

IP Address and Cross-border Cooperation for Resolving the Cyber Attribution Challenge

Eun Chang Choi
eunchang.choi@aya.yale.edu

Table of Contents

Cyber Attack Maps: Global Scale

What Makes an IP Address untraceable?

IP Addresss Spoofing, VNC (Virtual Network Computing)

Why Cyber Attacks Are So Difficult to Trace

The Difference of IP Address, Real Location,
Borderline, and National Jurisdictions

Why are IP Addresses at Odds with Jurisdiction?

Threatbutt Internet Hacking Attack Attribution Map



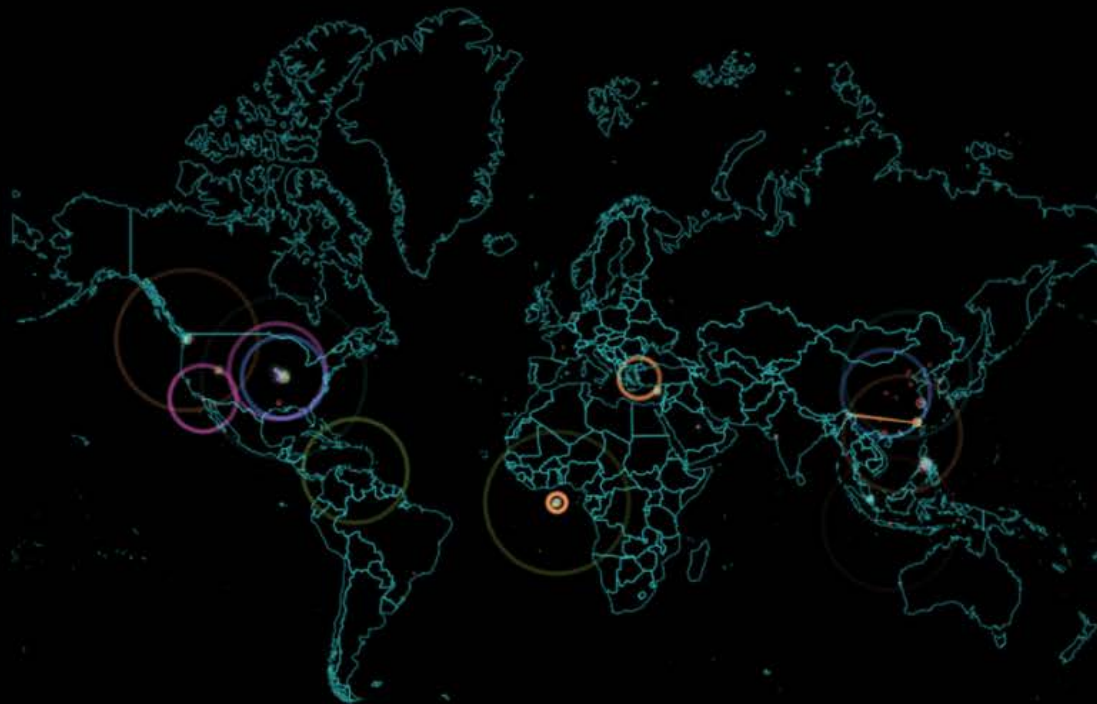
13) -- UPGRADE TO PREMIUM FOR MORE INFO\$

.140.21.79) -- IT'S CYBER POMPEII 🚩!

140.21.79 (2.02)

140.21.79 (2.02)





ATTACK ORIGINS

COUNTRY	#	PORT	SERVICE TYPE
China	15	1433	ms-sql-s
United States	5	5900	vnc
South Korea	4	3306	mysql
Netherlands	4	902	iss-realsecure
India	3	5800	vnc-http
Indonesia	3	23	telnet
Canada	2	26577	unknown

ATTACK TYPES

ATTACK TARGETS

#	COUNTRY
33	United States
15	Philippines
8	MilGov
5	Singapore
5	Cyprus
1	Saudi Arabia

LIVE ATTACKS

TIMESTAMP	ATTACKER	ATTACKER IP	ATTACKER GEO	TARGET GEO	ATTACK TYPE	PORT
17:18:39.761	Qualys provides Internet Security	62.210.136.206	Security, US	Saint Louis, US	telnet	23
17:18:40.043	BTC Broadband Service	77.85.1.152	BG	Riverton, US	unknown	19191
17:18:40.382	Universitas Negeri Semarang	103.23.102.5	Semarang, ID	CY	ssh	22
17:18:40.712	CHINANET hebei province network	111.225.74.11	Gaobeidian, CN	Saint Louis, US	unknown	2694
17:18:41.048	Cloud-Sense Technology Corporation Ltd.	119.9.90.66	HK	Seattle, US	telnet	23
17:18:41.381	CANTV Servicios, Venezuela	201.210.252.14	Caracas, VE	milgov	microsoft-ds	445
17:18:41.715	CHINANET SHAANXI PROVINCE NETWORK	1.85.61.21	Xian, CN	Saint Louis, US	unknown	17862

ATTACKS TODAY

[since 12AM PST]

2,376,611

ATTACKS YESTERDAY

10,834,822

TOP TARGETS BY COUNTRY

LEARN ABOUT CHECK POINT
THREAT PREVENTION SOLUTIONS >



TIME	ATTACK	SOURCE	TARGET
16:23:18	REP.TC.aad	Germany	Germany
16:23:18	Andromeda.TC.ijfgeqhbh	TX,USA	Nigeria
16:23:18	Andromeda.TC.eabbaaabb	TX,USA	Nigeria
16:23:18	REP.ivcoqk	TX,USA	Nigeria
16:23:18	Operator.Virus.Win32.Sality.s.bq	TX,USA	Taiwan
16:23:18	Operator.Virus.Win32.Sality.s.bq	TX,USA	Taiwan

 Source
 Target

FIREEYE CYBER THREAT MAP



Powered by FireEye

TOP 5 REPORTED INDUSTRIES [PAST 30 DAYS]

FINANCIAL SERVICES

SERVICES/CONSULTING

TELECOM

MANUFACTURING

INSURANCE

[VIEW FULL SCREEN](#)

