to carry out all of the following:
   a. Execution of searches on the basis of 'hard selectors'; and
   b. Mapping of the relational network of an individual or of a group of people.

Note *5.A.1.j. does not apply to systems or equipment, specially designed for any of the following:*

a. Marketing purpose;
b. Network Quality of Service (QoS); or
c. Quality of Experience (QoE).

Technical Note

'Hard selectors': data or set of data, related to an individual (e.g., family name, given name, e-mail, street address, phone number or group affiliations).

Conservazione di digital evidence

- Occorre garantire dimostrabilmente che i dati siano
  - originali
  - integri
- Continuità della "*Chain of custody*"
  - Che il supporto **originale** *non possa* aver subito modifiche dopo l'acquisizione
    (danneggiamenti accidentiali o manipolazioni)
  - Che le **copie** forensi siano identiche all'originale
  - Che ogni passaggio nel trattamento sia documentato

Quando si tratta di dati, di informazioni o di programmi informatici, la copia deve essere realizzata su adeguati supporti, mediante procedura che assicuri la conformità della copia all'originale e la sua immodificabilità

Legge 18 marzo 2008, n. 48

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT TACOMA

UNITED STATES OF AMERICA, Plaintiff, v. JAY MICHAUD, Defendant.	No. CR15-5351RJB DEFENDANT'S REPLY TO GOVERNMENT'S RESPONSE TO THIRD MOTION TO COMPEL[1]

least that the Government cannot prove beyond a reasonable doubt that Mr. Michaud intentionally downloaded illegal pictures.

In this regard, it is now undisputed that the Government inserted "malware" onto Mr. Michaud's computer that compromised and overrode its security settings. Therefore, either pornography from "Website A" itself was mistakenly or recklessly sent to his computer, or else the pornography came from other sources (such as viruses or remote users that gained access to the computer) after the security settings on Mr. Michaud's computer had been compromised by the Government's NIT.[3]

Può l'accusato essere ritenuto responsabile per dati contenuti in un computer la cui sicurezza è stata dimostrabilmente compromessa da un malware, seppure usato come strumento di indagine?

12 maggio

5/ ***Lawful Interception*** e “captatore informatico”

