COMBATING CYBER CRIME

Police advisor, Associate Professor
Krunoslav Antoliš**,** PhD,
Senior Research Associate

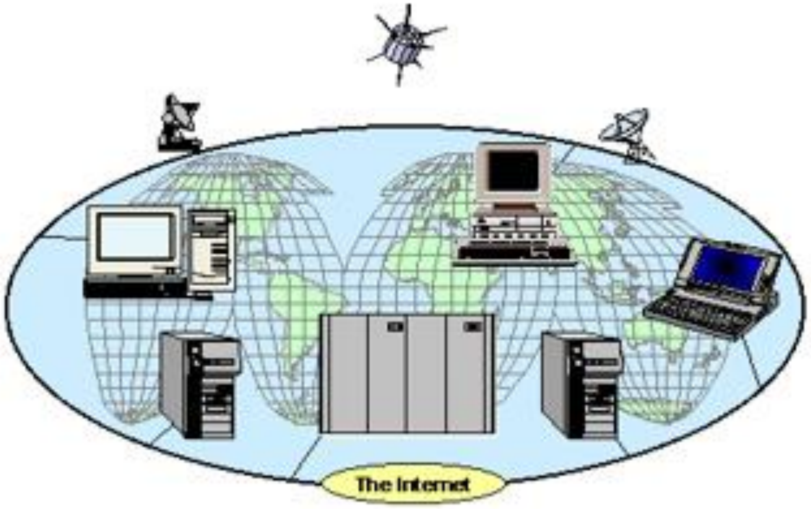
POLICE ACADEMY
Zagreb, Croatia

Contemporary World & Ongoing Global Processes

Evolving strategic environment and strategic drives of changes:

- ✓ globalization,
- ✓ political geometry,
- ✓ demographic & climate changes,
- ✓ environmental changes,
- ✓ new bio and nanotechnologies,
- ✓ ICT and the Internet http://www.internetlivestats.com/

The 21st Century Information Environment



Satellites

Cameras everywhere

Mobile Phones, PDAs

Disinformation, conspiracy theories, rumours, etc

ICT IS FAST, POROUS, GLOBAL, PERSONAL, OVERLOADED & UNSTOPPABLE

New Info-players

Cybersecurity

- **Up to 0.7 of world's GDP is lost to cyber crime**

- ***Cybersecurity Ventures predicts cybercrime damages will cost the world $6 trillion annually by 2021, up from $3 trillion in 2015***

  (Official Annual Cybercrime Report)

THE COMMUNICATORS
KIM ZETTER
Author, “Countdown
STUXNET'S BRAVE NEW WORLD
C-SPAN
COUNTDOWN TO ZERO DAY
KIM ZETTER
STUXNET AND THE LAUNCH OF THE WORLD'S FIRST DIGITAL WEAPON

- Intelligence agencies and militaries pay huge sums for the malicious code they need to carry out infiltrations and attacks.
- Stuxnet targets centrifuges used to produce enriched uranium
- Stuxnet is considered by analysts to be the first digital weapon

Cybersecurity

Ambassador Omar Arouna

„**Nobody is secure**
unless everybody is secure!”

US-Africa Cyber Security Group (USAFCG)

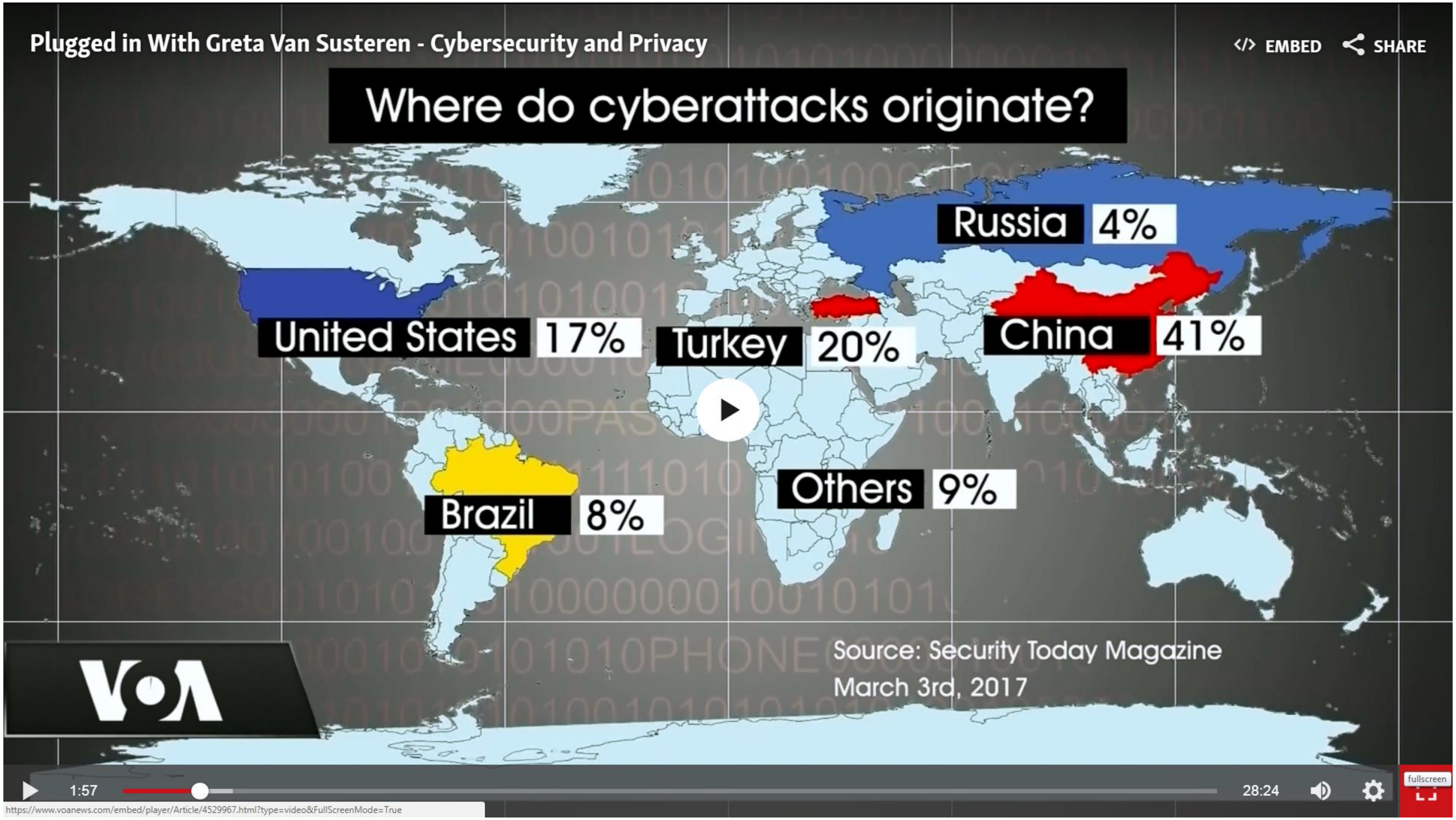
- Nigerian banking system stores $ 3.5 billion of the world's largest oil companies, especially those from the US

? cyber attack could destabilize world finance

- **Up to 0.7 of world's GDP is lost to cyber crime**

- ***Cybersecurity Ventures predicts cybercrime damages will cost the world $6 trillion annually by 2021, up from $3 trillion in 2015***

  (Official Annual Cybercrime Report)