Real Time Web Monitor

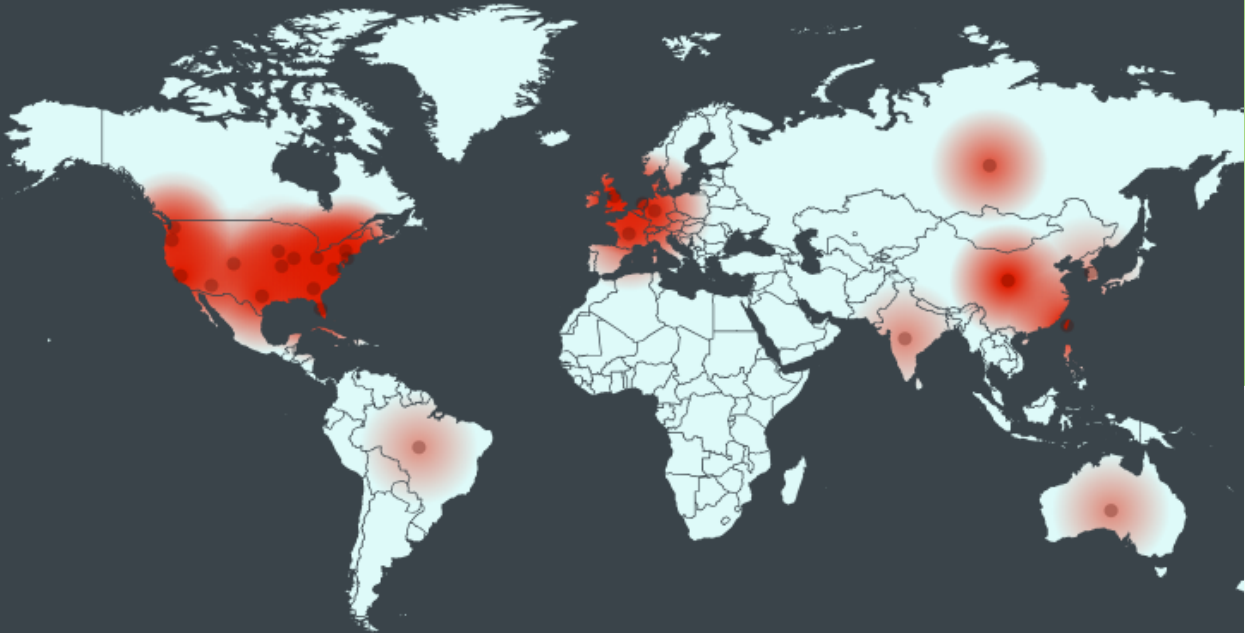
Traffic

Attacks

November 16, 2018 12:55:00 PM



North America	+
South America	+
Europe	+
Asia	+
Africa	+
Australia	+

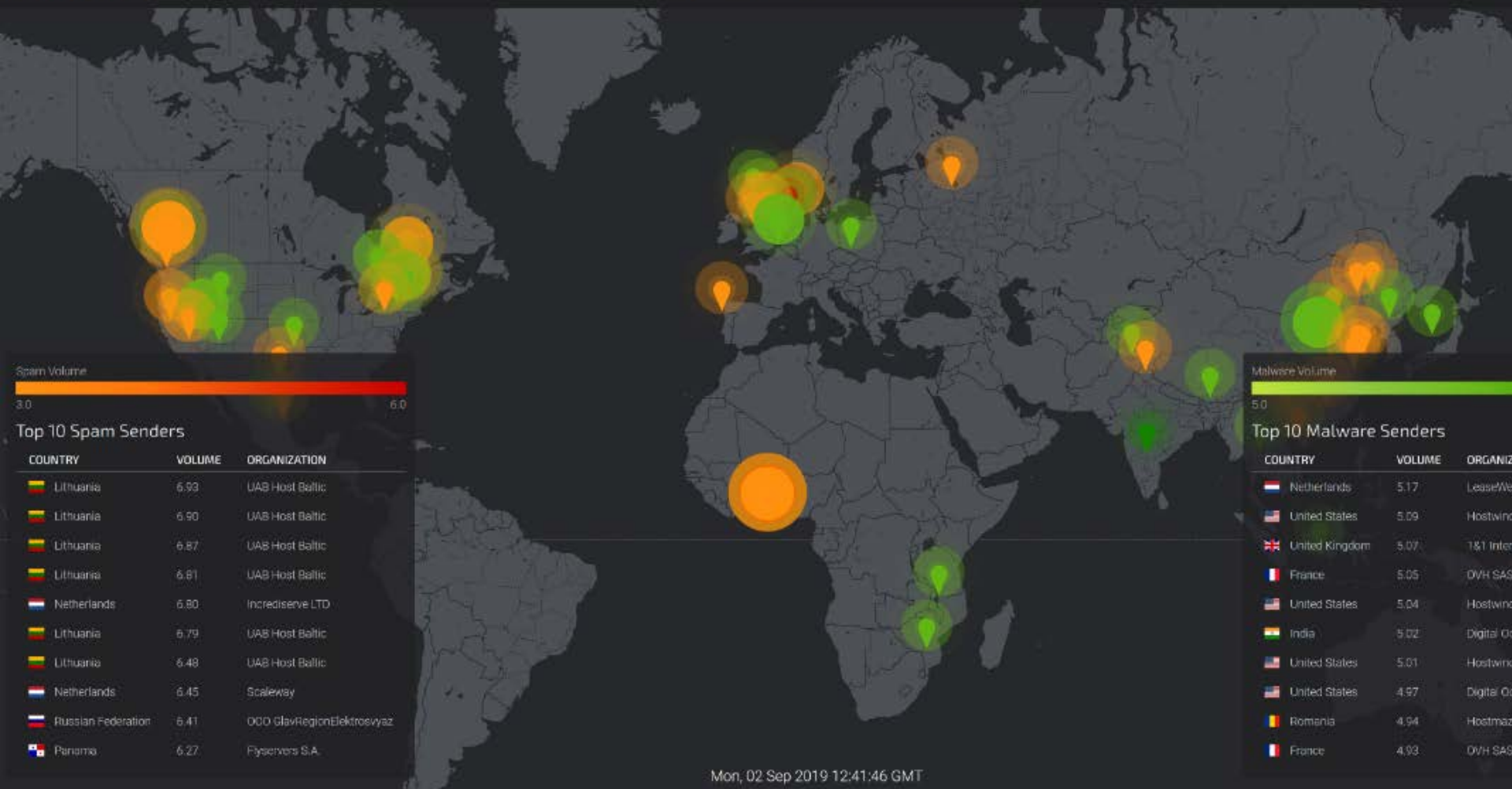


Attack Traffic Overview

Displayed are the current number of network attacks by major geographic region (State or Country). Highest volume regions are called out below.

100% Below normal





Norse Hacking Attack Map : Real Time

NORSE

ATTACK ORIGINS

Country

- China
- United States
- Hong Kong
- Germany
- Netherlands
- Colombia
- Italy
- Mil/Gov
- Taiwan
- India

ATTACK TARGETS

#	Country
424	United States
13	Hong Kong
8	Thailand
7	Netherlands
5	Italy
4	Portugal
4	Germany
3	France
3	Singapore
2	Turkey

ATTACKS

Timestamp	Organization	Attacker Location	IP	Target Location	Type	Port
05:35:03.62	CariNet	San Diego, United States	66.240.192.138	Seattle, United States	unknown	9151
05:35:03.93	N/A	unknown, China	202.112.51.64	San Rafael, United States	domain	53
05:35:04.27	BSNL	Aurangabad, India	117.218.19.164	Seattle, United States	telnet	23
05:35:04.60	N/A	unknown, Mil/Gov	103.224.165.47	Seattle, United States	vnc	5900
05:35:04.93	Petersburg Internet	Saint Petersburg, Russia	146.185.239.104	Saint Louis, United States	unknown	8090