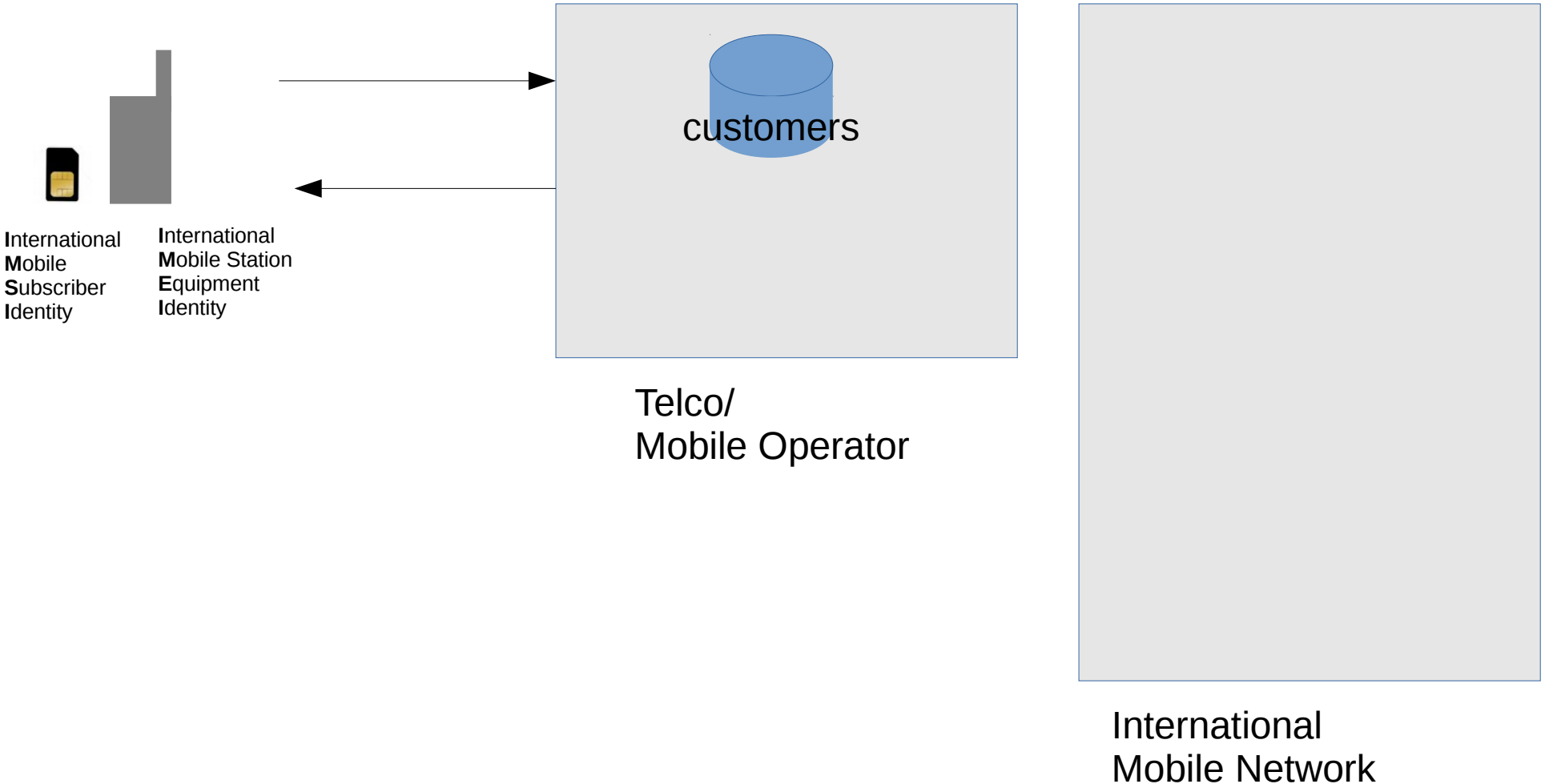
6/ Telefonia Cellulare: SS7, Stingray

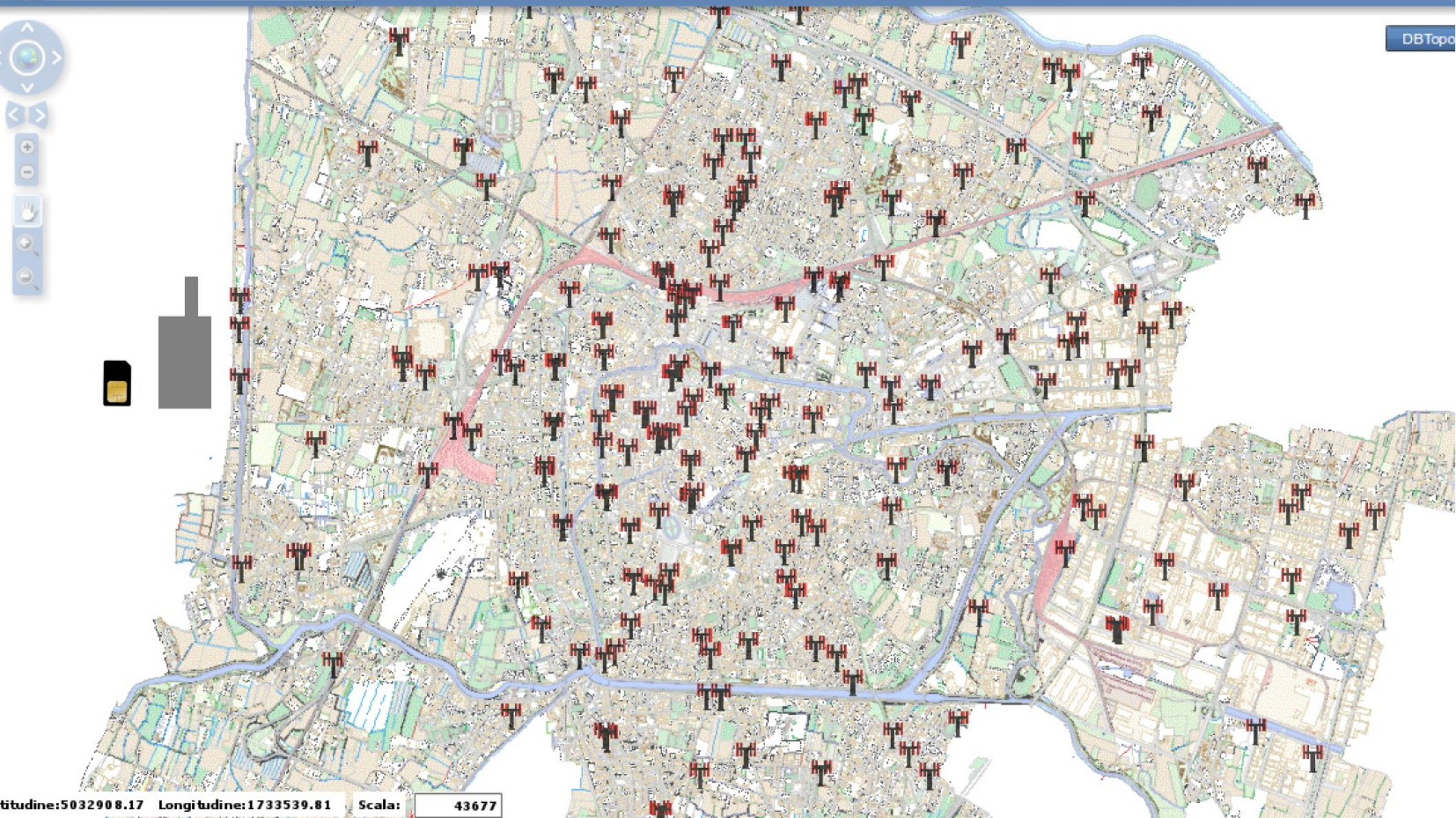
7/ **Cifratura** dei dati

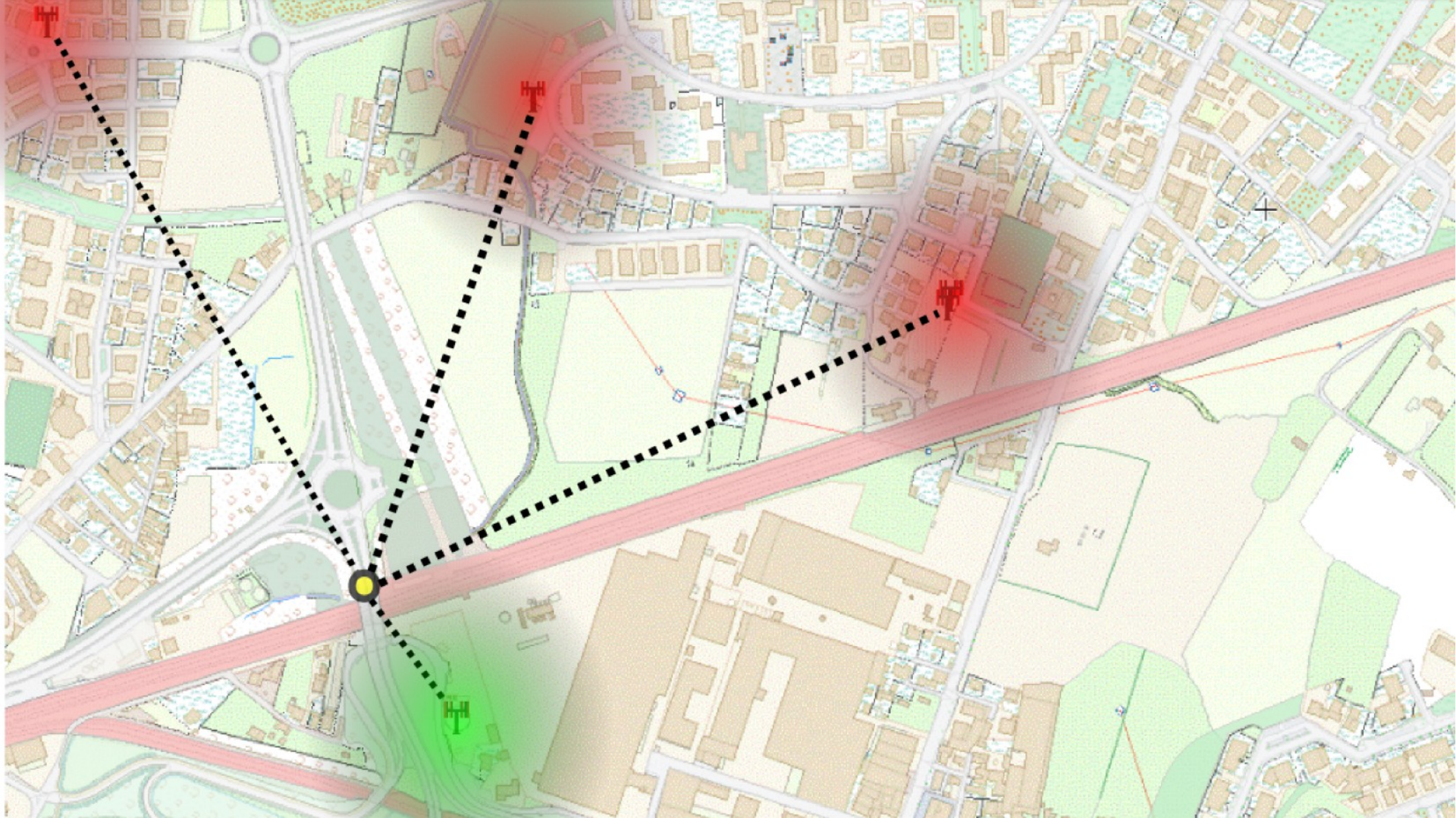
8/ vari tipi di **Censura** online e il caso **Wikileaks**. Aggiramento con TOR, VPN. **Darkweb, deepweb.**

Mobile phone tracking

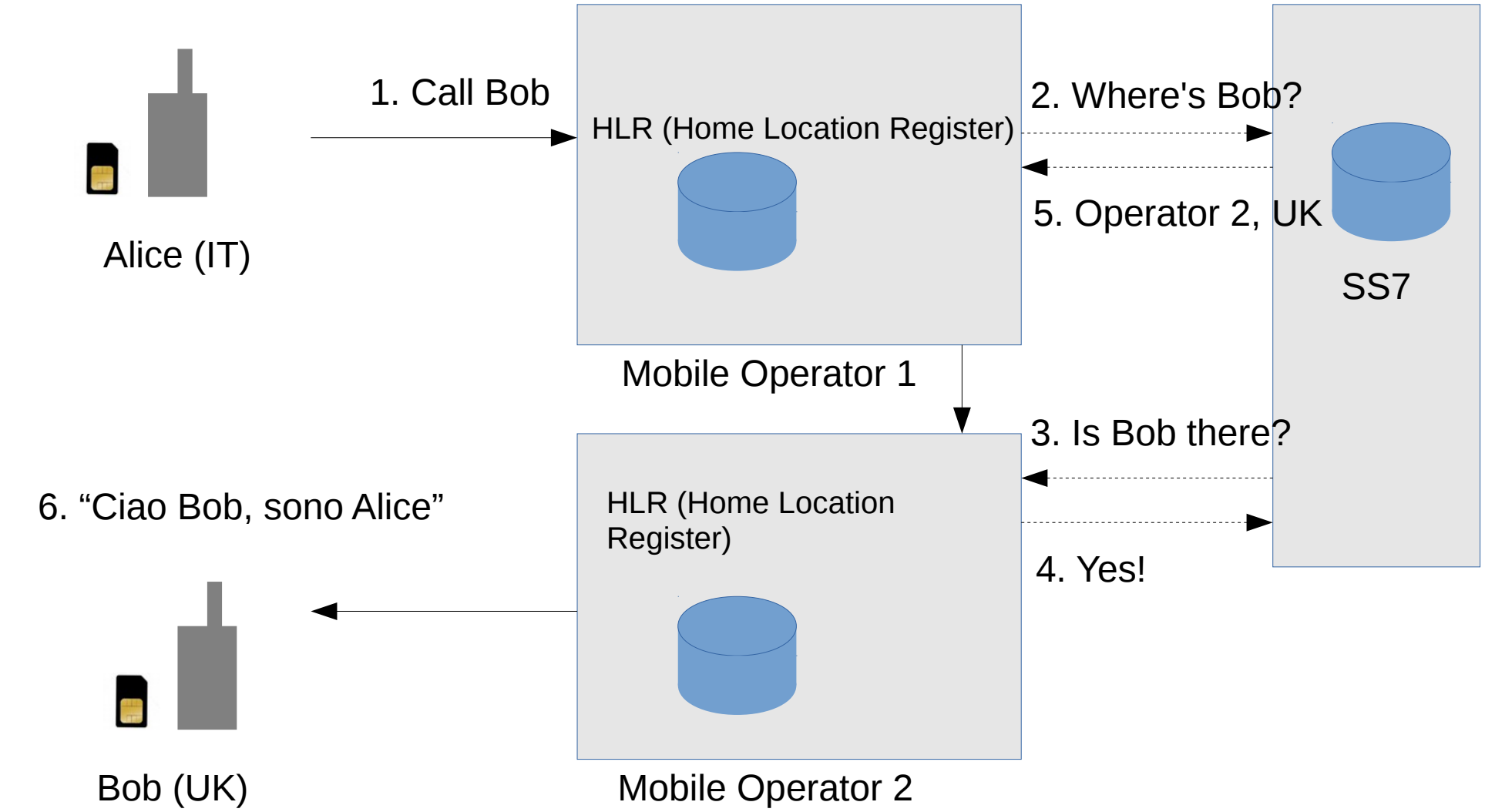
Che succede quando accendete il telefono?

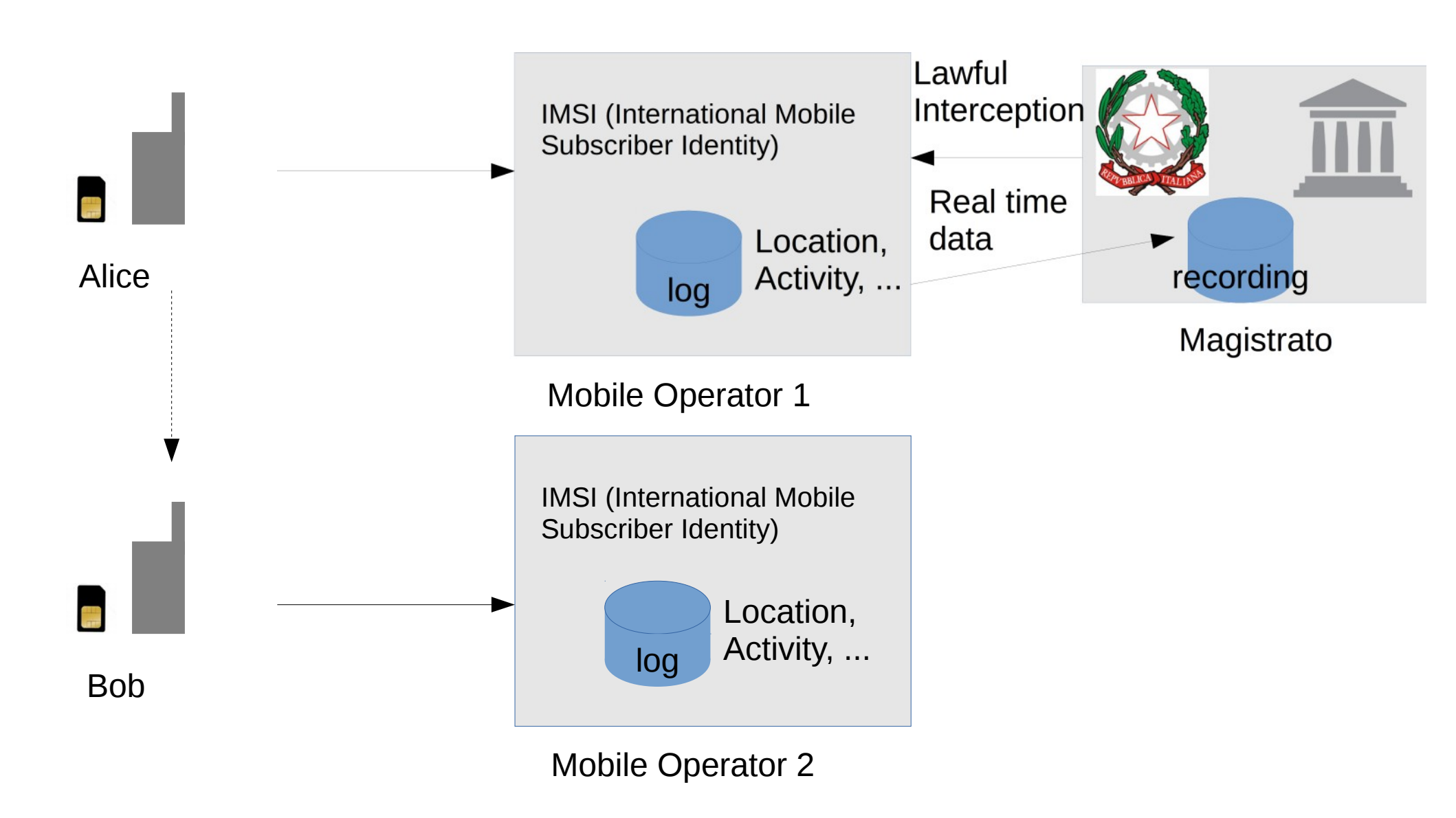

customers
International
Mobile
Subscriber
Identity
International
Mobile Station
Equipment
Identity
Telco/
Mobile Operator
International
Mobile Network


DBTopo
titudine:5032908.17 Longitudine:1733539.81 Scala: 43677



Cosa succede quando faccio una chiamata?


1. Call Bob
HLR (Home Location Register)
2. Where's Bob?
5. Operator 2, UK
SS7
Alice (IT)
Mobile Operator 1
3. Is Bob there?
HLR (Home Location Register)
4. Yes!
6. “Ciao Bob, sono Alice”
Bob (UK)
Mobile Operator 2


Alice
IMSI (International Mobile Subscriber Identity)
log
Location, Activity, ...
Mobile Operator 1
Lawful Interception
Real time data
recording
Magistrato
Bob
IMSI (International Mobile Subscriber Identity)
log
Location, Activity, ...
Mobile Operator 2

Global Dialplan Validator

You can use our free validator tool to verify if your number is in the correct format to be a valid number anywhere in the world.

If your number is verified we'll let you know what type of number it is, the country that the number belongs to and original network information where available.

For current network and number status information you will need to perform a full HLR Lookup by creating an account.

MSISDN [redacted]

Submit

MSISDN	[redacted]	HLR Lookup This Number
Type	Mobile	
Location	Italy	
Region	IT	
Area	National	
Country Code	39	
Original Network	Wind *	
Timezone	Europe/Rome Europe/Vatican	

* Original Network - This does not indicate that this is the network the number currently belongs to due to the possibility of the number being ported. For mobile numbers you will need to perform a full HLR Lookup to access portability information.

SS7: Locate. Track. Manipulate.
You have a tracking device in your pocket

Tobias Engel

Chaos Computer Club Congress 2014

Companies are now **selling the ability to track your phone number** wherever you go. With a precision of up to 50 meters, detailed movement profiles can be compiled by somebody from the other side of the world without you ever knowing about it. But that is just the tip of the iceberg.

SkyLock™ Product Description

Locate. Track. Manipulate.