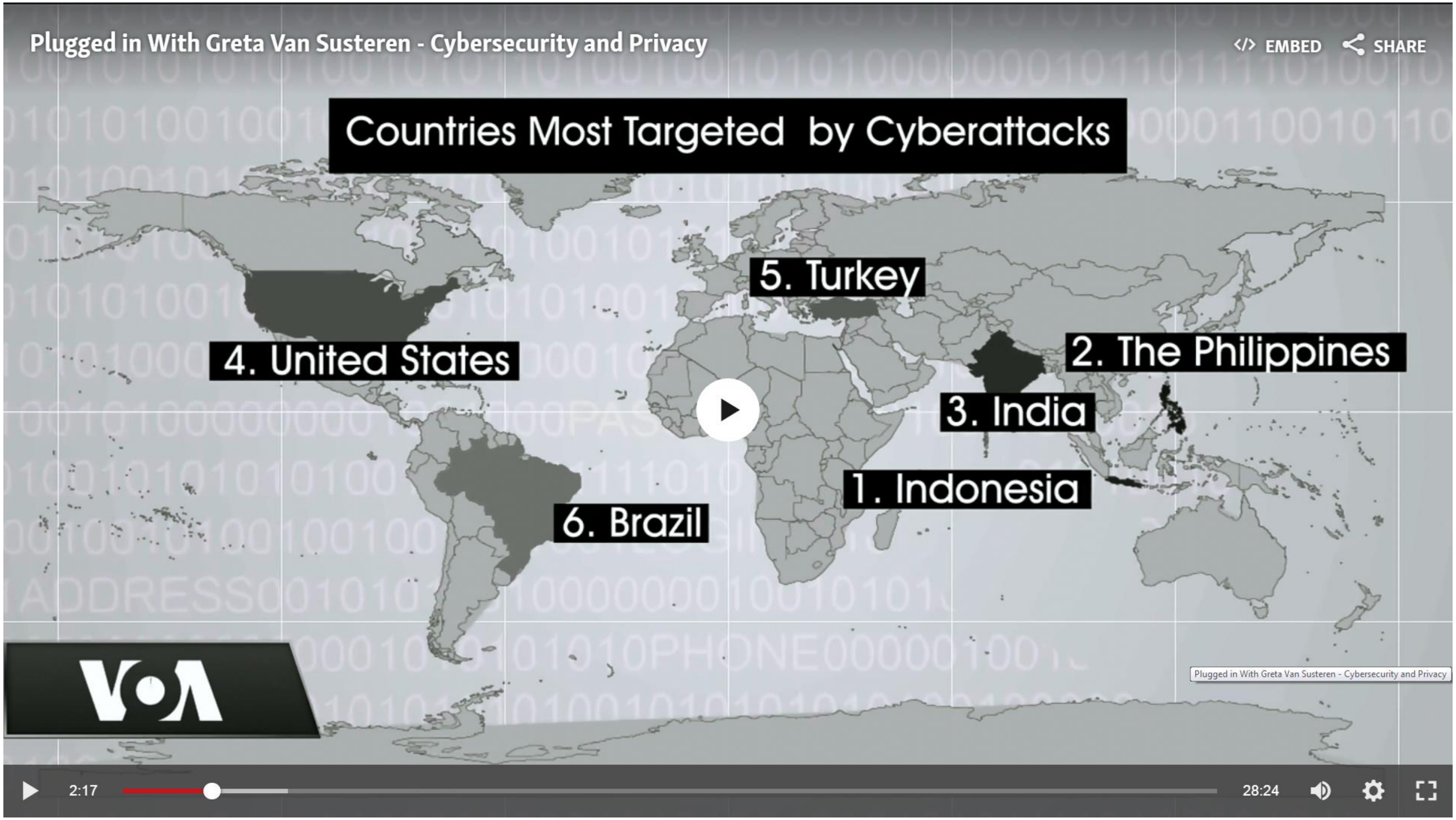


Plugged in With Greta Van Susteren - Cybersecurity and Privacy

Where do cyberattacks originate?

Source: Security Today Magazine
March 3rd, 2017

https://www.voanews.com/embed/player/Article/4529967.html?type=video&FullScreenMode=True



Plugged in With Greta Van Susteren - Cybersecurity and Privacy

Countries Most Targeted by Cyberattacks

1. Indonesia

2. The Philippines

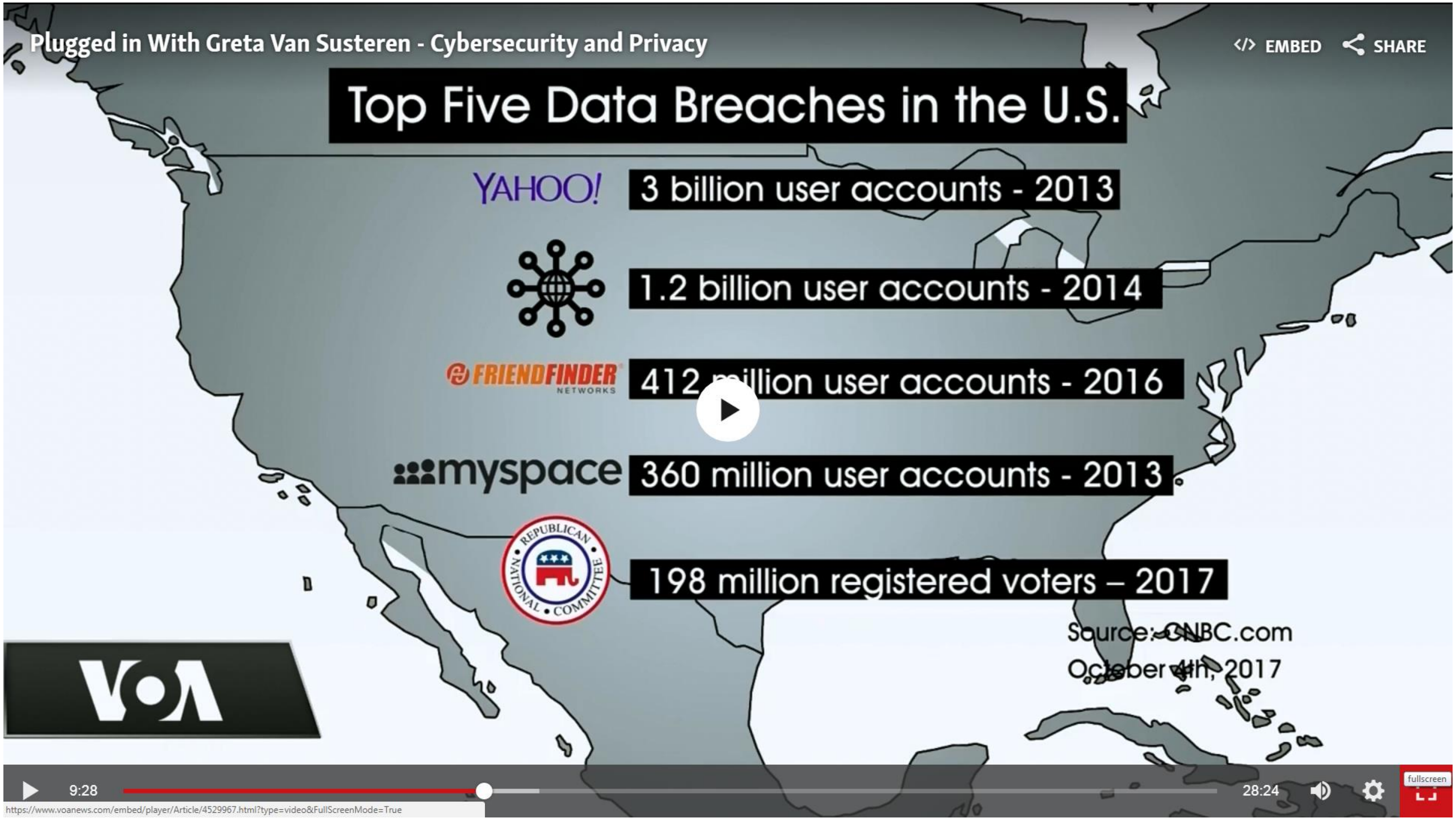
3. India

4. United States

5. Turkey

6. Brazil

EMBED
SHARE
VOA
Plugged in With Greta Van Susteren - Cybersecurity and Privacy
2:17
28:24