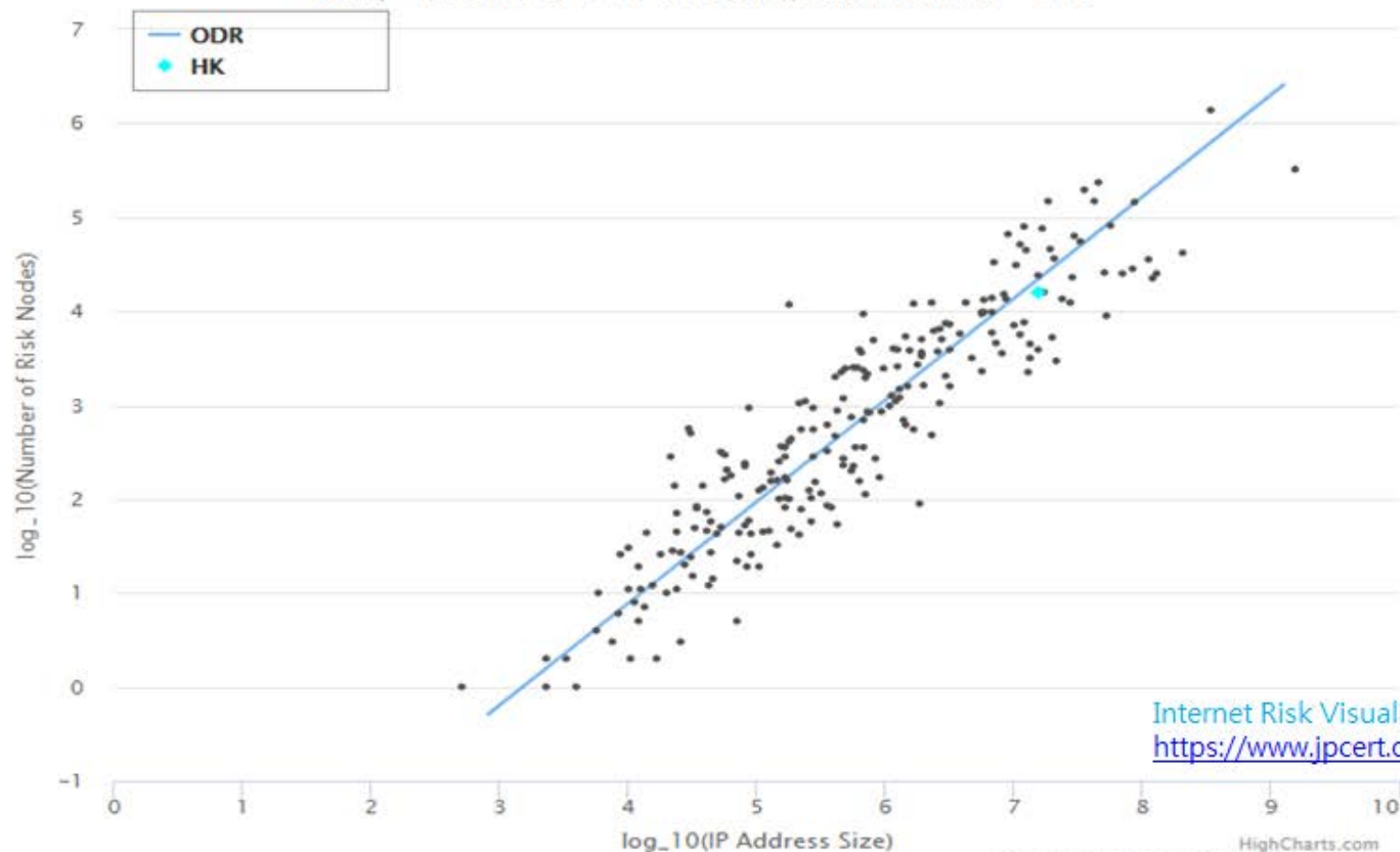
ATTACK TYPES

#	Service	Port
228	ssh	22
68	telnet	23
15	netbios-dgm	138
15	domain	53
14	ms-sql-s	143

Count of DNS(SHODAN) Nodes vs. IP address assigned to ccTLD



ODR: $y = (1.08 \pm 0.03) * x + (-3.44 \pm 0.18)$, ResidualVariance = 0.12



Internet Risk Visualization Service -Mejiro
<https://www.jpCERT.or.jp/english/mejiro/#>

Supporting the Internet Security in ASIA PACIFIC

APCERT cooperates with CERTs (Computer Emergency Response Teams) and CSIRTs (Computer Security Incident Response Teams) to ensure Internet security in the Asia Pacific region, based around genuine information sharing, trust and cooperation.

[▶ More about APCERT](#)



KrCERT



What's NEW

[▶ Back Number](#)

31 July 2019

[APCERT Drill 2019 – Catastrophic Silent Draining in Enterprise Network](#) updated

28 May 2019

[FAQ — Membership/Partnership Updated](#)

9 May 2019

[APCERT Annual Report 2018 Released](#)

4 March 2019

[FINCSIRT joins APCERT Liaison Partner](#)

FINCSIRT (Financial Sector CSIRT, Sri Lanka)'s Liaison Partnership application has been accepted.

[Panasonic PSIRT joins APCERT Corporate Partner](#)

Panasonic PSIRT's Corporate Partnership application has been accepted.

24 February 2019

[APCERT Policy on Information Sharing and Handling](#) approved

23 October 2018

[Results of the APCERT Steering Committee \(SC\) Election 2018](#)

- Chair: ACSC (2018-2019)

▶ APCERT AGM & Conference

Date: 29 September - 2 October

Venue: Singapore

Hosted by: SingCERT (Singapore)