VERINT

POWERING ACTIONABLE INTELLIGENCE

History Module - Recalling targets past movements

The History module enables simple recollection and filtering of all SkyLock query results, alerts and notifications. This includes single queries as well as automatic (recurring queries). The main SkyLock functions which rely on the history module include:

Figure 5 – SkyLock tabular history screen

DEFENTEK

Vital Solutions

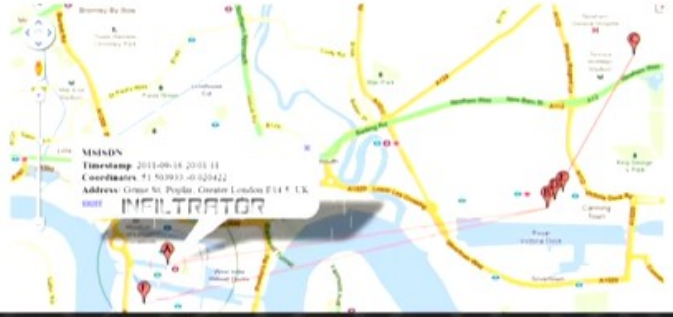
The **Infiltrator Real-Time Tracking System** is an innovative tool for governmental and security organizations that require real-time data about suspects' location and movement.

INFILTRATOR

Innovative Location Technology

The combination of the **Infiltrator Real-Time Tracking System** as a strategic location solution and the **Intelligence Interceptor**, a tactical interception and location system, provides accurate, real-time data of target suspects and people of interest by tracking their mobile phones.

The **Infiltrator Real-Time Tracking System** will provide the location (GPS coordination) at a Cell-ID level. The input will be t
target mobile number or the IMSI and the result will show the BTS coordination, where the target is registered on any map.



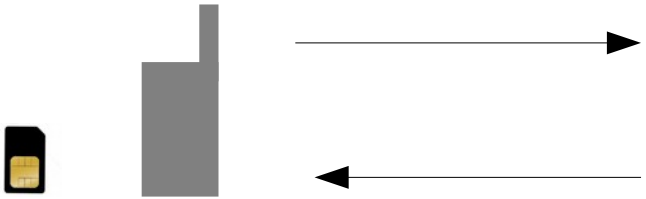
ICE

a new dawn

Signalling System #7 today

- Getting access is easier than ever
  - Can be bought from telcos or roaming hubs for a few hundred euros a month
  - Usually (not always), roaming agreements with other networks are needed, but some telcos are reselling their roaming agreements
  - Some network operators leave their equipment unsecured on the internet
  - Femtocells are part of the core network and have been shown to be hackable

IMSI catcher “Stingray”

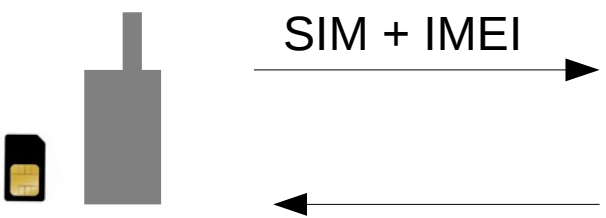


International
Mobile
Subscriber
Identity

International
Mobile Station
Equipment
Identity

IMEI

"The GSM specification requires the handset to authenticate to the network, but does not require the network to authenticate to the handset."



Simulated Mobile Operator

Move In On Target

Accurately locate, intercept, and control GSM and 3G (UMTS) target mobile phones using an active solution

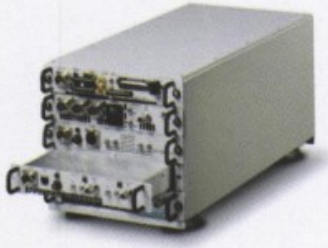
ENGAGE GI2

Highlights

- Accurately locate target using dedicated homing device without disabling target's ability to communicate
- Extract target's mobile phone GPS coordinates on both GSM and UMTS (3G) networks
- Listen to, read, edit, and reroute incoming and outgoing calls and text messages (A5/1 and A5/3 encryption)
- Remotely activate a mobile phone's microphone
- Identify the presence of target mobile phones
- Block cellular communications to neutralize IEDs and more

ENGAGE GI2-M™ Trolley Case

All-in-one portable solution for rapid deployment



ENGAGE GI2 -R™ Rack Mount

Modular units for fixed insta in vehicles and buildings

ENGAGE GI2-C™

Commercial Tracking Providers

- Several commercial providers offer cell-level tracking as service, claim coverage of about 70% of ***worldwide*** mobile subscribers (with some restrictions...)
- Only the MSISDN (phone number) is required to locate a subscriber

communication service providers' collaboration.

- A fully committed solution with a predicted hit rate of 70% and above
- No need for software or hardware changes neither in the network core

The **Infiltrator Real-Time Tracking System** is an innovative tool for governmental and security organizations that require real-time data about suspects' location and movement.

operational.

- The system will not present the location of Israeli subscribers in Israel, and USA subscribers worldwide (country code 972 and 1).
- Target's Location will be based on the target's MSISDN (public mobile number). In most case

12 maggio

5/ ***Lawful Interception*** e “captatore informatico”

6/ Telefonia Cellulare: SS7, Stingray

7/ **Cifratura** dei dati

8/ vari tipi di **Censura** online e il caso **Wikileaks**. Aggiramento con TOR, VPN. **Darkweb, deepweb.**

Crittografia

Alice

Messaggio
“in chiaro”

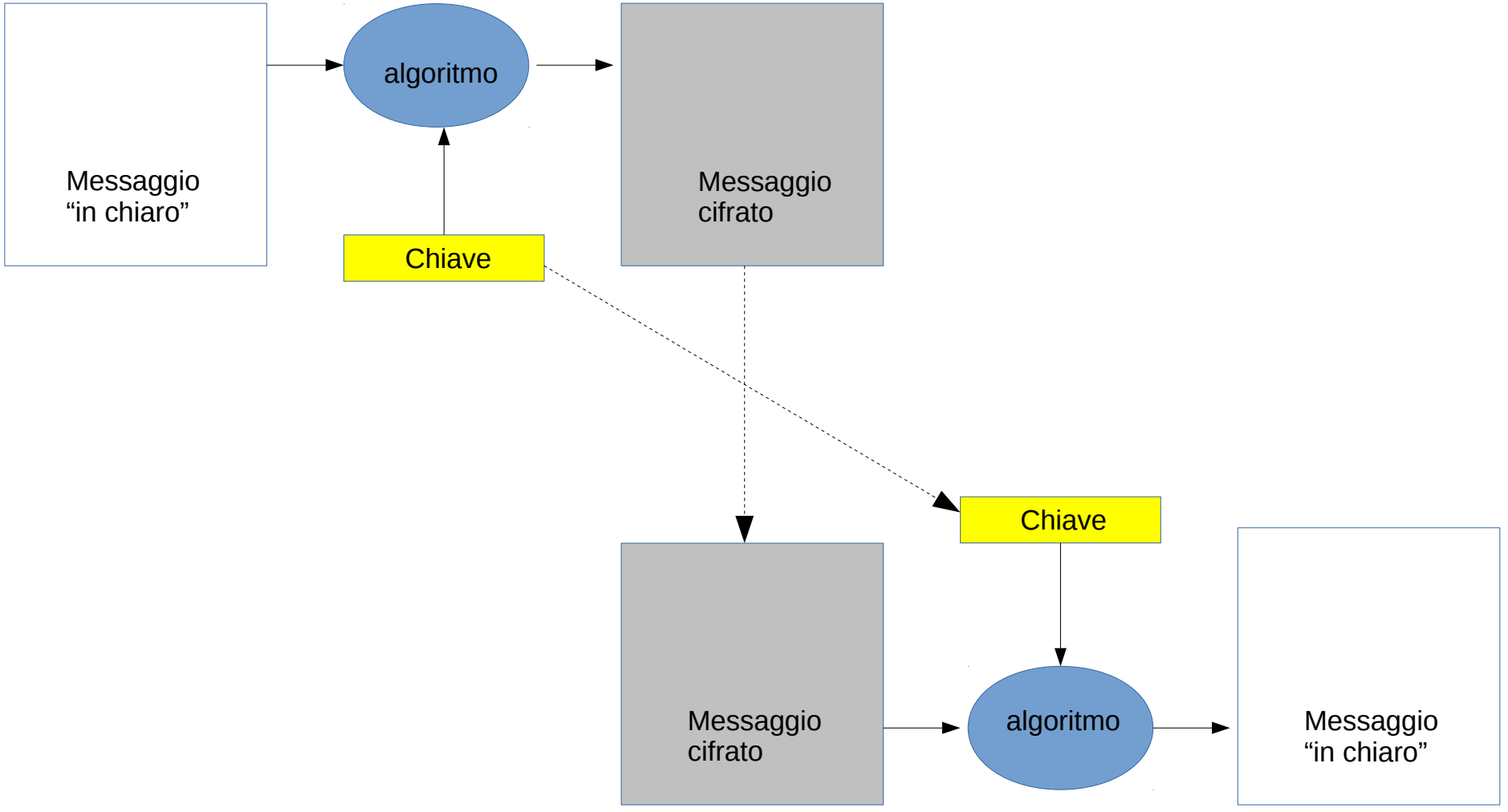
Messaggio
cifrato

Messaggio
“in chiaro”

Bob

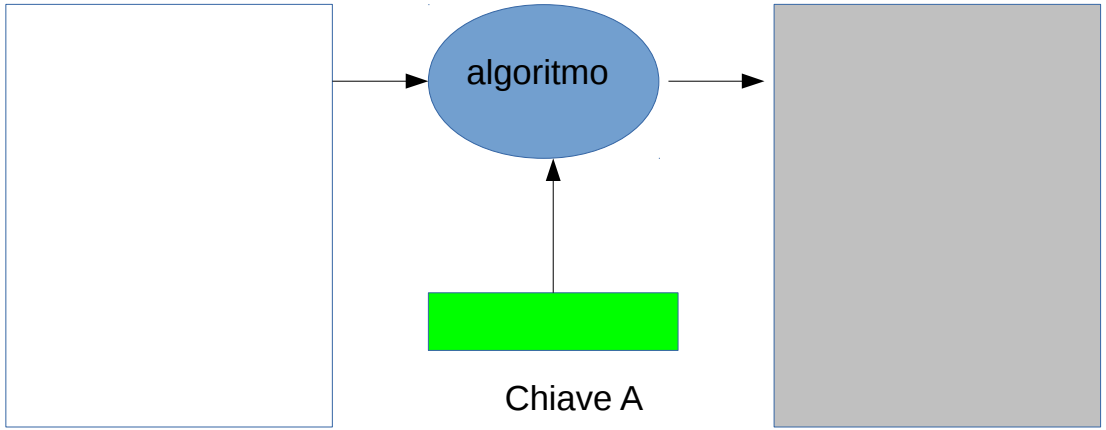
Crittografia Simmetrica

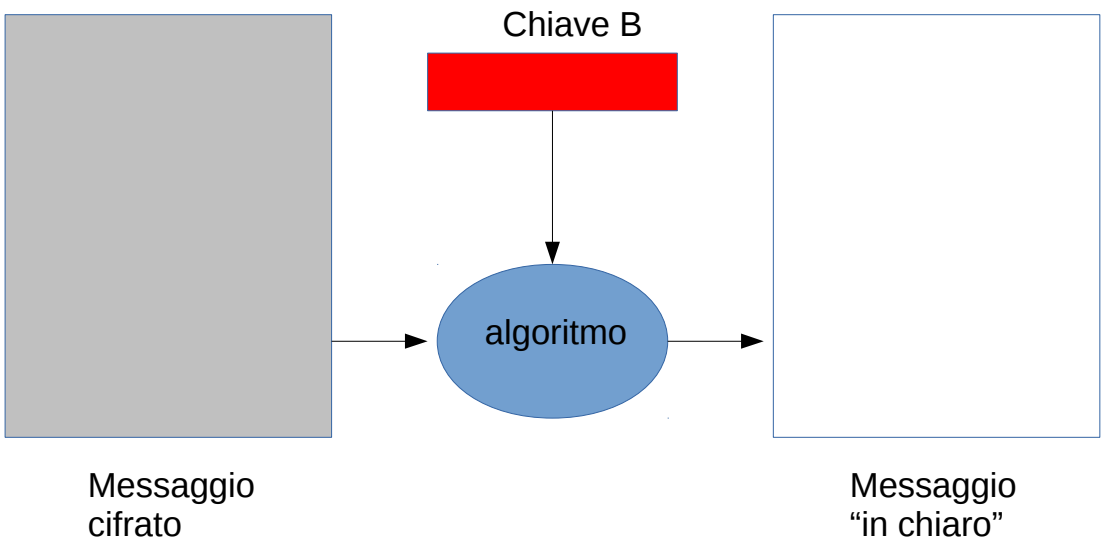
- Stesso algoritmo
- Stessa chiave per cifrare e decifrare
- Problema: come passare la chiave dal mittente al destinatario?