Plugged in With Greta Van Susteren - Cybersecurity and Privacy

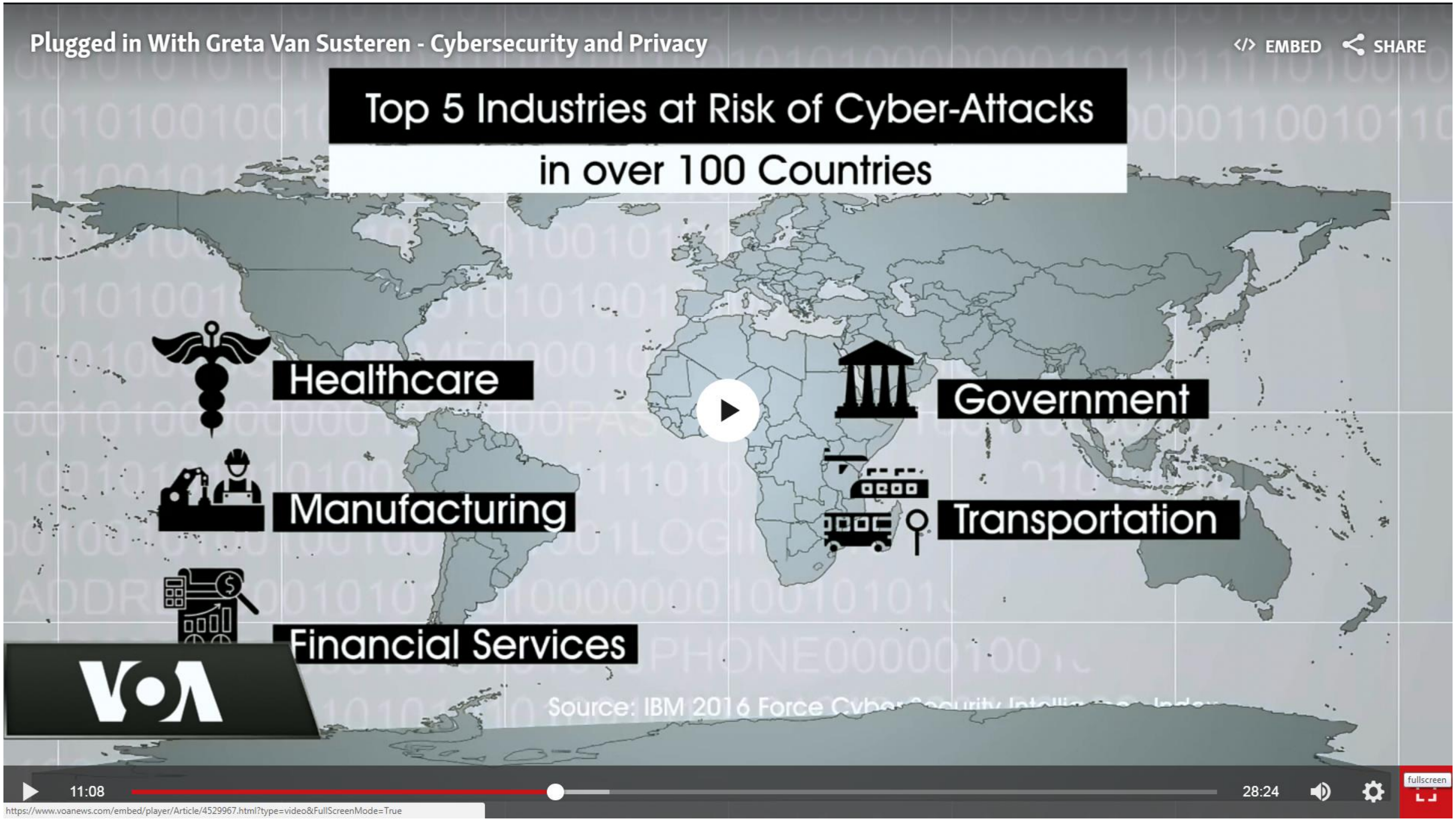
Top Five Data Breaches in the U.S.

YAHOO!	3 billion user accounts - 2013
	1.2 billion user accounts - 2014
FRIENDFINDER NETWORKS	412 million user accounts - 2016
myspace	360 million user accounts - 2013
REPUBLICAN NATIONAL COMMITTEE	198 million registered voters – 2017

Source: CNBC.com
October 4th, 2017

EMBED
SHARE
VOA
9:28
28:24
fullscreen
https://www.voanews.com/embed/player/Article/4529967.html?type=video&FullScreenMode=True

Marshall Center Security Forum - Ohrid 2018



Plugged in With Greta Van Susteren - Cybersecurity and Privacy

Top 5 Industries at Risk of Cyber-Attacks

in over 100 Countries

Healthcare

Manufacturing

Financial Services

Government

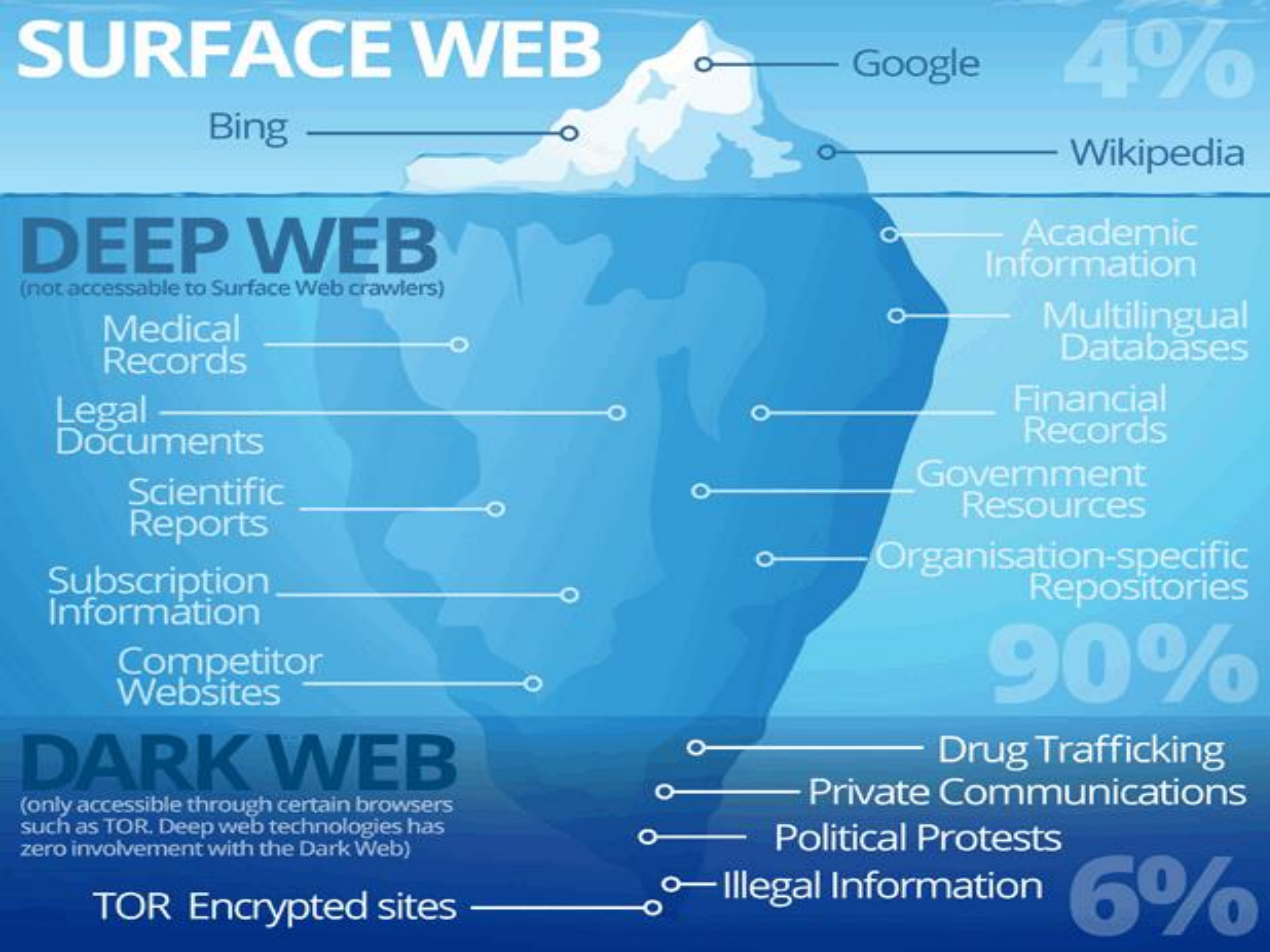
Transportation

Source: IBM 2016 Force Cyber Security Intelligence Index

https://www.voanews.com/embed/player/Article/4529967.html?type=video&FullScreenMode=True

An Overview of Important Risks – Powered by ICT Development

- Cyberwars,
- Cyberterorism and Cyber Riot,
- Security of Critical National Infrastructure,
- Intellectual Property in Cyber Space,
- Networks and Networked Information Thinking,
- Censorship in a cyber environment,
- Neutrality in cyber space,
- Privacy (GDPR) and
- Anonymity in the Cyber Space.