▶ APCERT Annual Report

APCERT Annual Report 2018 activity updates of member teams. ▶



▶ Event Calendar



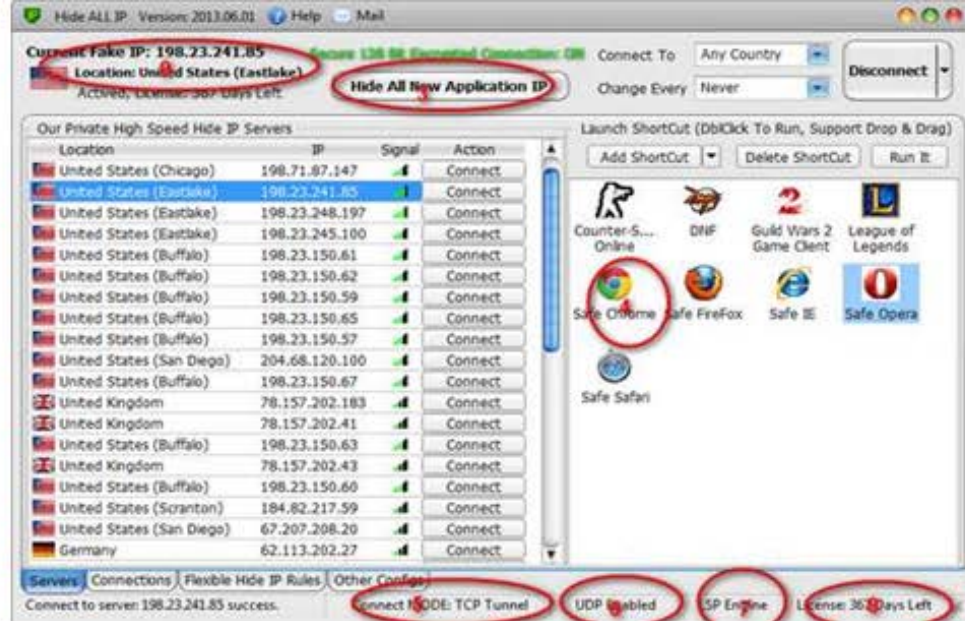
International
Security Event



Cooperation of CERTS
in Asia-Pacific Regions
regardless of borderlines

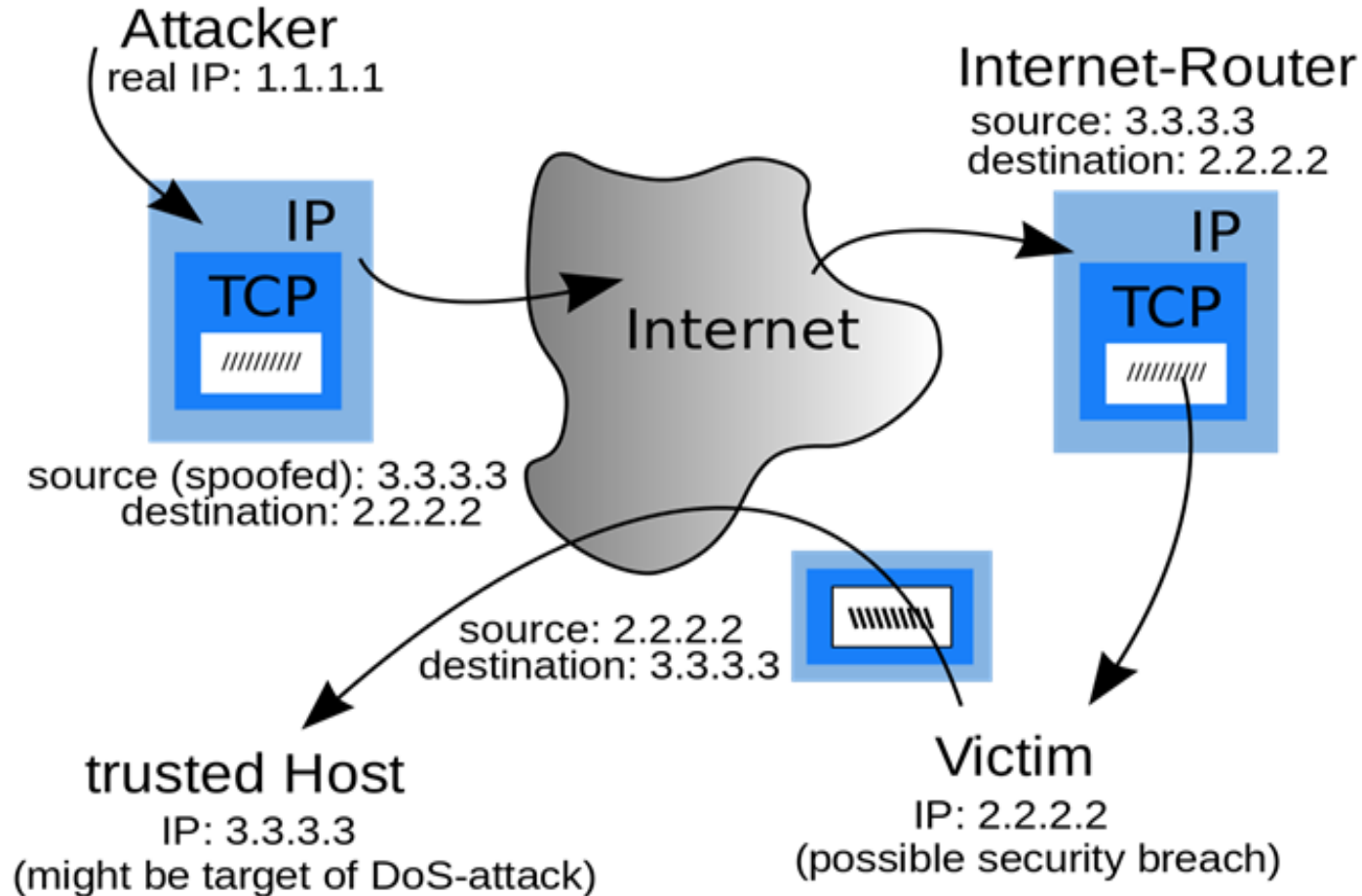


Fake IP Address, Fake Location



- IP address is used to uniquely identify and locate that system for the purpose of data transmission
- What if IP Numbers are fake?

IP Address Spoofing



IPv4 Network Packet Headers

0	4	8	16	19	31
Version	Header Length	Service Type	Total Length		
Identification			Flags	Fragment Offset	
TTI	Protocol		Header Checksum		
8.8.8.8		Source IP Addr			
5.6.7.8		Destination IP Addr			
Options				Padding	

VNC (Virtual Network Computing)



IP Information: **117.203.239.173**

ISP: BSNL
Organization: BSNL
Connection: Broadband
Services: None Detected
City: Aurangabad
Region: Maharashtra
Country: India

117.203.239.173

Additional IP Details

**Before IP spoofing
my location is India**



IP Information: **202.142.24.192**

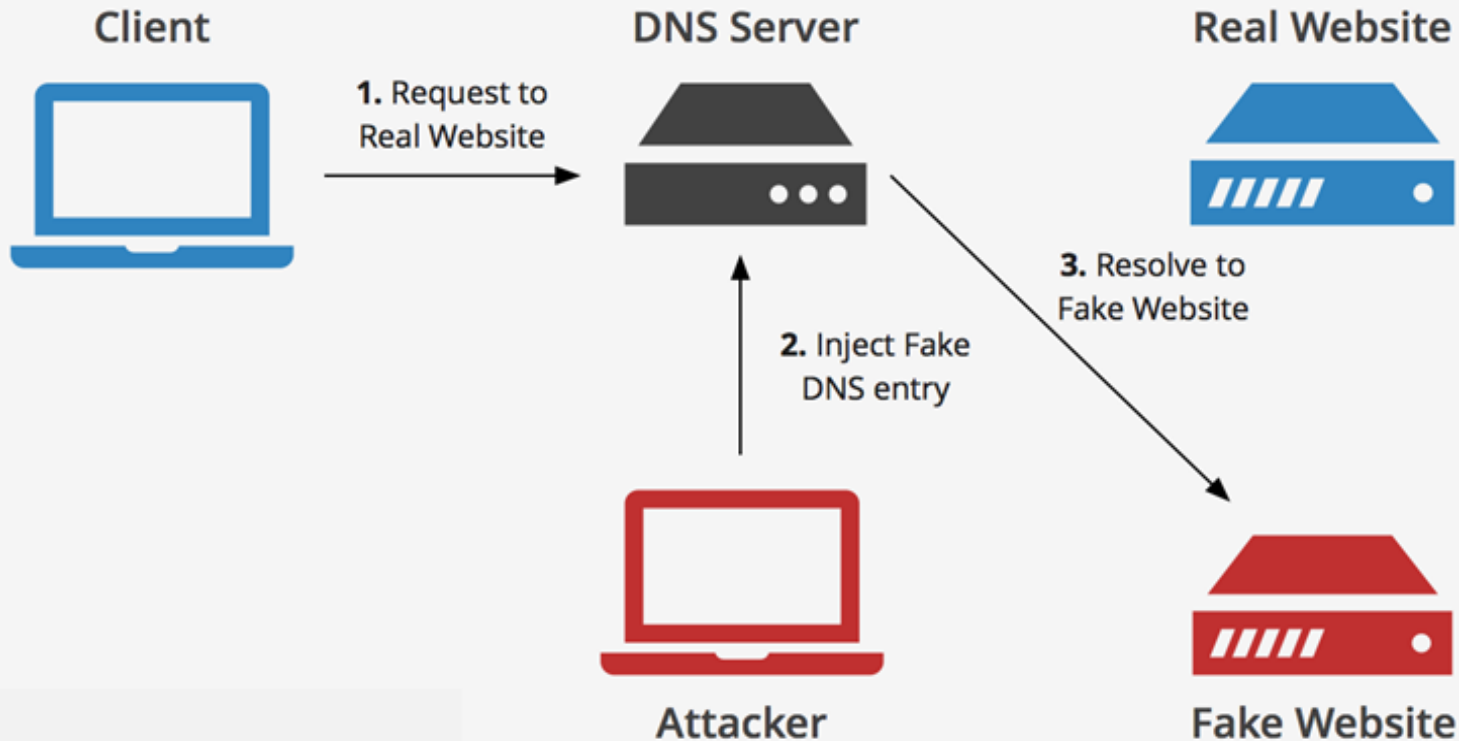
ISP: Chijun Network (Beijing)Consulting&Service
Organization: Chijun Network (Beijing)Consulting&Service
Connection: Broadband
Services: Suspected Network Sharing Device
City: Beijing
Region: Beijing
Country: China