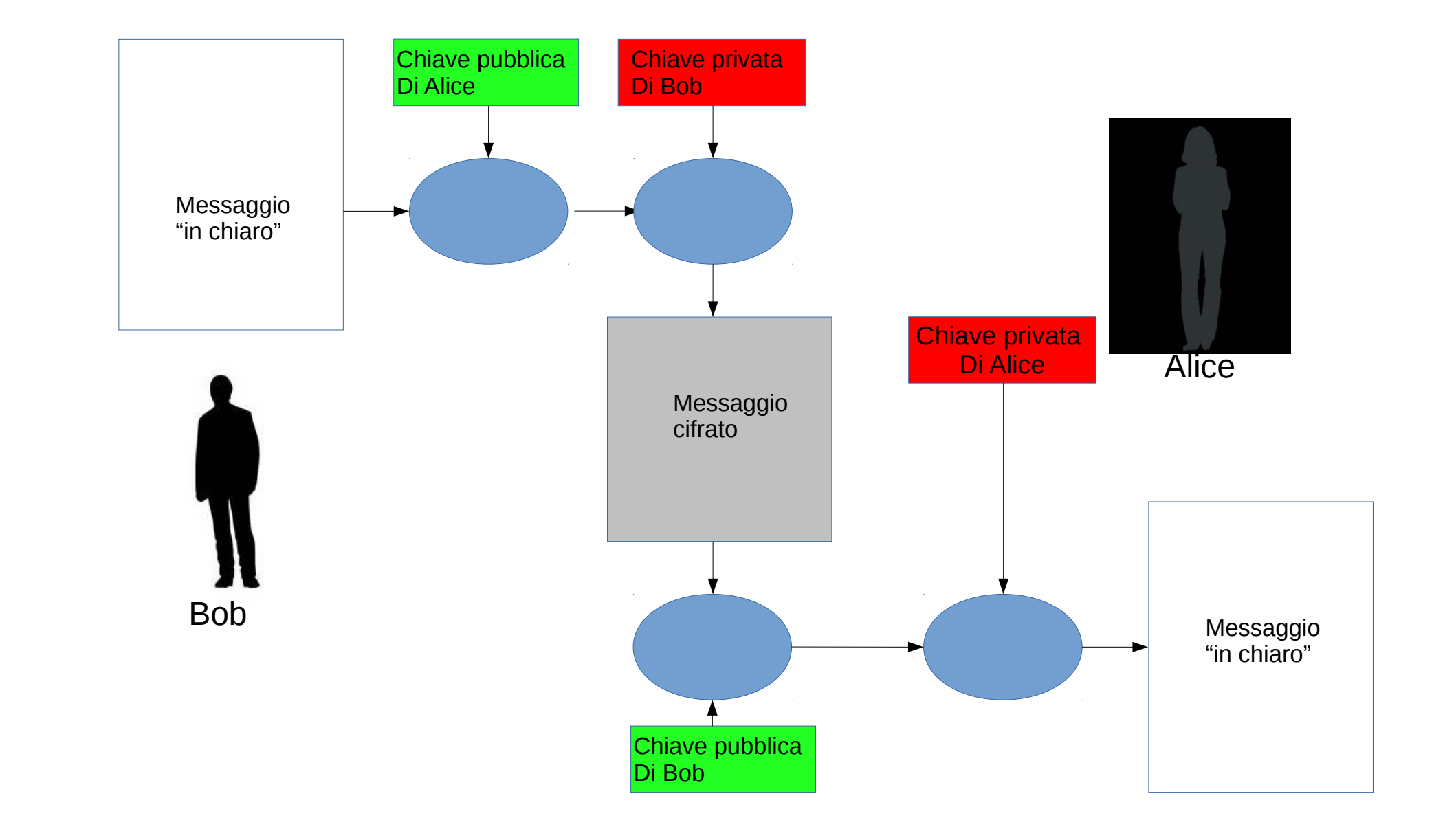

Messaggio
“in chiaro”
algoritmo
Chiave
Messaggio
cifrato
Chiave
Messaggio
cifrato
algoritmo
Messaggio
“in chiaro”

Crittografia Asimmetrica

- Stesso algoritmo
- Ognuno ha una **coppia** di chiavi: una *decifra* quella che l'altra *cifra*
- Si può rendere ***pubblica*** una chiave e **segreta** l'altra (*privata*)
- Problema: distribuzione autorevole delle chiavi pubbliche


algoritmo
Chiave A
Messaggio
“in chiaro”
Messaggio
cifrato


Chiave B
algoritmo
Messaggio
cifrato
Messaggio
“in chiaro”


Messaggio
“in chiaro”
Chiave pubblica
Di Alice
Chiave privata
Di Bob
Messaggio
cifrato
Chiave privata
Di Alice
Alice
Bob
Chiave pubblica
Di Bob
Messaggio
“in chiaro”

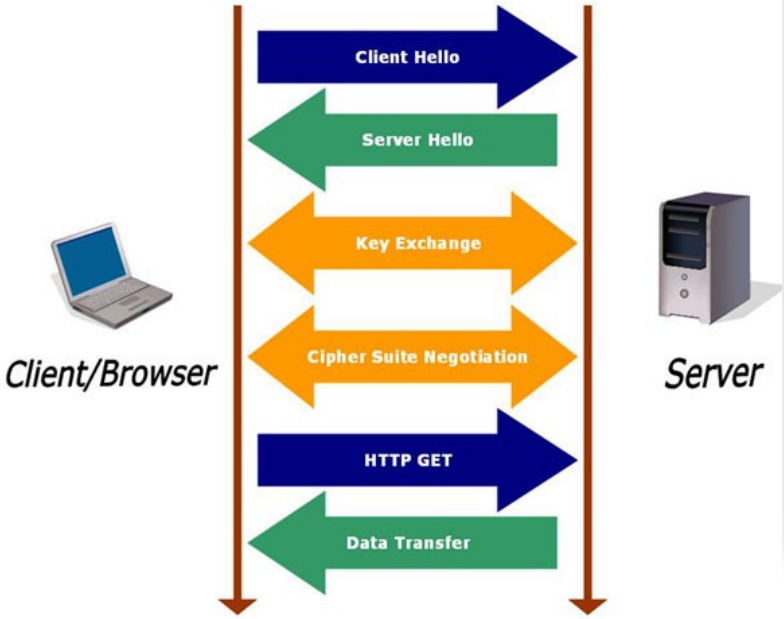
algoritmo

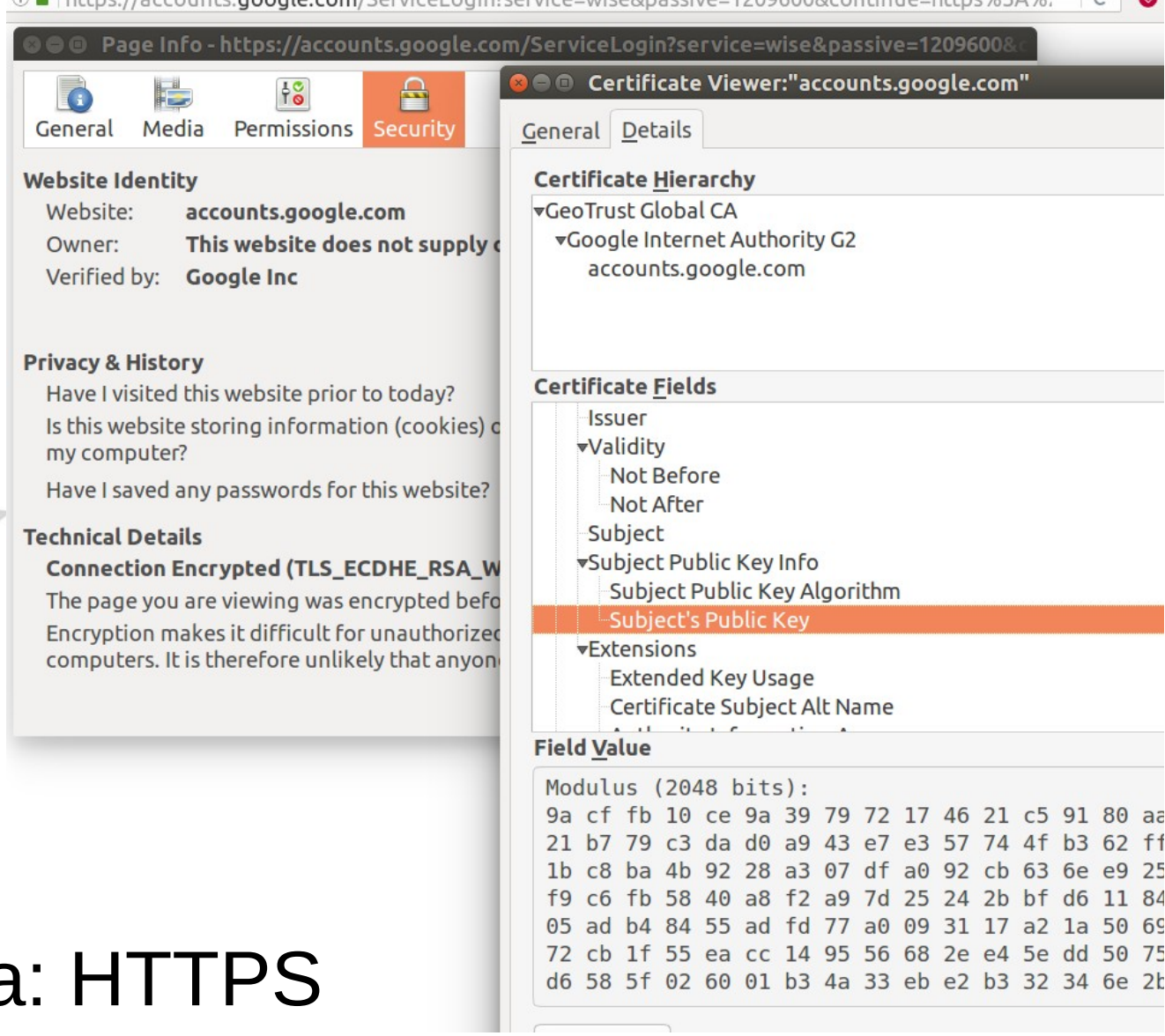
Chiave pubblica
Di Bob

Chiave pubblica
Di Alice

Messaggio
cifrato

?





Navigazione sicura: HTTPS

TECHNOLOGY

The Apple-F.B.I. Case

EDUARDO MUNOZ/REUTERS

Apple's New Challenge: Learning How the U.S. Cracked Its iPhone

The company lacks information on the method used to break into the iPhone of a

ANDREW BURTON FOR THE NEW YORK TIMES

U.S. Says It Has Unlocked iPhone Without Apple

The Justice Department announcement, in a court filing, ends an immediate legal battle over the San Bernardino shooting case but raises questions about Apple's security.