SURFACE WEB

Google

Bing

Wikipedia

4%

DEEP WEB

(not accessable to Surface Web crawlers)

Medical Records

Legal Documents

Scientific Reports

Subscription Information

Competitor Websites

Academic Information

Multilingual Databases

Financial Records

Government Resources

Organisation-specific Repositories

90%

DARK WEB

(only accessible through certain browsers such as TOR. Deep web technologies has zero involvement with the Dark Web)

TOR Encrypted sites

Drug Trafficking

Private Communications

Political Protests

Illegal Information

6%

Surface Internet

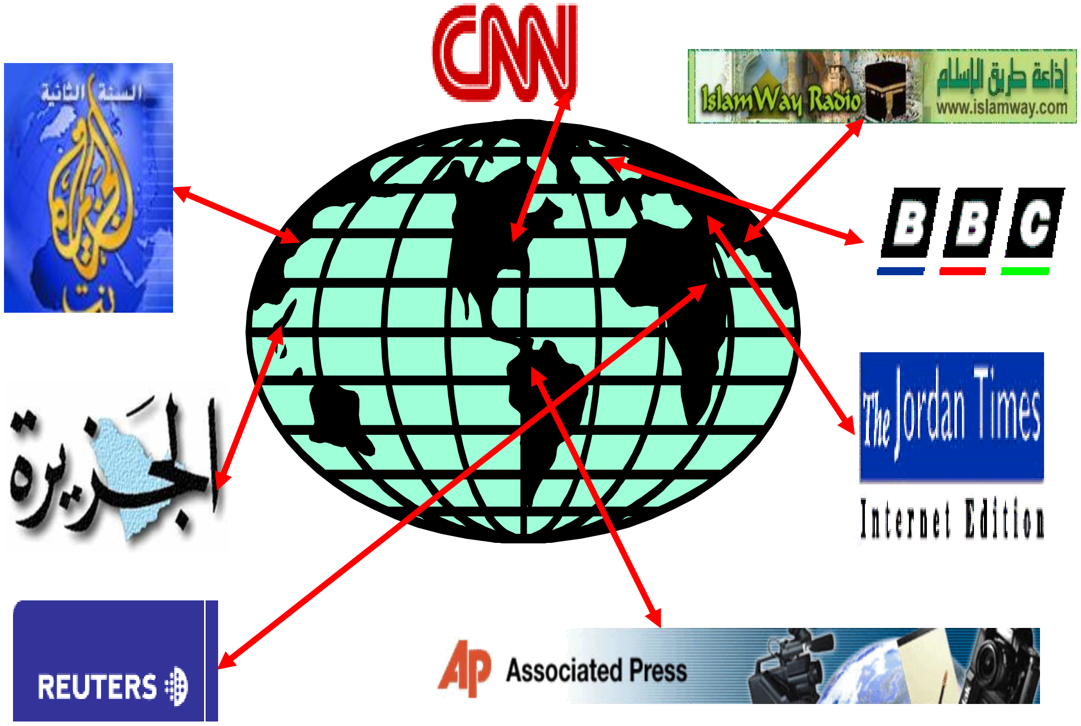
- ✓ decentralization of infrastructures,
- ✓ easy approach and anonymousness,
- ✓ global influence on the world public,
- ✓ fast communication and cheap maintenance and web application development
- ✓ multimedia possibilities
- ✓ superiority over traditional mass media which search for information on the Internet in the news making ,...

The Influence Media Interface

“Almost by definition . . . a war waged on live television is a war in which political and public relations considerations become inextricably bound up with military tactics and strategy. . . .

… how victory is won is almost as important as victory itself.”

(Washington Post, March 24, 2003)



Abuse of the surface internet

ISLAMIST WEBSITE

JIHADI WEBSITE

Terrorist BLOG

Terrorist FORUM

Jihadists use mobiles as propaganda tools

A Jihadist’s Course in the Art of Recruitment

Abu `Amr’s handbook

Feds Consider Searches of Terrorism blogs

By Thomas Frank**, USA TODAY**

WASHINGTON — The Homeland Security Department may **soon** start scouring the Internet to find blogs and message boards that terrorists use to plan attacks in the USA.

The effort comes as researchers are seeing terrorists increasingly use the Internet to plan bombings, recruit members and spread propaganda. "Blogging and message boards have played a substantial role in allowing communication among those who would do the United States harm," the department said in a recent notice.

Homeland Security officials are looking for companies to search the Internet for postings "in near to real-time which precede" an attack, particularly a bombing. Bombings are "of great concern" because terrorists can easily get materials and make an improvised-explosive device (IED), the department said.

"There is a lot of IED information generated by terrorists everywhere — websites, forums, people telling you where to buy fertilizer and how to plant IEDs," said Hsinchun Chen, director of the University of Arizona's Artificial Intelligence Lab. Chen's "Dark Web" research project has found:

500,000,000 terrorist pages and postings,

including tens of thousands that discuss IEDs.

http://www.usatoday.com/news/washington/2008-12-23-terrorblogs_N.htm

FBI chief: Terrorist & VE Group Turning to Encrypted Communications

FBI Director James B. Comey said that the **Islamic State has attracted at least 21,000 English-speaking followers** on the **Twitter** social media platform, bombarding them with incitements to violence.

When Islamic State operatives encounter a potential recruit, Comey said,
"we see them giving directions" to move to a mobile messaging app that is encrypted, he said. "And they disappear."

Terrorists & VE Abuse WhatsApp

London terror suspect Khalid Masood sent a WhatsApp message to an unknown person just before Sunday's attack that killed four people and injured dozens. The message’s contents — and its intended recipient — can't be accessed by police because the popular, Facebook-owned messaging service encoded them. Criminals and terrorists can now "go dark" by using strong encryption.

FBI Director James Comey said "That is a shadow falling across our work" . The darkness is spreading through the whole room, he also said last week at a security conference at the University of Texas at Austin.

Ms Amber Rudd - Secretay of State for the Home Department, UK

"I don't need to understand how encryption works to understand how it's helping – end-to-end encryption – the criminals. I will engage with the security services to find the best way to combat that".

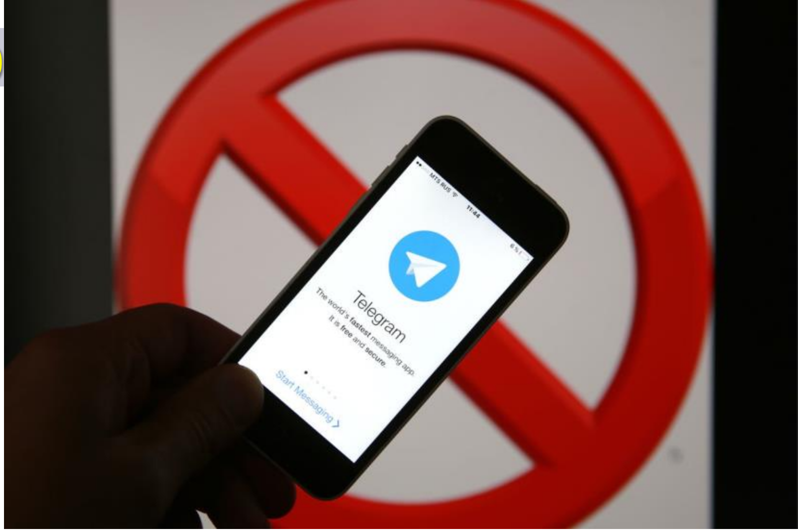
Use/Abuse End-to-end Encryption

End-to-end encryption is used in a variety of the most secure messaging apps, including those made Apple, WhatsApp, Signal and Telegram.