202.142.24.192

Additional IP Details

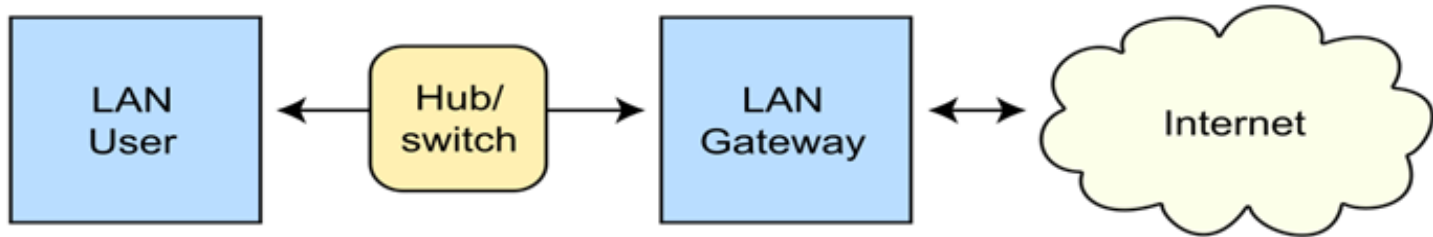
**After IP spoofing
my location is China**

DNS Spoofing

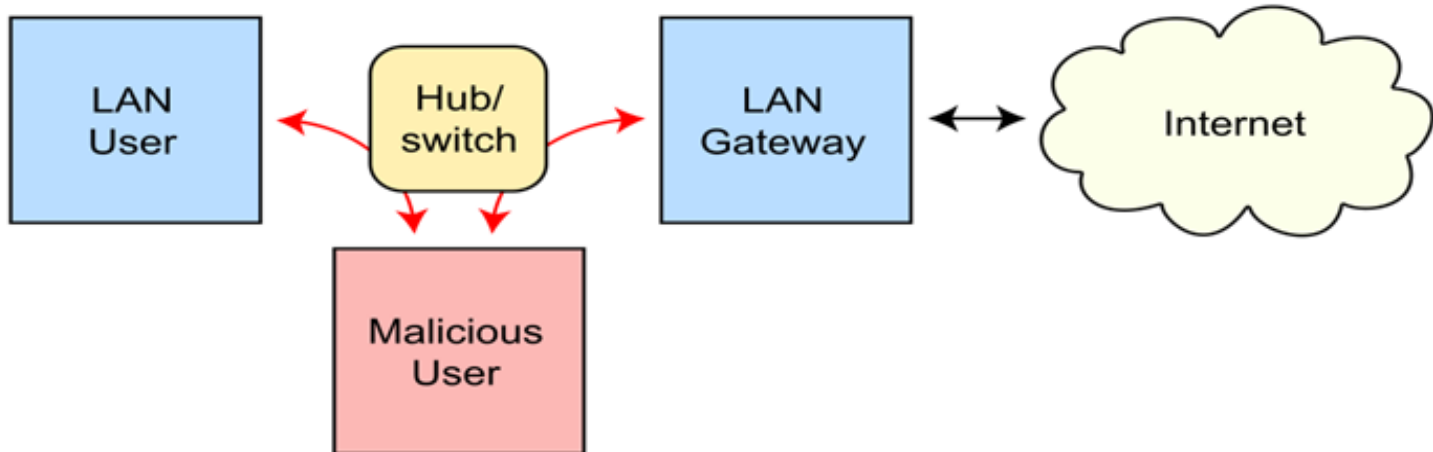


Address Resolution Protocol Spoofing

Routing under normal operation



Routing subject to ARP cache poisoning

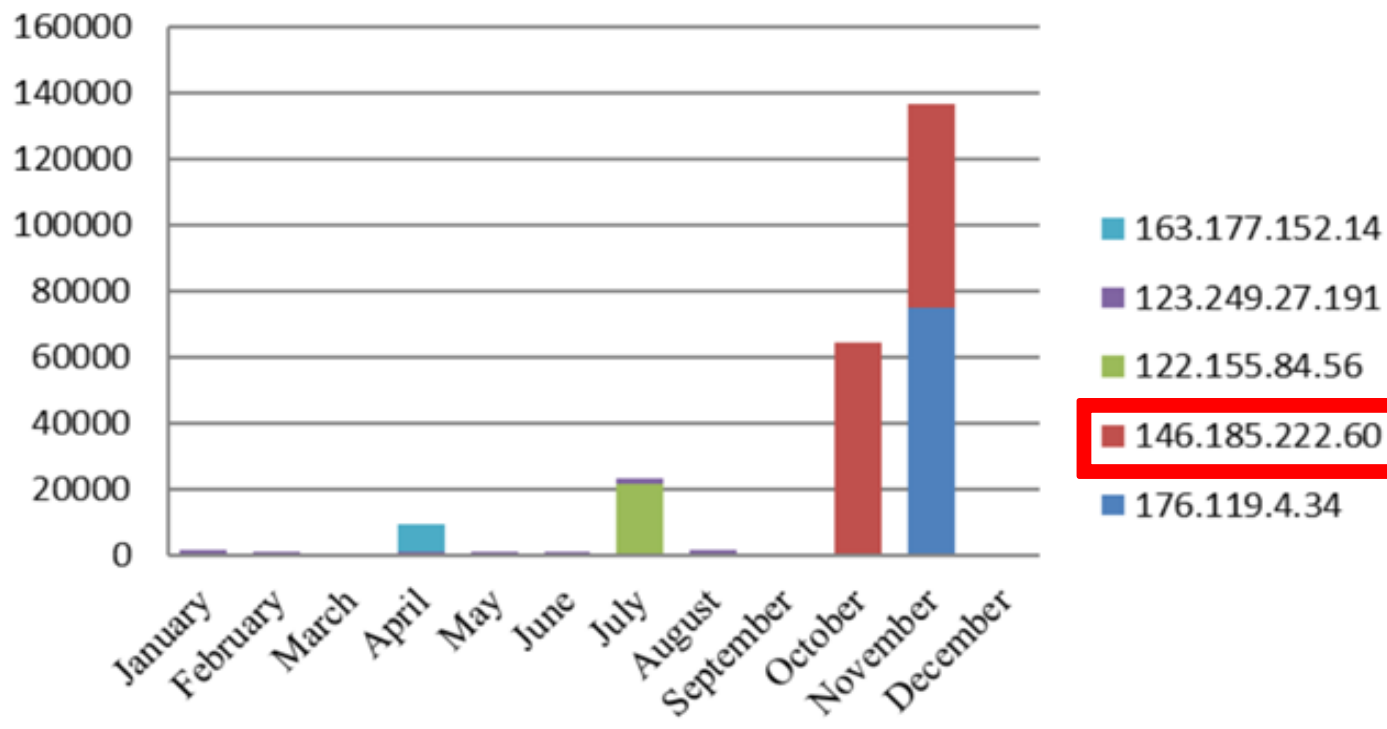


Seeking Address: Why Cyber Attacks Are So Difficult to Trace Back to Hackers

Sony, Google, RSA and now Citigroup are just some of the prominent victims of cyber attacks as defenses at large organizations prove porous and attackers elude detection

....invasive attacks on a much more regular basis, but **IP address unknown**

Top 5 Source IP Address in 2018





?



[Home](#) > [Whois Lookup](#) > 146.185.222.60

IP Information for 146.185.222.60

— Quick Stats

IP Location	 Russian Federation Saint Petersburg Petersburg Internet Network Ltd.
ASN	 AS44050 PIN-AS, RU (registered Nov 09, 2007)
Whois Server	whois.ripe.net
IP Address	146.185.222.60



% Abuse contact for '146.185.222.0 - 146.185.222.255' is ' abuse@pinspb.ru '

```
inetnum:      146.185.222.0 - 146.185.222.255
netname:      cust17011
country:      RU
admin-c:      MC40674-RIPE
tech-c:       MC40674-RIPE
status:       ASSIGNED PA
mnt-by:       MNT-PINSUPPORT
created:      2019-08-21T13:08:04Z
last-modified: 2019-08-21T13:08:04Z
source:       RIPE
```

Sony Pictures hacked



Hacked By #GOP

Warning :

We've already warned you, and this is just a beginning.

We continue till our request be met.

We've obtained all your internal data including your secrets and top secrets.