March 29, 2016 · By KATIE BENNER and ERIC LICHTBLAU

American Tech Giants Face Fight in Europe Over Encrypted Data

As Apple battles the F.B.I. over "unlocking" an iPhone, European governments are pushing for greater access to people's digital lives.

March 27, 2016 · By MARK SCOTT

In Apple Debate on Digital Privacy and the iPhone, Questions Still Remain

It is unclear what will happen the next time the government tries to force Apple to break into one of its own phones.

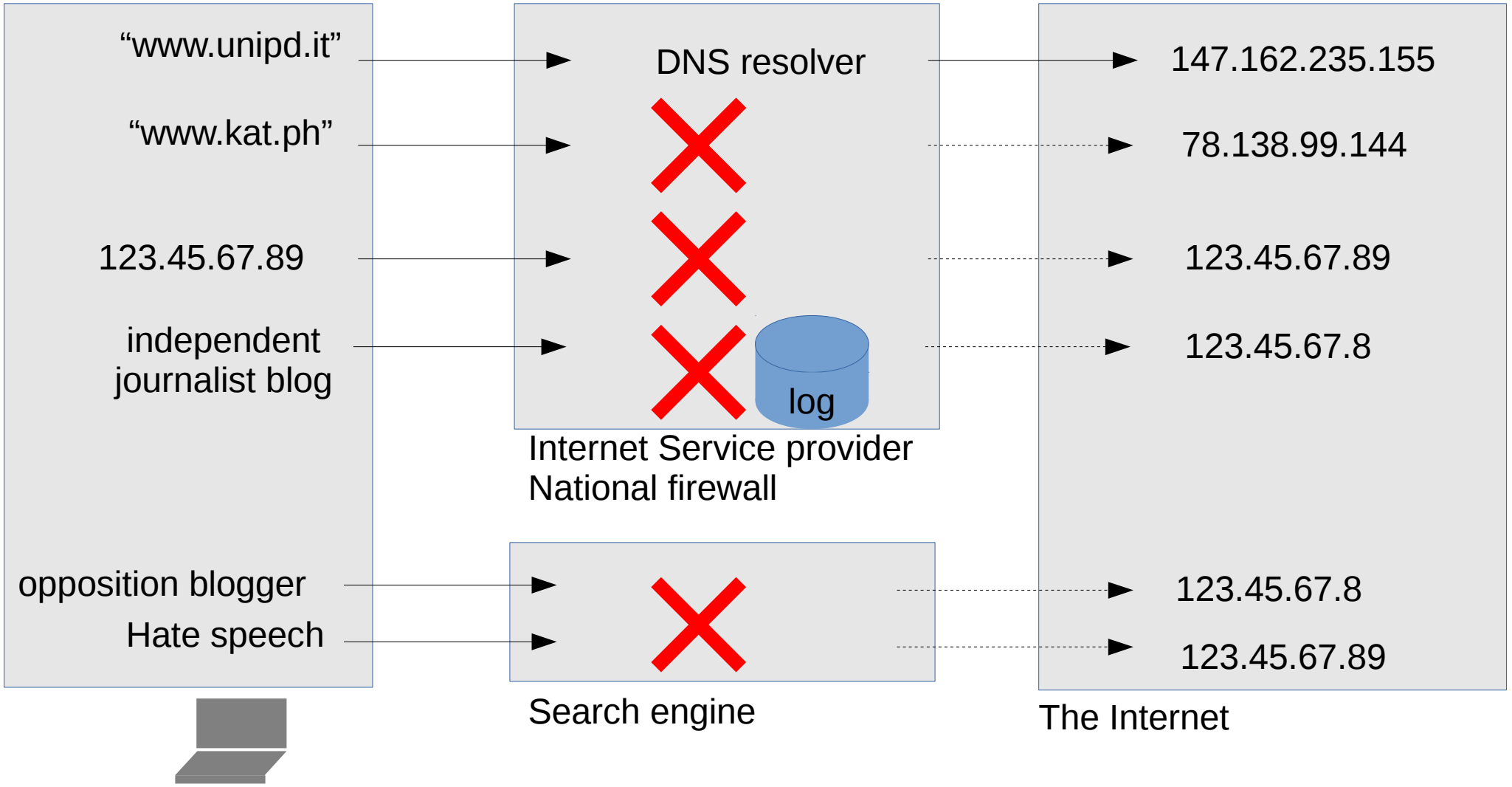
12 maggio

5/ ***Lawful Interception*** e “captatore informatico”

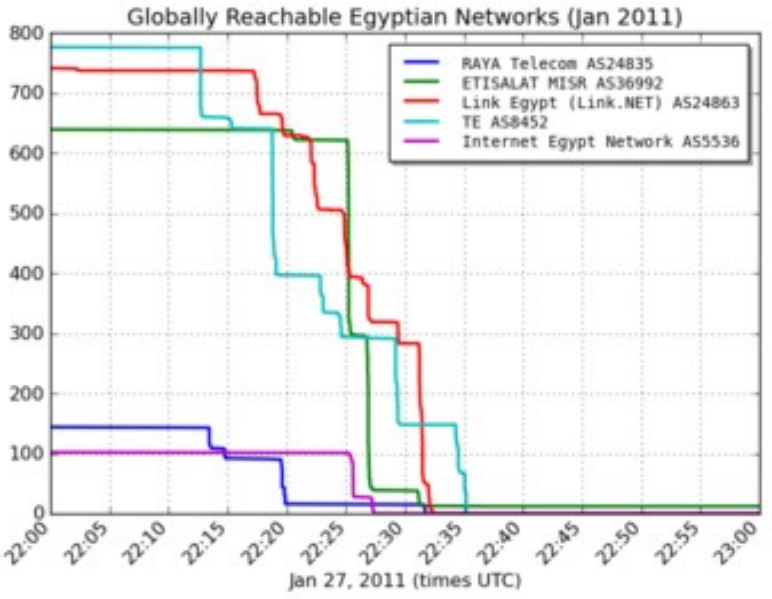
6/ Telefonia Cellulare: SS7, Stingray

7/ **Cifratura** dei dati

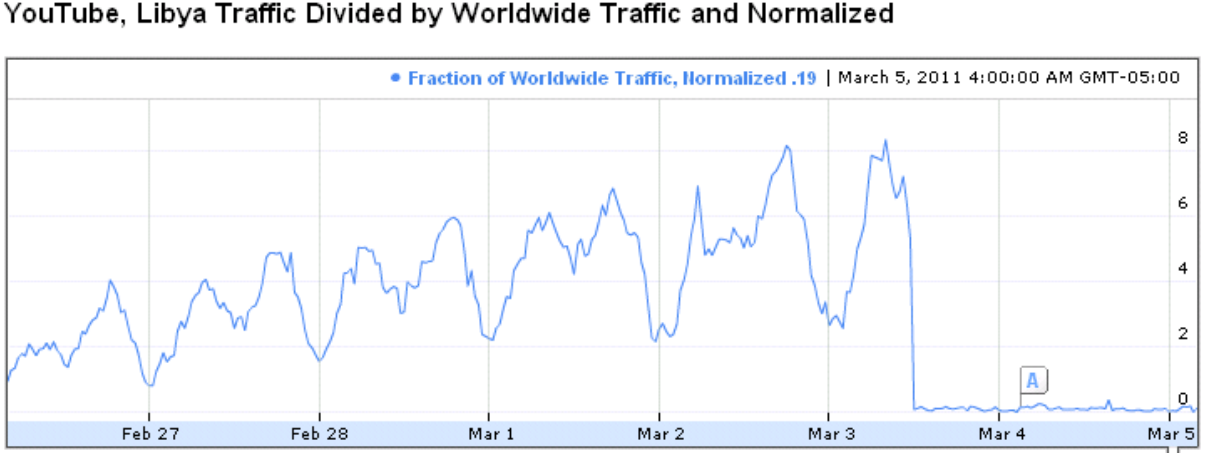
8/ vari tipi di **Censura** online e il caso **Wikileaks**.
Aggiramento con TOR, VPN. **Darkweb, deepweb.**


“www.unipd.it”
“www.kat.ph”
123.45.67.89
independent
journalist blog
opposition blogger
Hate speech
DNS resolver
log
Internet Service provider
National firewall
Search engine
147.162.235.155
78.138.99.144
123.45.67.89
123.45.67.8
123.45.67.8
123.45.67.89
The Internet

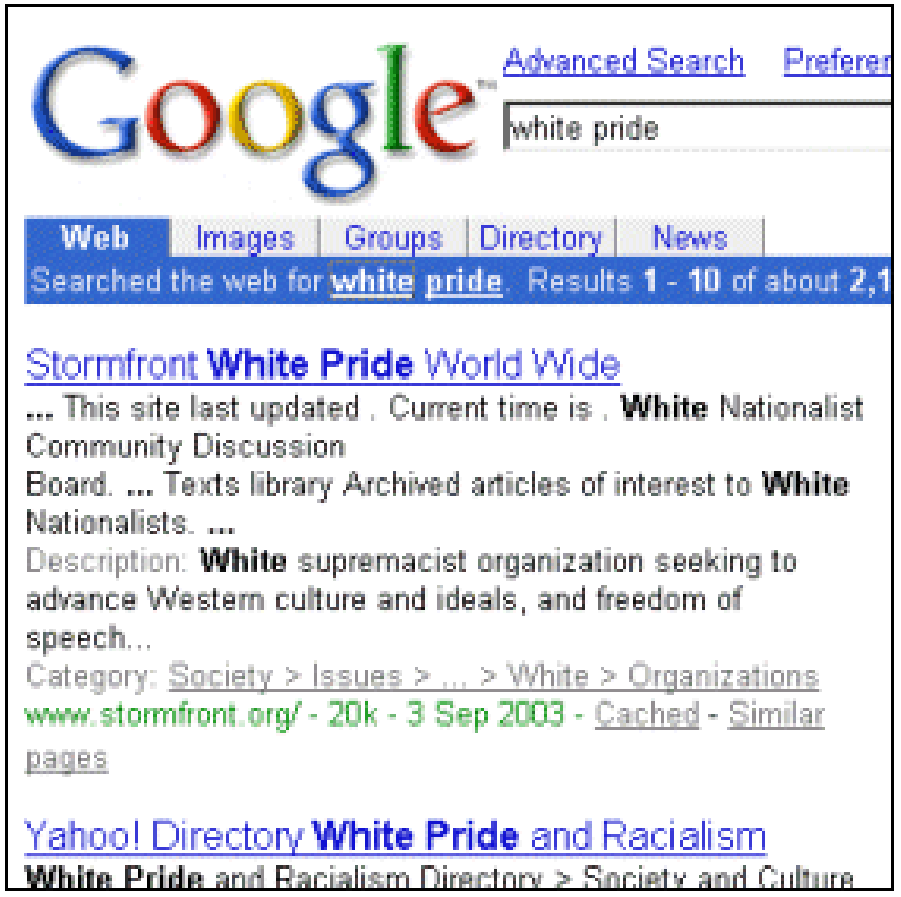
Jan 2011 – Egypt:
BGP routes
withdrawal



March 2011 – Libya
“warm standby mode”:
Unique State ISP
First chokes traffic
Then withdraws
BGP routes



US-Google



Censored Google Germany

http://blogoscoped.com/archive/2003_09_04_index.html

Zittrain, Jonathan; Edelman, Benjamin.
"Localized Google search result exclusions: Statement of issues and call for data." http://cyber.law.harvard.edu/filtering/google/results1.html
Harvard Law School: Berkman Center for Internet & Society. October 22, 2002.