The UK government has said that **it is concerned that the technology keeps them from reading terrorists' and criminals' messages.**

Experts warn that the same technology also keeps private citizens from having their messages read by criminals, and is used to secure banking technologies, among other functions …

VE &Terrorists’ Love for Telegram



Terrorism and intelligence experts have known for years that **the encrypted messaging application Telegram is now the “app of choice” for terrorists,** and specifically for ISIS.

- ✓ **The ISIS members behind the 2015 Paris attacks used Telegram to spread propaganda.**
- ✓ **ISIS also used the app to recruit the perpetrators of the Christmas market attack in Berlin last year and claim credit for the massacre.**
- ✓ **More recently, a Turkish prosecutor found that the shooter behind the New Year’s Eve attack at the Reina nightclub in Istanbul used Telegram to receive directions for it from an ISIS leader in Raqqa.**

Russia Follows Iran in Blocking Telegram Messaging App

Russia's telecoms watchdog on Friday asked a Moscow court to block the popular messaging app Telegram, after a deadline for it to hand over encryption keys to security services expired.
Roskomnadzor said in a statement it had filed a lawsuit **"demanding the limiting of access on Russian territory" to encrypted app Telegram.**
Telegram's self-exiled **Russian founder Pavel Durov** has long said **he will reject any attempt by the country's security services to gain backdoor access to the app.**

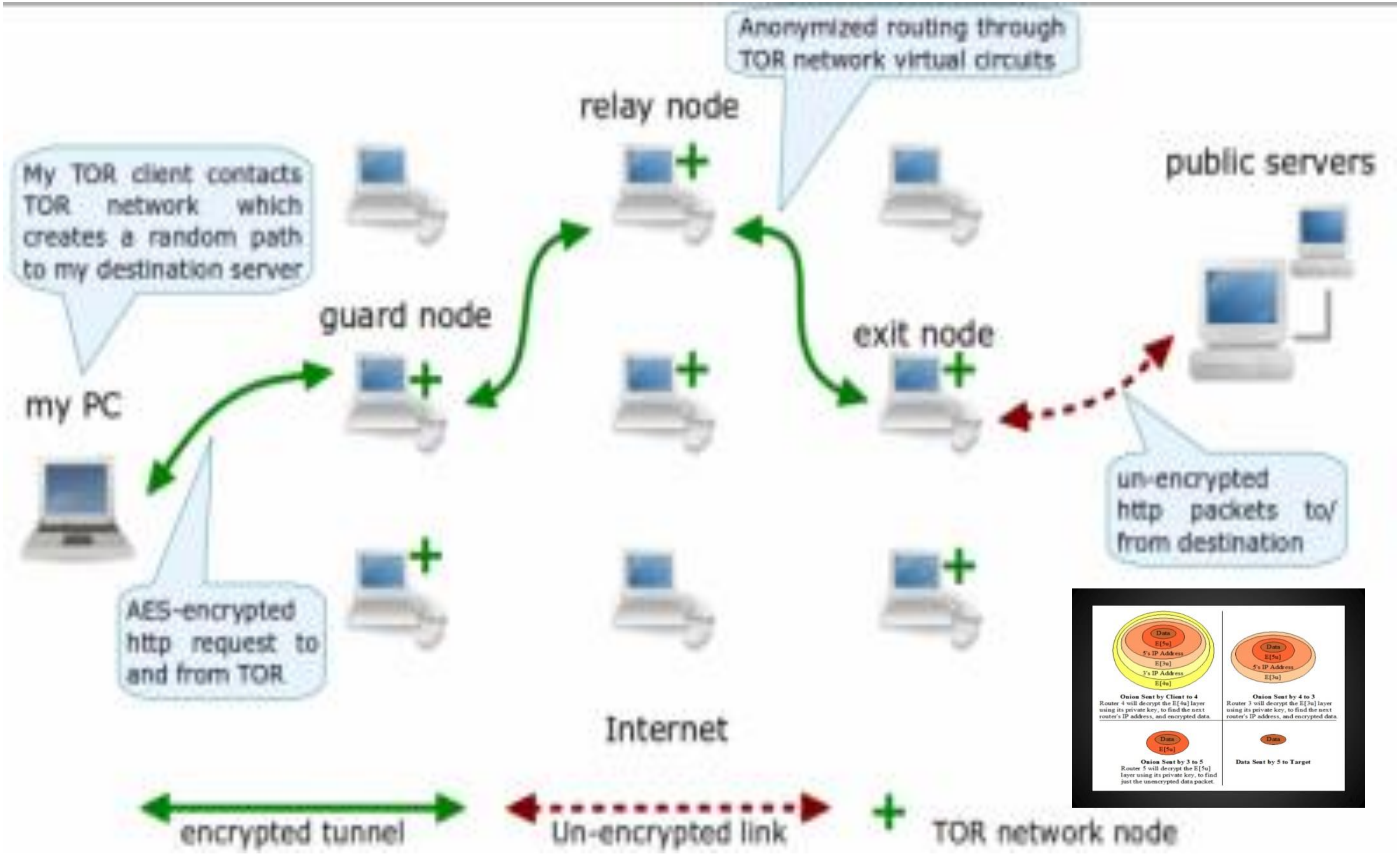
VE & Terrorists Use the Dark Web to Hide

The Dark Web is the hidden portion of the Internet that's **only available through specialized browsers TOR**.

"It's a place where all sorts of illicit activities can happen. It's the sort of place where you would go if you **wanted to buy weapons**," said Herb Lin, a senior research scholar for cyber policy at the Hoover Institution at Stanford University.

"One of the things they do is **they train each other on how to run all the traffic on their Android mobile phones through the dark web** so **all their Internet and voice traffic is sent through encrypted channels and so unreadable by law enforcement,**" said Aaron Brantly, a professor of cyber studies at the U.S. Military Academy.

TOR - The Onion Router



Anonymized routing through TOR network virtual circuits

My TOR client contacts TOR network which creates a random path to my destination server

AES-encrypted http request to and from TOR

un-encrypted http packets to/ from destination

Onion Sent by Client to 4
Router 4 will decrypt the E[4u] layer using its private key, to find the next router's IP address, and encrypted data.

Onion Sent by 4 to 3
Router 3 will decrypt the E[3u] layer using its private key, to find the next router's IP address, and encrypted data.

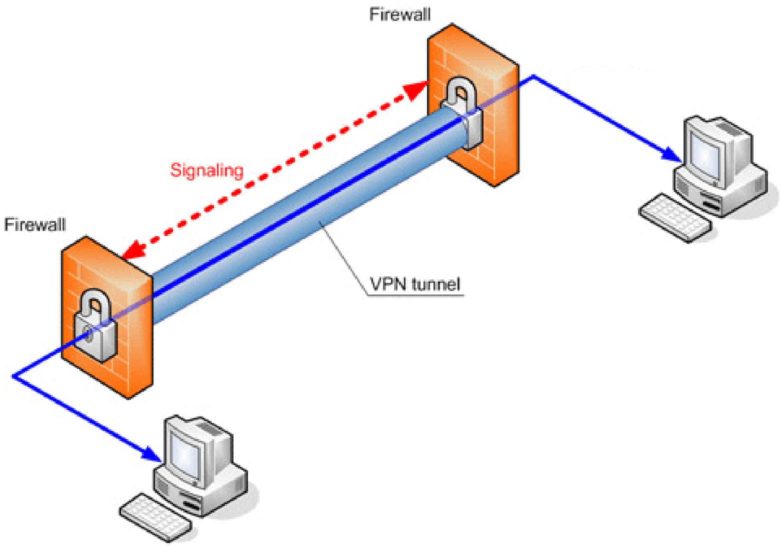
Onion Sent by 3 to 5
Router 5 will decrypt the E[5u] layer using its private key, to find just the unencrypted data packet.