If you don't obey us, we'll release data shown below to the world.

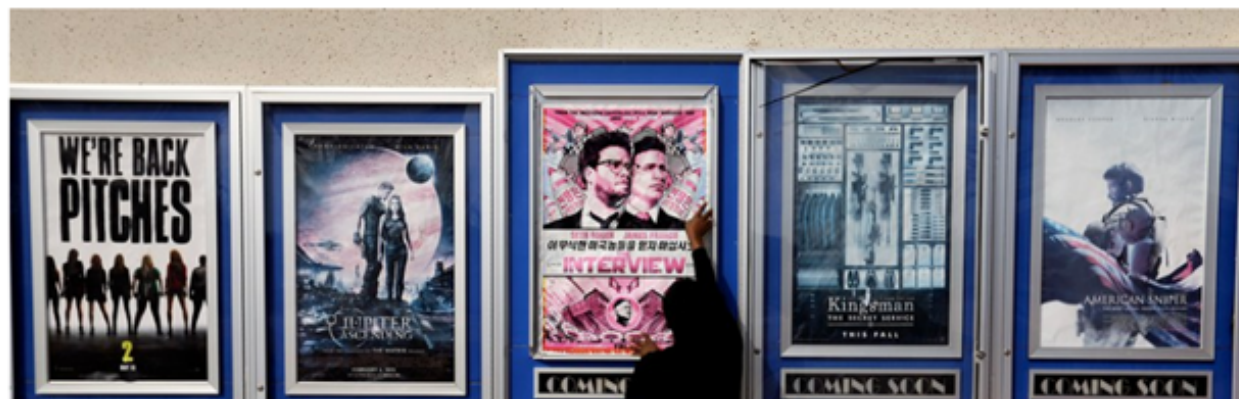
Determine what will you do till November the **24th, 11:00 PM(GMT).**

False allegation owing to **bogus IP address**

The Evidence That North Korea Hacked Sony Is Flimsy



WIRED



- South Korea blamed North Korea for the attack as well as China—since an IP address in China appeared
-Officials later retracted the allegations.



tty198410@gmail.com

@hyon_u

@erica_333u

agena316@gmail.com

"Andoson David" FB

yardgen@gmail.com

watsonhenny@gmail.com

agena316@gmail.com's FB



BANGLADESH BANK
Central Bank of Bangladesh

ACCOUNT ATTACK INFRASTRUCTURE

MALWARE DEPLOYED

SIERRA CHARLIE
(msoutc.exe)

Shared Framework

Secure Delete Function

evtsys.exe

MACKTRUCK
BACKDOOR

NESTEGG
BACKDOOR

BRAMBUL
WORM

MACKTRUCK
BACKDOOR

DESTOVER

Same Family

Same Family & Shared
Encryption Key

Secure
Delete
Function

Philippine Bank

NESTEGG
BACKDOOR

CONTOPEE
BACKDOOR

Dropper/Variant Shared IP

Shared Passive Table (TLS)

Shared Passive Table (TLS)

Secure Delete Function

Secure Delete Function

Shared Passive Table (TLS)

Variant Infected
Common Victim

WANNACRY
V0, V1, or V2

Shared Passive Table (TLS)

Shared Passive Table (TLS)

Code Similarities/DDNS Link

Chart 3



How US authorities tracked down the North Korean hacker behind WannaCry

US authorities put together four years worth of malware samples, domain names, email and social media accounts to track down one of the Lazarus Group hackers.