2010
Wikileaks “Cablegate”

This webpage is not available

chromium

The server at **wikileaks.net** can't be found, because the DNS lookup failed. DNS is the web service that translates a website's name to its internet address. This error is most often caused by having no connection to the internet or a misconfigured network. It can also be caused by an unresponsive DNS server or a firewall preventing Chromium from accessing the network.

Here are some suggestions:

- Reload this web page later.
- Check your internet connection. Reboot any routers, modems, or other network devices you may be using.
- Check your DNS settings. Contact your network administrator if you're not sure what this means.
- Try disabling DNS prefetching by following these steps: Go to **Wrench menu > Preferences > Under the Hood** and deselect "Use DNS pre-fetching to improve page load performance."
- Try adding Chromium as a permitted program in your firewall or antivirus software's settings. If it is already a permitted program, try deleting it from the list of permitted programs and adding it again.
- If you use a proxy server, check your proxy settings or check with your network administrator to make sure the proxy server is working.

Wikileaks shutdown attempts – Dec, 2010

DynDNS and **Amazon** AWS end support to Wikileaks.org

PayPal restricts account used by WikiLeaks due to a "violation of the PayPal Acceptable Use Policy"

Mastercard and **Visa** withdraw ability to make donations to WikiLeaks

Apple removes an unofficial WikiLeaks app from the iTunes App Store

Postfinance, the Swiss postal system, shuts Assange's bank accounts

French minister Eric Besson warns Internet providers of "consequences" for those helping to keep WikiLeaks online

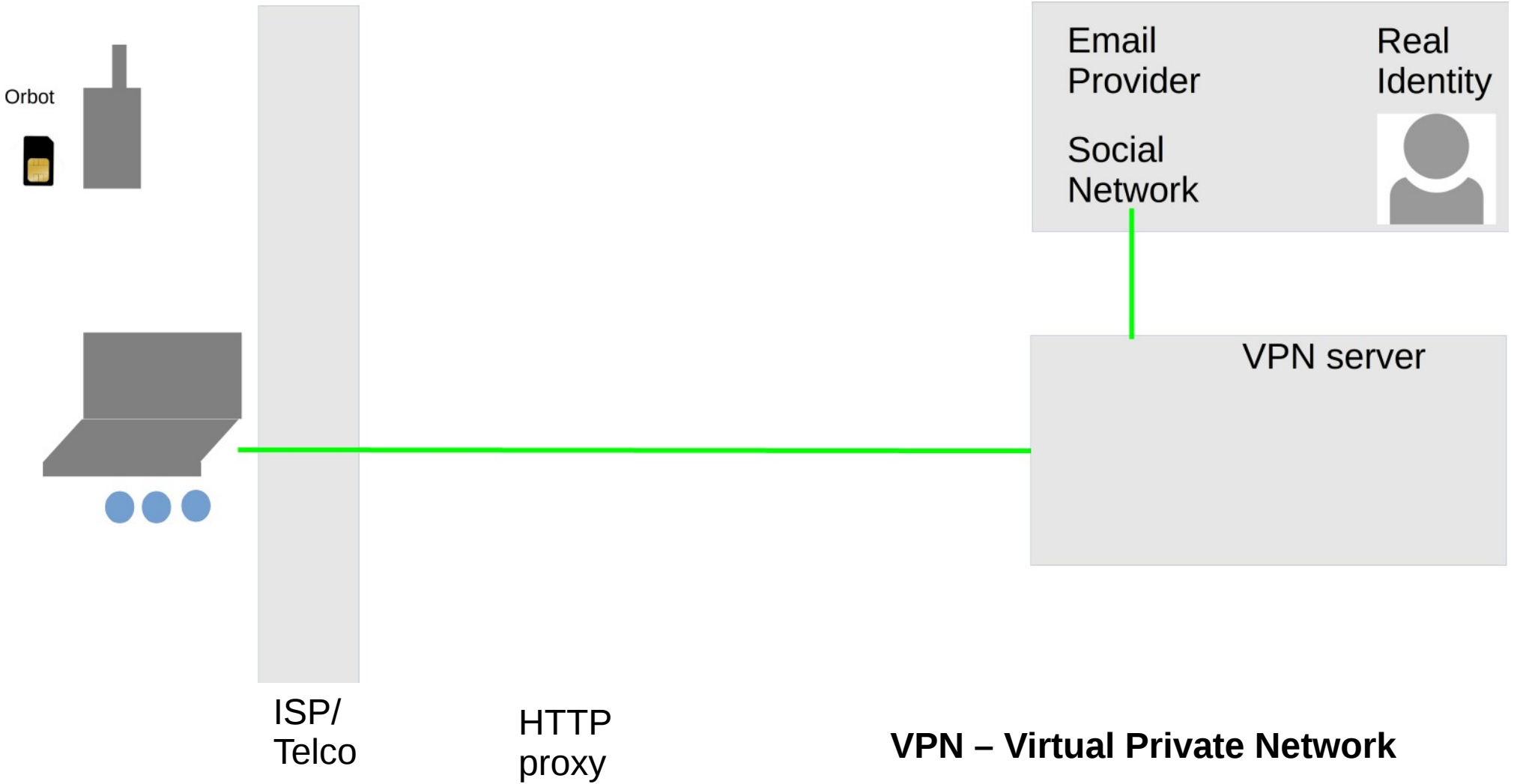
US access to Wikileaks banned in selected locations (eg **Library of congress**)

DDOS attacks ...

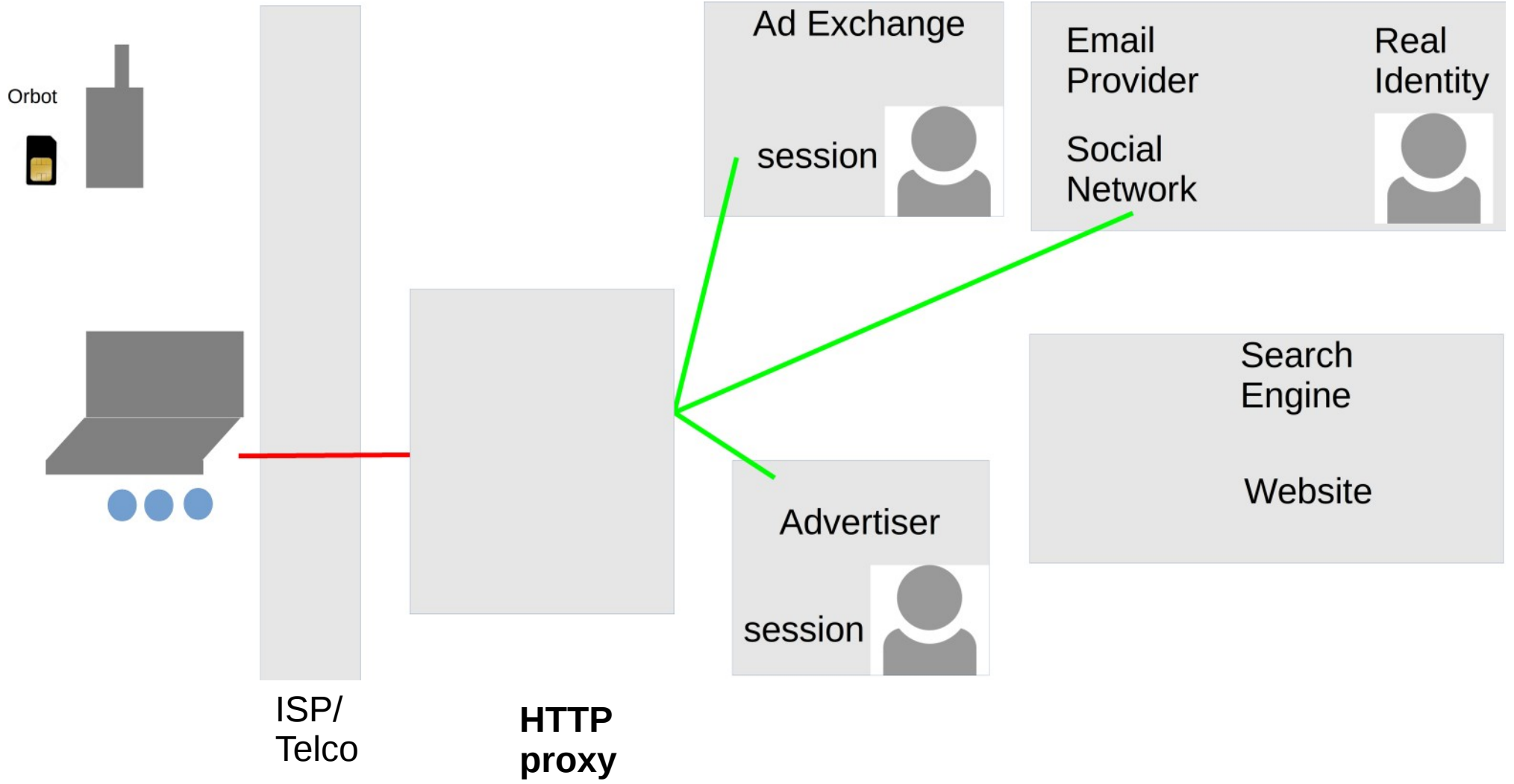
Da → A	**Territorio**	**Cyberspace**
Territorio	Reclusione, sequestro, minaccia, intimidazione, aggressione, distruzione di supporti	Rendere irraggiungibile l'IP *address* o i dati presso ISP
Cyberspace	Dirottamento DNS presso DNS server Sottrazione mezzi di finanziamento	Isolamento delle rotte presso ISP Denial of Service

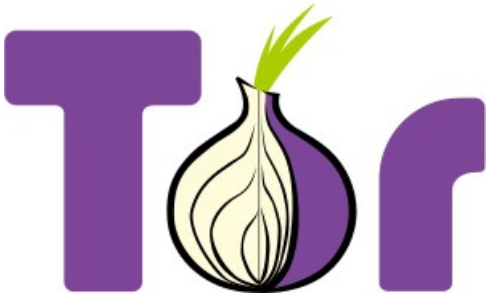
Misure anti censura basate sulla cifratura