Data Sent by 5 to Target

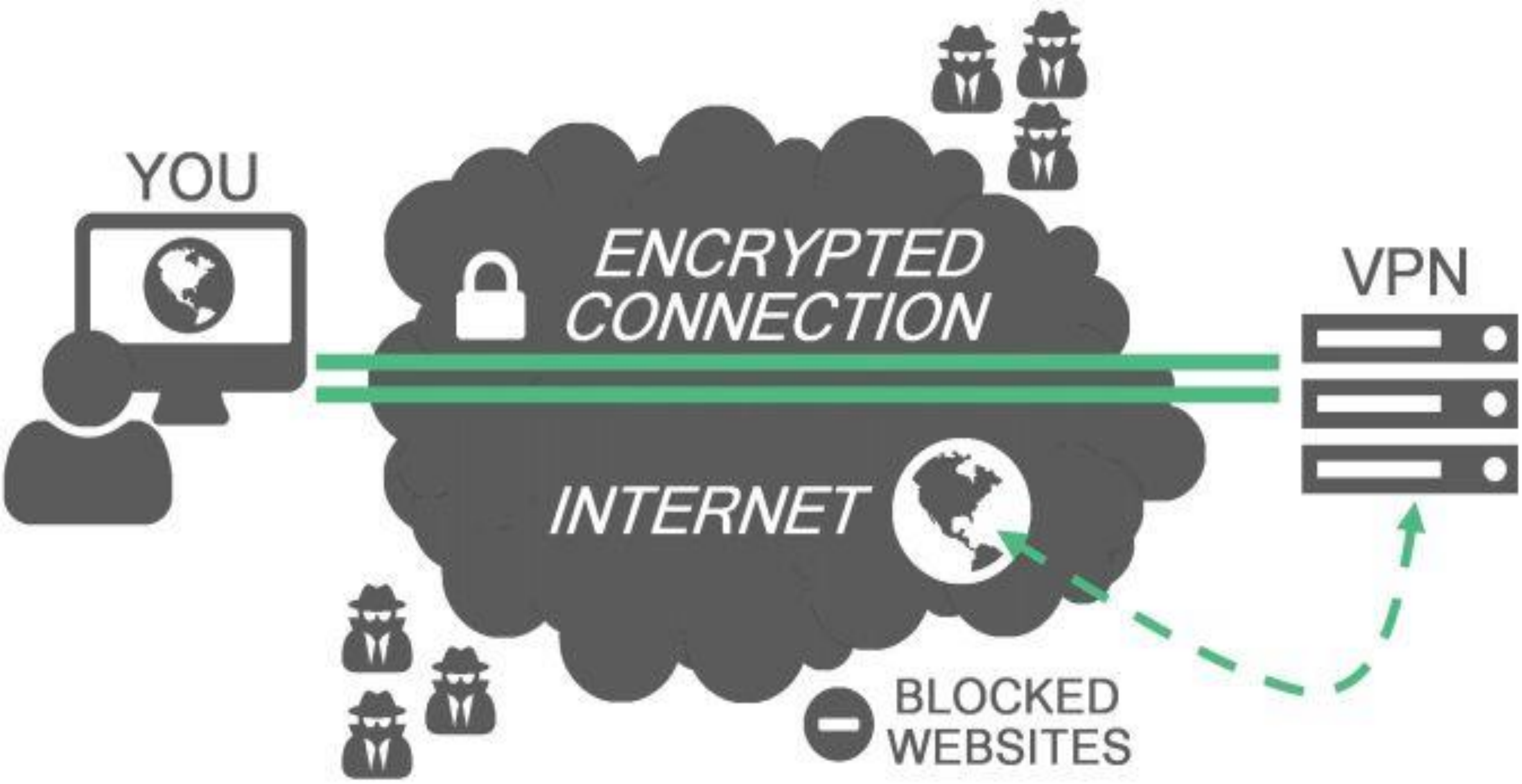
VPN

- Provide users with the ability to send and receive data over public or shared networks as if their computers are locally connected

- Allows - security
  - functionality
  - manageability
  - anonymity



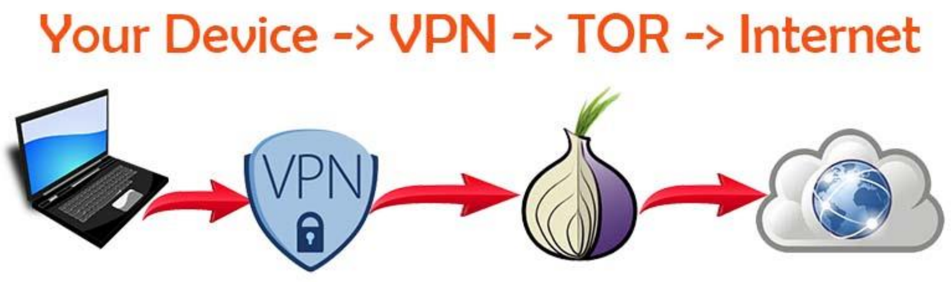
Access Restricted by IP Address



How to Hide an IP Address

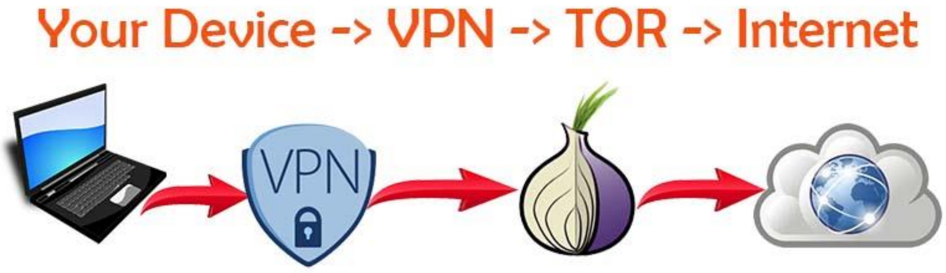
- IPVanish VPN
- NordVPN, PureVPN
- Private Internet Access VPN
- Keep Solid VPN Unlimited
- TunnelBear VPN
- Golden Frog VyprVPN
- TorGuard VPN
- AnchorFree Hotspot Shield Elite
- Hide My Ass VPN

Tor Through VPN



- In this configuration you connect **first to your VPN server, and then to the Tor network before accessing the internet**:
- Your computer -> VPN -> Tor -> Internet
  - your apparent IP on the internet is that of the Tor exit node.

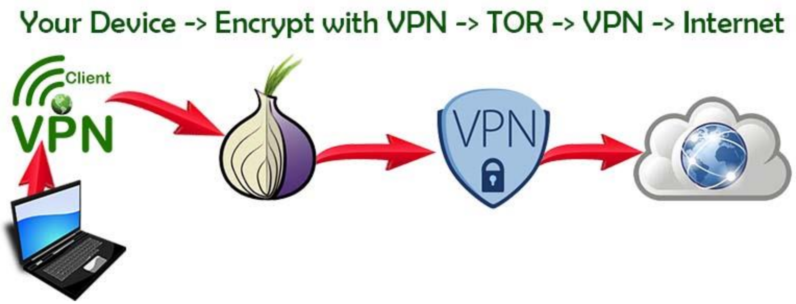
Tor Through VPN



- **Pros:**
- **Your ISP will not know that you are using Tor (although it can know that you are using a VPN)**
- The Tor entry node will not see your true IP address, but the IP address of the VPN server.
- If you use a good no-logs provider this can provide a meaningful additional layer of security
- Allows access to Tor hidden services

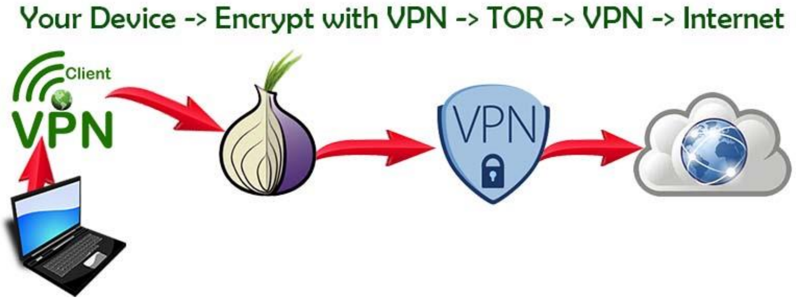
- **Cons:**
- **Your VPN provider knows your real IP address**
- No protection from malicious Tor exit nodes. Non-HTTPS traffic entering and leaving Tor exit nodes is unencrypted and could be monitored
- Tor exit nodes are often blocked
- We should note that using a Tor bridge can also be effective at hiding Tor use from your ISP (although a determined ISP could in theory use deep packet inspection to detect Tor traffic).