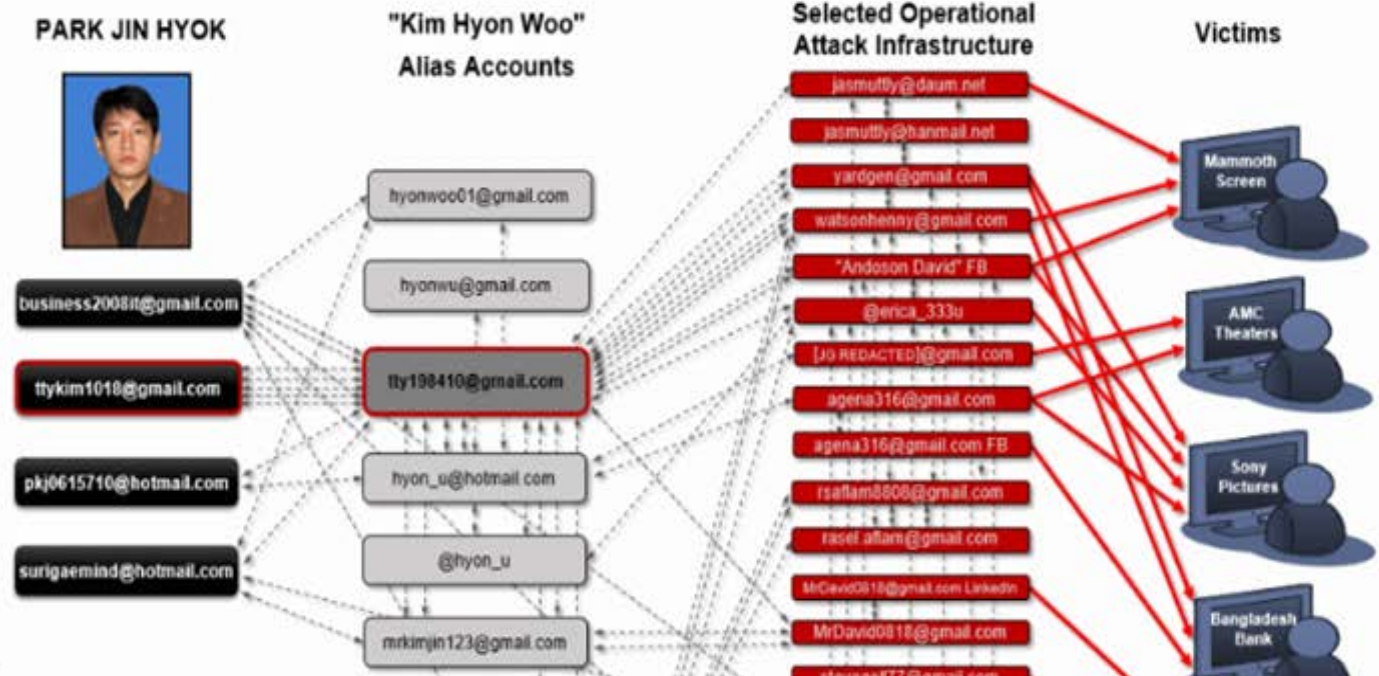
- The WannaCry ransomware outbreak of 2017
- Attempts of hacking Lockheed Martin in 2016
- The 2016 Bangladesh Central Bank cyber-heist
- The breach at Sony Pictures Entertainment in 2014

North Korean Hacker spreaded WannaCry and Trojan.Alphanc using

IP address 84.92.36.96

FAKE

→ for “Command-and-Control”



The hardest problem in finding the source of cyber attacks is **attribution** . You will be trying to find out who's doing it, but purely technical means are insufficient.

Untraceable of IP Addresses

- Murky Real Physical Location
- Impossible to Trace Attackers
- **Elusive Quest of Cyber Attribution**

determining the actor responsible for a cyberattack

Technical attribution

- * **The body of evidence collected for technical attribution**
- * **Identifying IP address. and conducting extensive forensic investigations,**

IOCs: IP addrs,
logfiles, hashes,
domain names,
pcap, netflow, etc



Higher level IOCs:
programming languages,
coding patterns, patterns of
life/time of day, TTPs, and
tradecraft

**signals intelligence,
human intelligence**

Info:
SIGINT,
HUMINT,
OSINT

Context: geopolitical,
economic, individual
motives; military or
intelligence tradecraft


Political attribution

APTs: Nation-state,
nation-state actor,
criminal group, terrorists

What makes Cyber Attribution difficult..

- **Untraceable IP Address**. Fake metadata are the Most Potent Weapon in Cyberwar.
- **Lack of end-to-end accountability** in the current Internet infrastructure.
- **Invisibility** : Cyber attacks spanning jurisdictions, networks, and devices are only partially observable from the point of view of a defender.
- **Lack of Jurisdiction** allowing investigation



 **Zeljka Zorz**, Managing Editor
May 10, 2016

Share this article



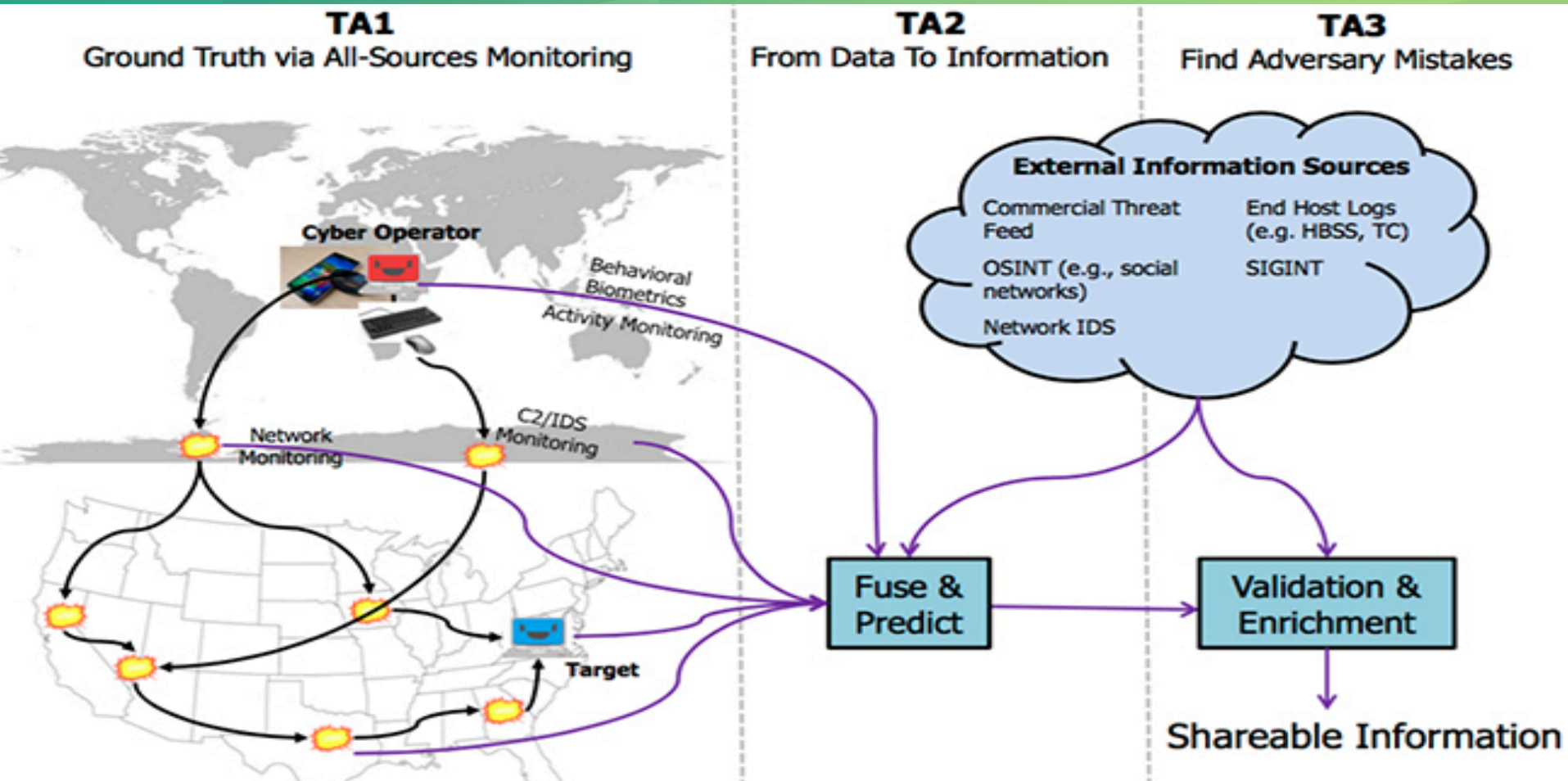
DARPA calls for help to improve cyber attack attribution

9th annual (ISC)2 Security Congress in Orlando, FL – Trainings, Keynotes and More!