1- VPN/Proxy
2- ToR
3 - PgP – gnuPG – Enigmail

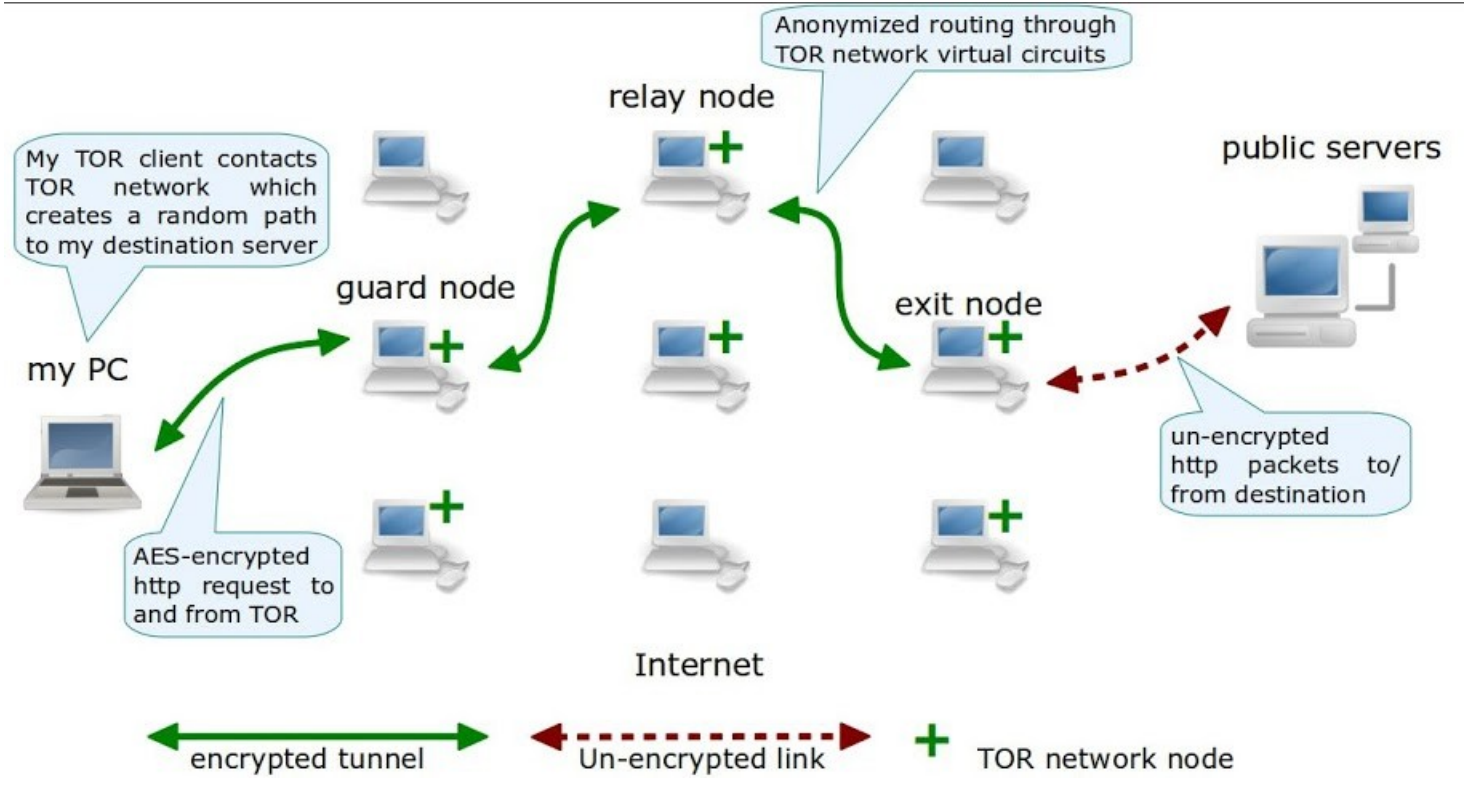


VPN – Virtual Private Network


Orbot
Ad Exchange
session
Email Provider
Real Identity
Social Network
Search Engine
Website
Advertiser
session
ISP/ Telco
HTTP proxy



TOR
The Onion Router
“il router a cipolla”


Anonymized routing through TOR network virtual circuits
relay node
public servers
My TOR client contacts TOR network which creates a random path to my destination server
guard node
exit node
my PC
un-encrypted http packets to/ from destination
AES-encrypted http request to and from TOR
Internet
encrypted tunnel
Un-encrypted link
TOR network node

Tor Overview
Users of Tor
Tor People
Jobs
Sponsors
Financial Reports
Projects
Documentation

Tor Tip

Tor is written for and supported by people like you. Donate today!

Tor: Sponsors

The Tor Project's diversity of users means we have a diversity of funding sources too — and we're eager to diversify even further!

Thank you to all the people and groups who have made Tor possible so far, and thank you especially to the individual volunteers who have made non-financial contributions: coding, testing, documenting, educating, researching, and running the relays that make up the Tor network.

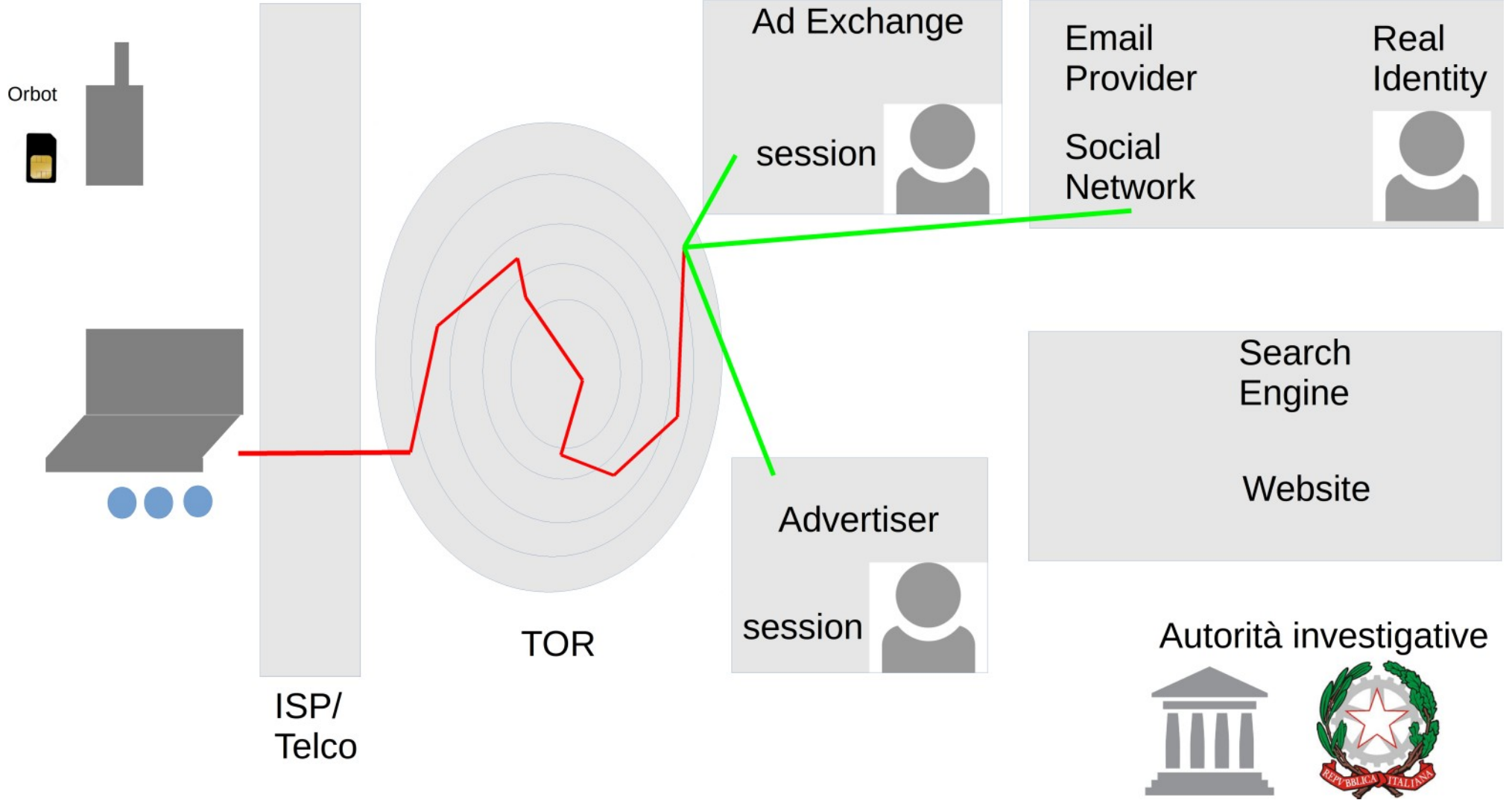
Active Sponsors in 2016:

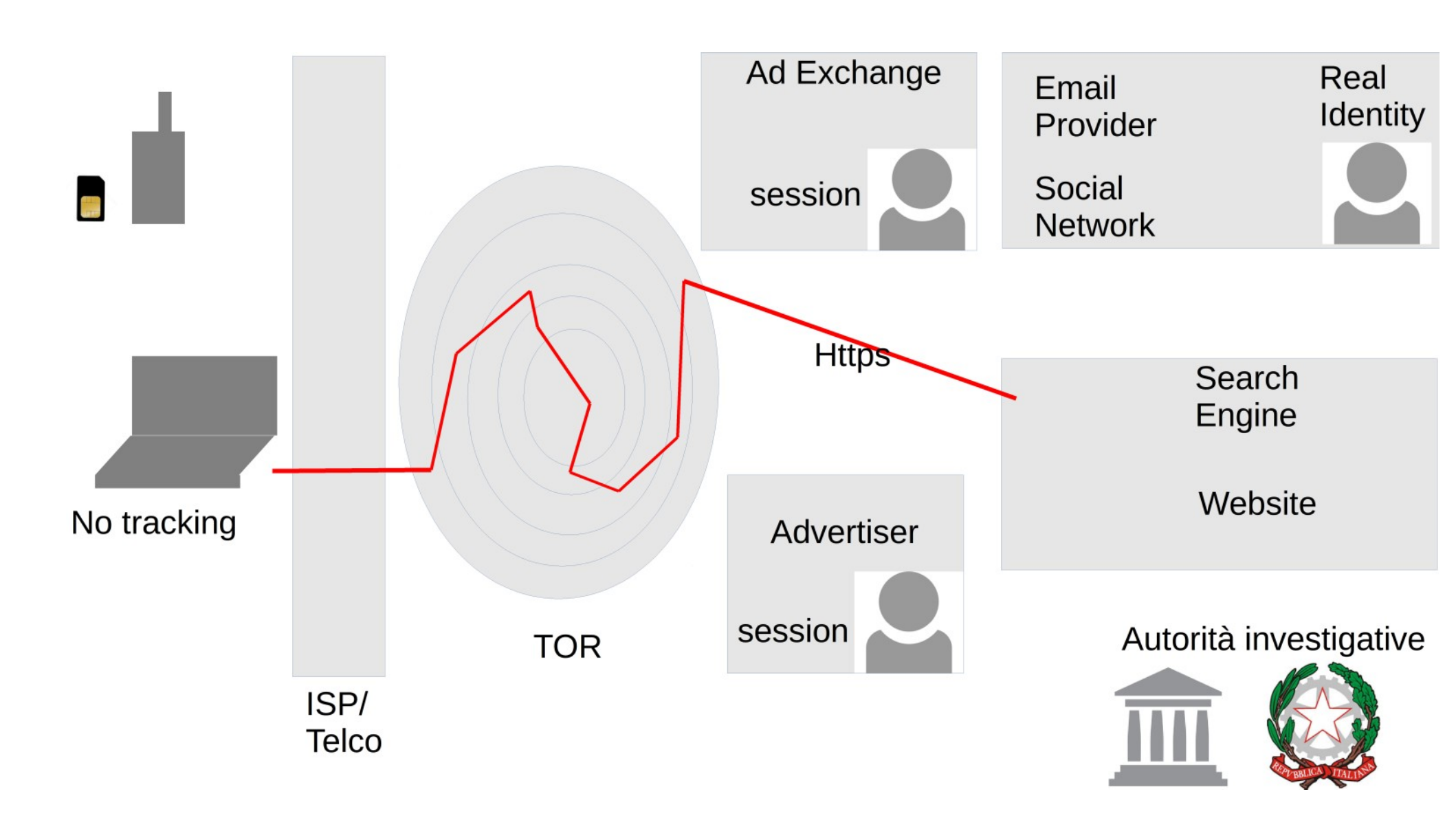
- Tens of thousands of personal donations from individuals like you (2006-present)
- Google Summer of Code (2007-2014 and 2016)
- Radio Free Asia (2012-2016)
- National Science Foundation joint with Georgia Tech and Princeton University (2012-2016)
- National Science Foundation via University of Minnesota (2013-2017)
- National Science Foundation joint with Georgetown (2015-2018)
- SRI International (2011-2016)
- US Department of State Bureau of Democracy, Human Rights, and Labor (2013-2016)
- An anonymous North American ISP (2009-present)