VPN Through Tor



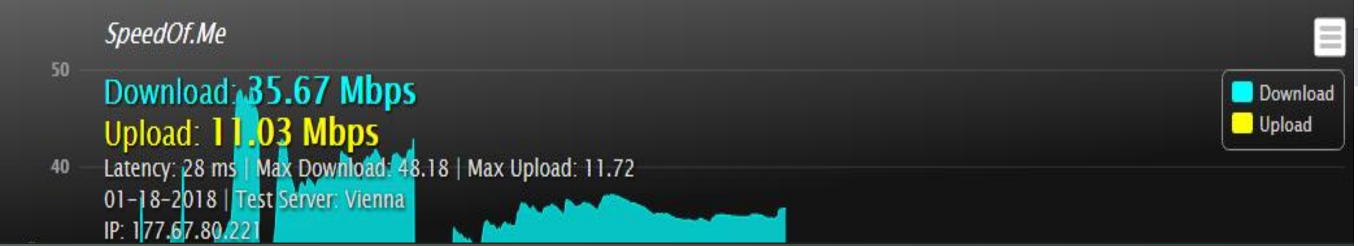
- This involves connecting **first to Tor,** and **then through a VPN server to the internet:**
- Your computer -> Encrypt with VPN ->Tor -> VPN -> internet
- This setup requires you to configure your VPN client to work with Tor, and the only VPN providers we know of to support this are AirVPN and BolehVPN. Your apparent IP on the internet is that of the VPN server.

VPN Through Tor



- **Pros**
- Because you connect to the VPN server through Tor, the VPN provider cannot ‘see’ your real IP address – only that of the Tor exit node. When combined with an anonymous payment method (such as properly mixed Bitcoins) made anonymously over Tor, this means the VPN provider has no way of identifying you, even if it did keep logs
- Protection from malicious Tor exit nodes, as data is encrypted by the VPN client before entering (and exiting) the Tor network (although the data is encrypted, your ISP will be able to see that it is heading towards a Tor node)
- Bypasses any blocks on Tor exit nodes
- Allows you to choose server location (great for geo-spoofing)
- All internet traffic is routed through Tor (even by programs that do not usually support it).

- **Cons**
- Your VPN provider *can* see your internet traffic (but has no way to connect it to you)
- Slightly more vulnerable to global end-to-end timing attack as a fixed point in the chain exists (the VPN provider).



SpeedOf.Me

Download: 35.67 Mbps

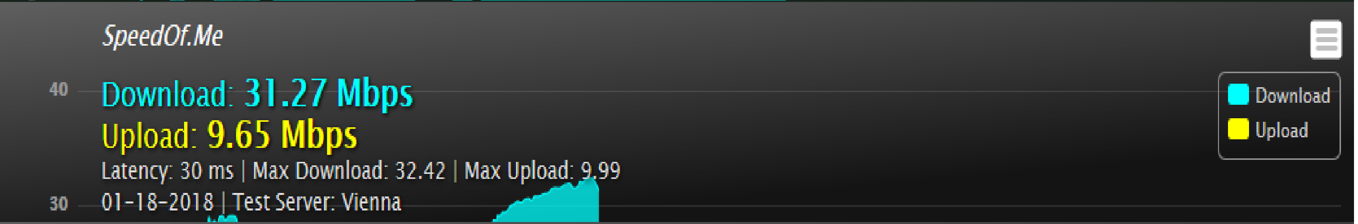
Upload: 11.03 Mbps

Latency: 28 ms | Max Download: 48.18 | Max Upload: 11.72

01-18-2018 | Test Server: Vienna

IP: 177.67.80.221

Speed
Unprotected Networks



SpeedOf.Me

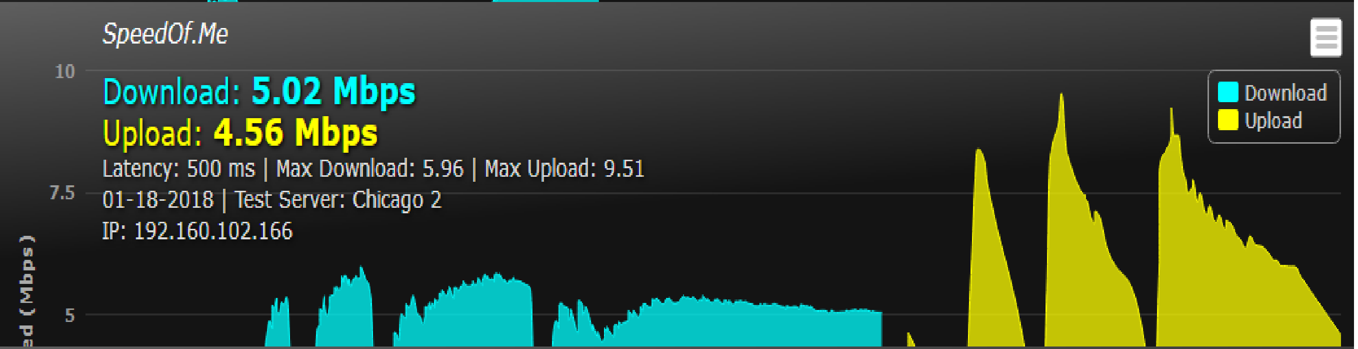
Download: 31.27 Mbps

Upload: 9.65 Mbps

Latency: 30 ms | Max Download: 32.42 | Max Upload: 9.99

01-18-2018 | Test Server: Vienna

Speed VPN



SpeedOf.Me

Download: 5.02 Mbps

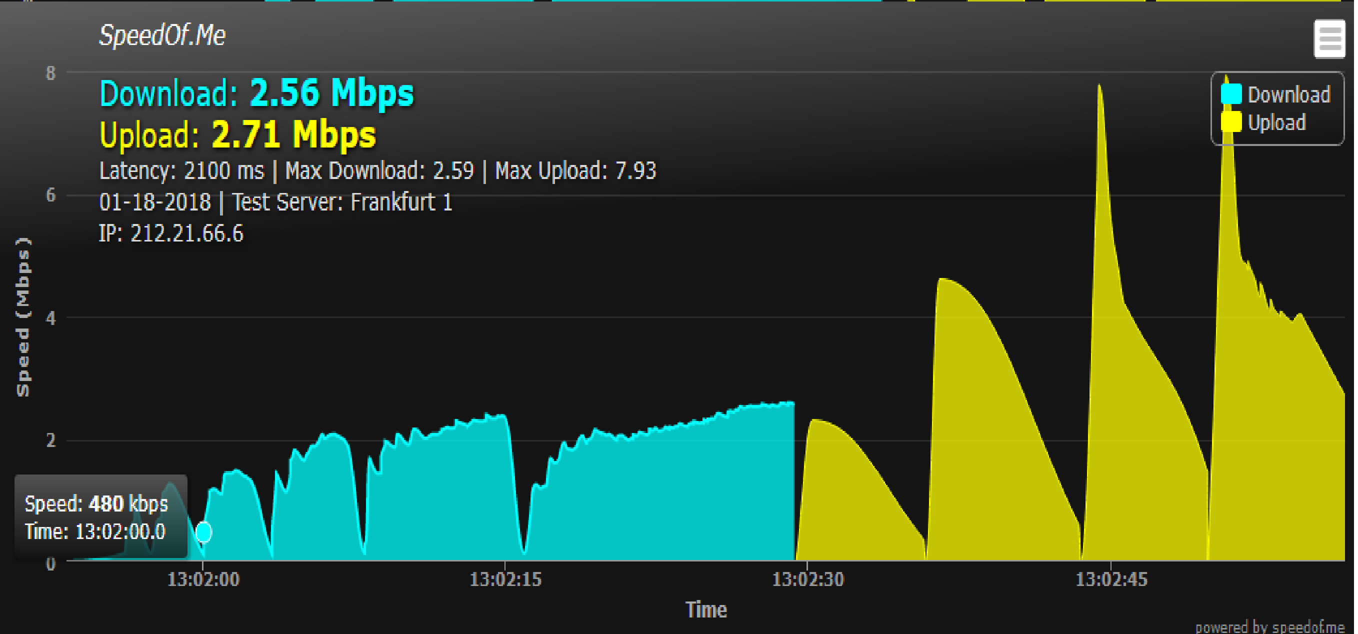
Upload: 4.56 Mbps

Latency: 500 ms | Max Download: 5.96 | Max Upload: 9.51

01-18-2018 | Test Server: Chicago 2

IP: 192.160.102.166

Speed TOR



SpeedOf.Me

Download: 2.56 Mbps

Upload: 2.71 Mbps

Latency: 2100 ms | Max Download: 2.59 | Max Upload: 7.93

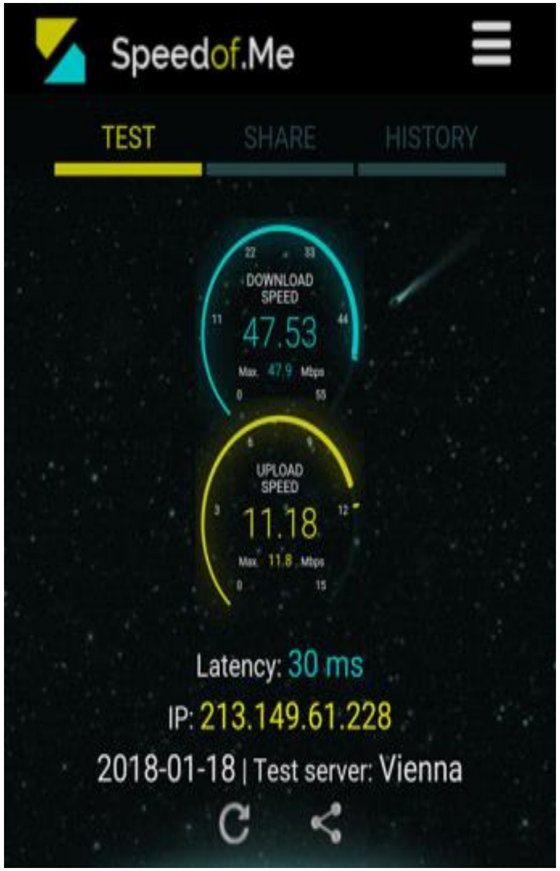
01-18-2018 | Test Server: Frankfurt 1

IP: 212.21.66.6

Speed
VPN & TOR

Mobile Device & Data Rate Measurement

Unprotected Network



DOWNLOAD SPEED 47.53 Max. 47.9 Mbps

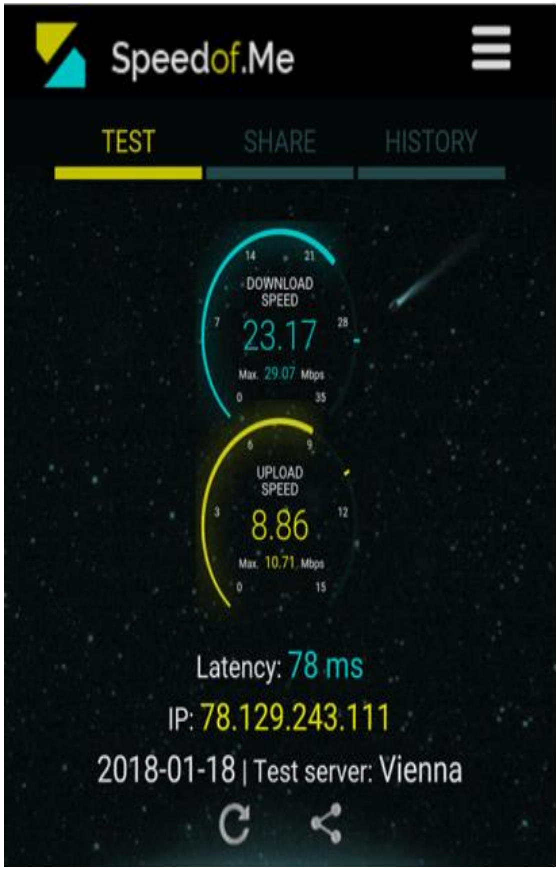
UPLOAD SPEED 11.18 Max. 11.8 Mbps

Latency: 30 ms

IP: 213.149.61.228

2018-01-18 | Test server: Vienna

VPN



DOWNLOAD SPEED 23.17 Max. 29.07 Mbps

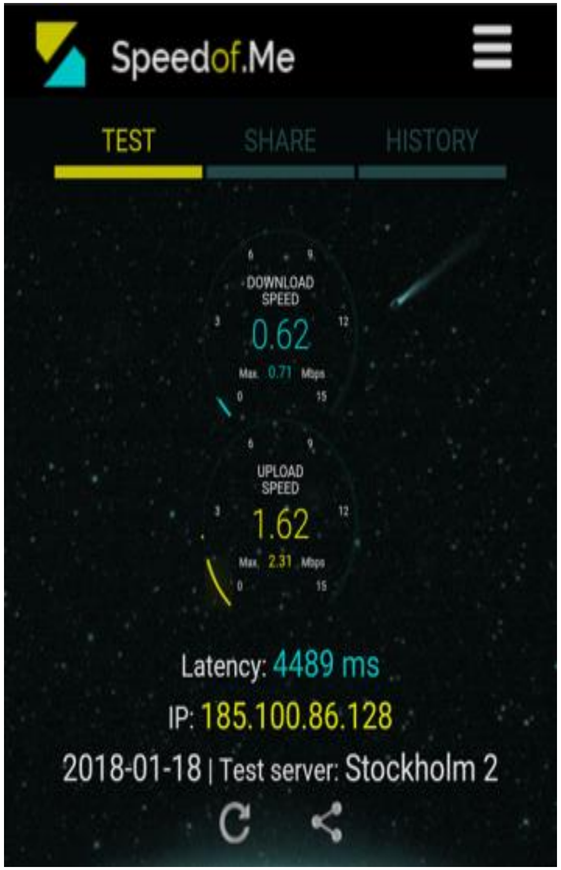
UPLOAD SPEED 8.86 Max. 10.71 Mbps

Latency: 78 ms

IP: 78.129.243.111

2018-01-18 | Test server: Vienna

TOR



DOWNLOAD SPEED 0.62 Max. 0.71 Mbps

UPLOAD SPEED 1.62 Max. 2.31 Mbps

Latency: 4489 ms

IP: 185.100.86.128

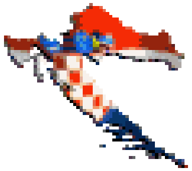
2018-01-18 | Test server: Stockholm 2

Apple Bans
Cryptocurrency Mining Apps
From Its App Stores

June 11, 2018

Due to the surge in cryptocurrency prices, **not only hackers but also legitimate websites and mobile apps are increasingly using cryptocurrency miners to monetize by levying the CPU power of your PC and phones to mine cryptocurrencies.**

EUROPOL & INTERPOL



Questions ???

Comments !!

Remarks .

Associate Professor Krunoslav Antoliš, Ph.D.
kantolis@fkz.hr