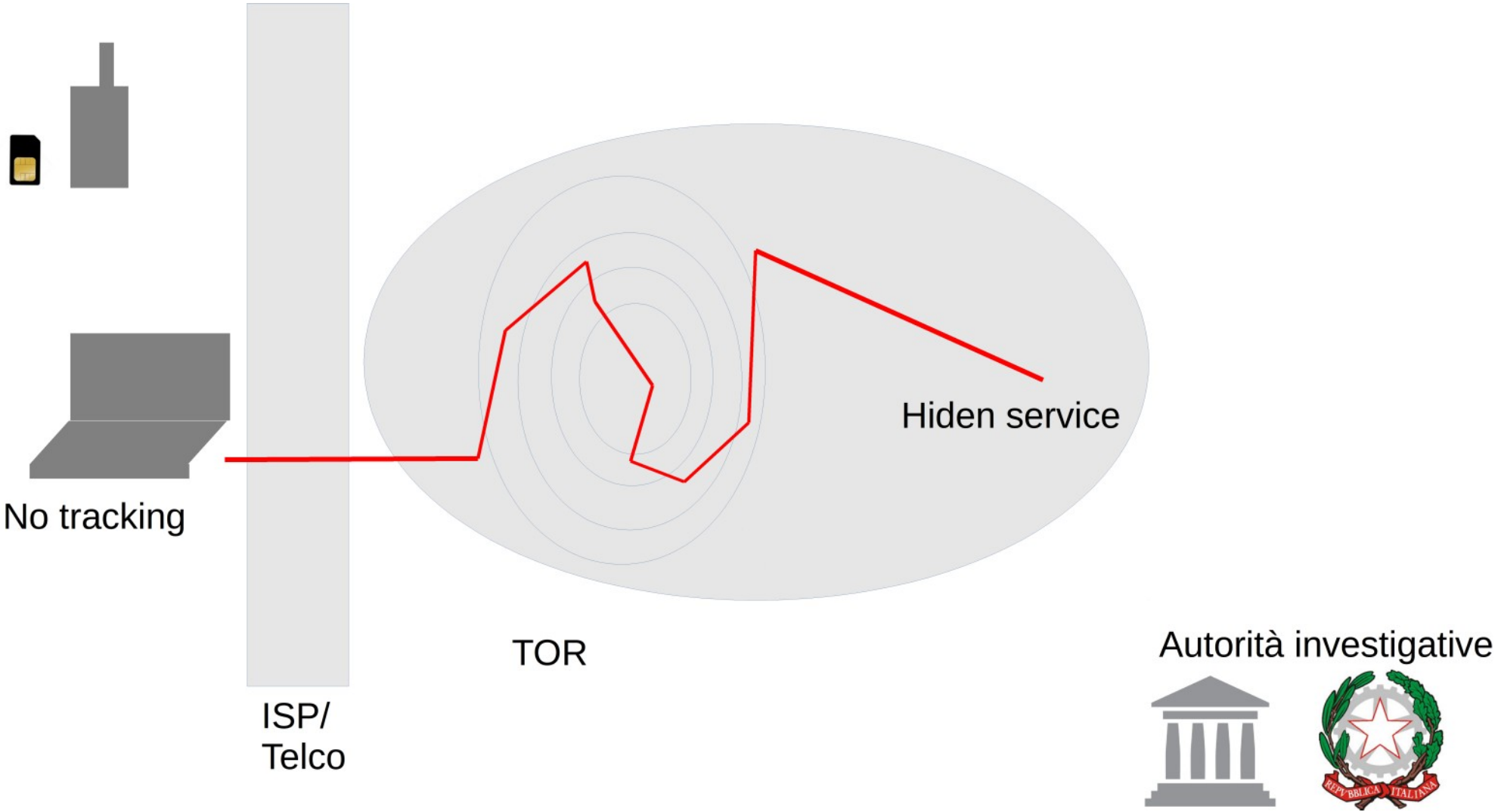
Past sponsors

We greatly appreciate the support provided by our past sponsors in keeping the Tor Project progressing through our ambitious goals:

- Federal Foreign Office of Germany (2015)


Orbot
ISP/
Telco
TOR
Ad Exchange
session
Email
Provider
Social
Network
Real
Identity
Search
Engine
Website
Advertiser
session
Autorità investigative

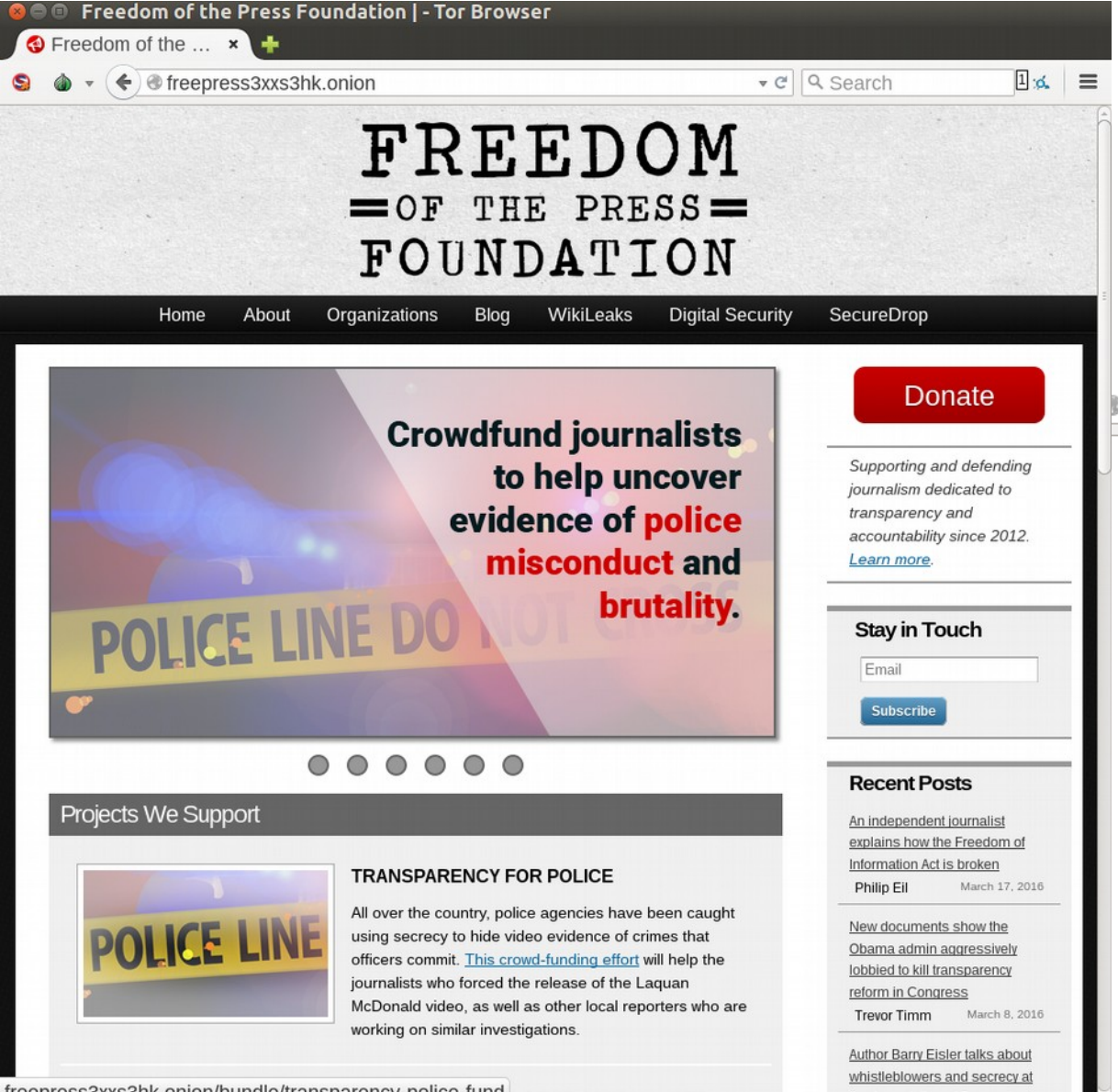

Ad Exchange
session
Email Provider
Social Network
Real Identity
Https
Search Engine
Website
No tracking
ISP/ Telco
TOR
Advertiser
session
Autorità investigative

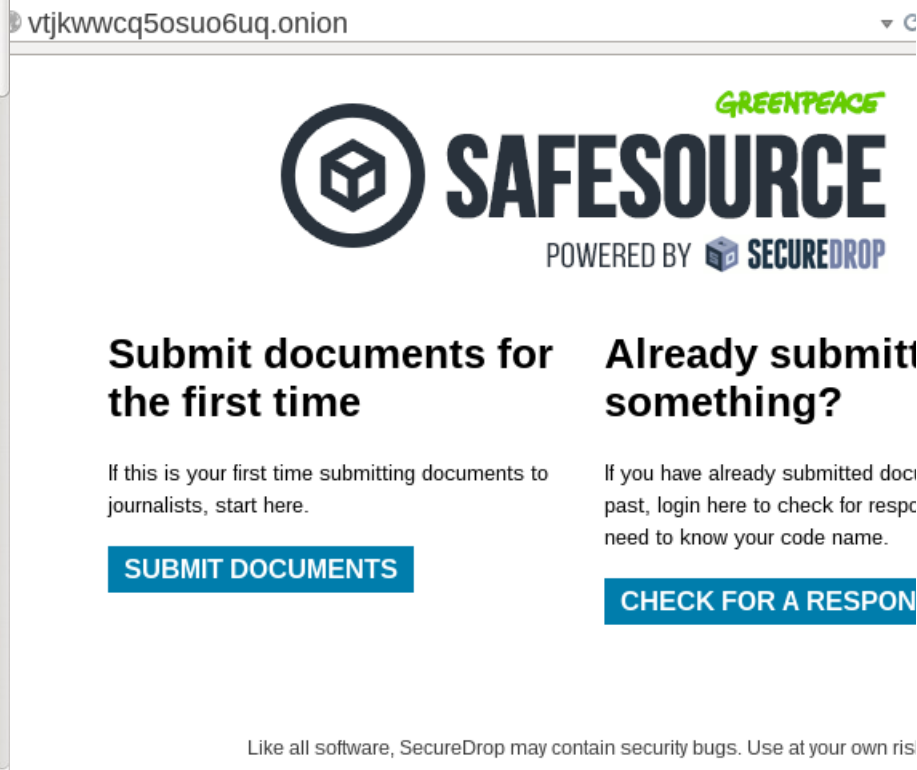

Hiden service
No tracking
TOR
ISP/
Telco
Autorità investigative

Deepweb/Darkweb

- **Deep Web**: porzione del Web che non può essere trovata da un motore di ricerca; siti non indicizzati
- **Dark Web**: piccola porzione del Deep Web intenzionalmente nascosta e inaccessibile con browser convenzionali
  - Es: servizi hidden di TOR

Esempio di servizio nascosto su TOR: SecureDrop per trasmettere alla stampa documenti.



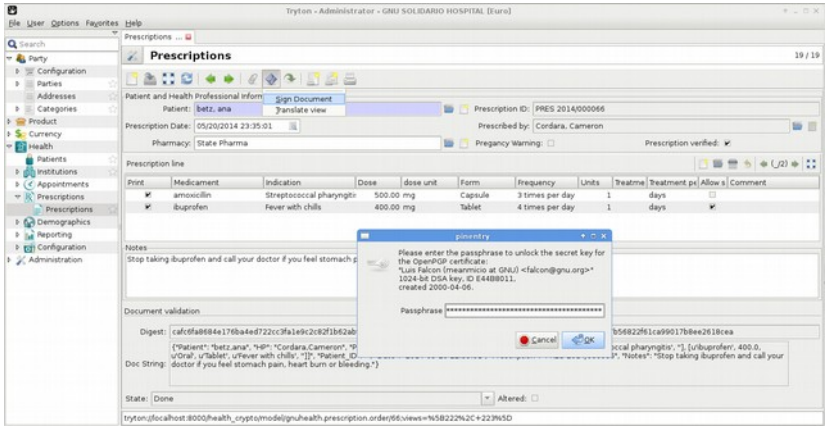


Email Cifrata

PGP (pretty good privacy)

GnuPG – versione GNU

EnigMail – plugin per Thunderbird



Richiede lo scambio delle *chiavi pubbliche*

Via keyserver o meglio via catene di chiavi firmate per mantenere la *chain of trust*