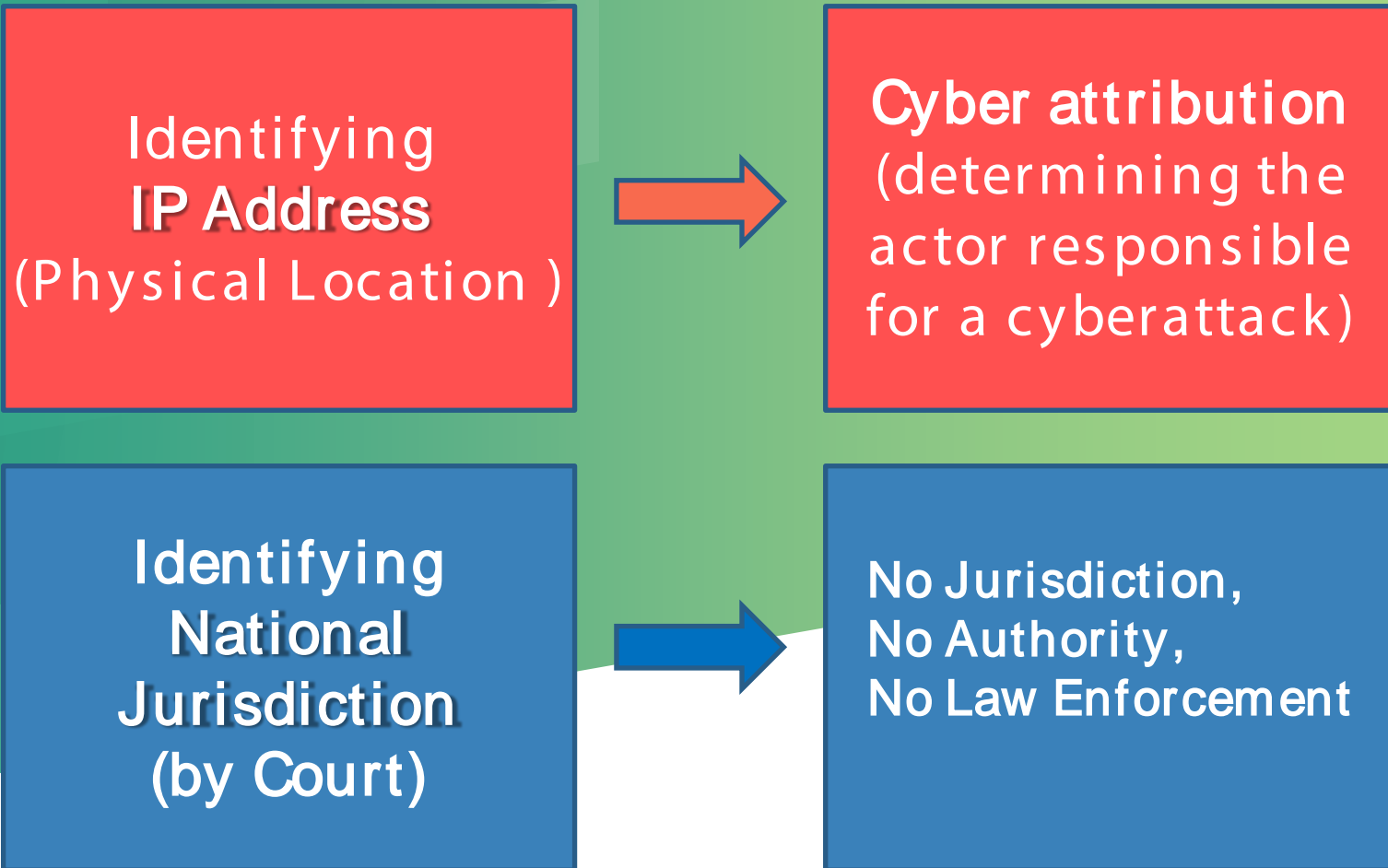
Reliable cyber attack attribution is currently almost impossible, and the Defense Advanced Research Projects Agency (DARPA) wants to find a solution for that problem.

<https://www.helpnetsecurity.com/2016/05/10/darpa-cyber-attack-attribution/>

Attribution program by U.S. DARPA



IP Addresses do not recognize National jurisdiction. Both are often mismatched



The Principality of Sealand with its own National Jurisdiction





SEALAND
E MARE LIBERTAS

[HOME](#)[ABOUT](#)[ONLINE SHOP](#)[MEDIA](#)[NEWS](#)[DONATIONS](#)[CONTACT](#)

PRINCIPALITY OF SEALAND

Sealand was founded as a sovereign Principality in 1967 in international waters, seven miles off the eastern shores of Britain.

[ABOUT SEALAND](#)[VISIT SEALAND STORE](#)

Since 1967, **SEALNAD** claimed its own sovereign nation with its own flag, currency, passports, jurisdictional and legal status



SEALNAD has fired a weapon towards a English government vessel in order to defend their territory.

English court found that it **lacked jurisdiction over SEALNAD.**

Which jurisdiction an unknown IP Address does fall under if a crime is committed using it?

[EXAMPLE] The Silk Road website used TOR that obfuscated user's real location online. TOR does not use any common Top Level Domain nor IP address

What country would have jurisdiction to try and shut down the Silk Road website?

Without IP address connected to any domain name, how can any Gov't authority trace bad guys?



Silk Road
anonymous marketplace

Welcome **OzFree**
messages(0) | orders(0) | account(฿0.00) | settings |

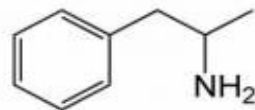
Online black market in The Darknet

Shop by category:

Drugs(1582)
Cannabis(271)
Dissociatives(33)
Ecstasy(217)
Opioids(106)
Other(65)
Prescription(274)
Psychedelics(306)
Stimulants(190)
Apparel(37)
Art(1)
Books(300)
Computer equipment(9)
Digital goods(218)
Drug paraphernalia(33)
Electronics(13)



10 Grams high grade
MDMA 80+ %
฿61.17



Amphetamines sulfate /
Speed freebase...
฿28.59



2g Jack Frost (weed) *420
SALE****
฿8.54



5 Grams of pure MDMA
crystals
฿42.04



100 red Y tablets 111mg
(lab tested)...
฿97.77



Michael Jackson
Discography 1971-2009...
฿2.52

News:

- The gift that ke on **giving**
- Who's your **favorite?**
- Acknowledging **Heroes**
- A new annonyr market **The Armory!**
- **State of the F Address**



Congratulations!

This browser is configured to use Tor.

You are now free to browse the Internet anonymously.

[Test Tor Network Settings](#)

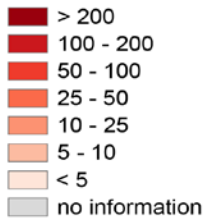
Search securely with Startpage.

Tor ("The Onion Router") conceals the location and IP address

Originally designed to protect the identity of U.S. operatives and dissidents in repressive countries like China.

The anonymous Internet

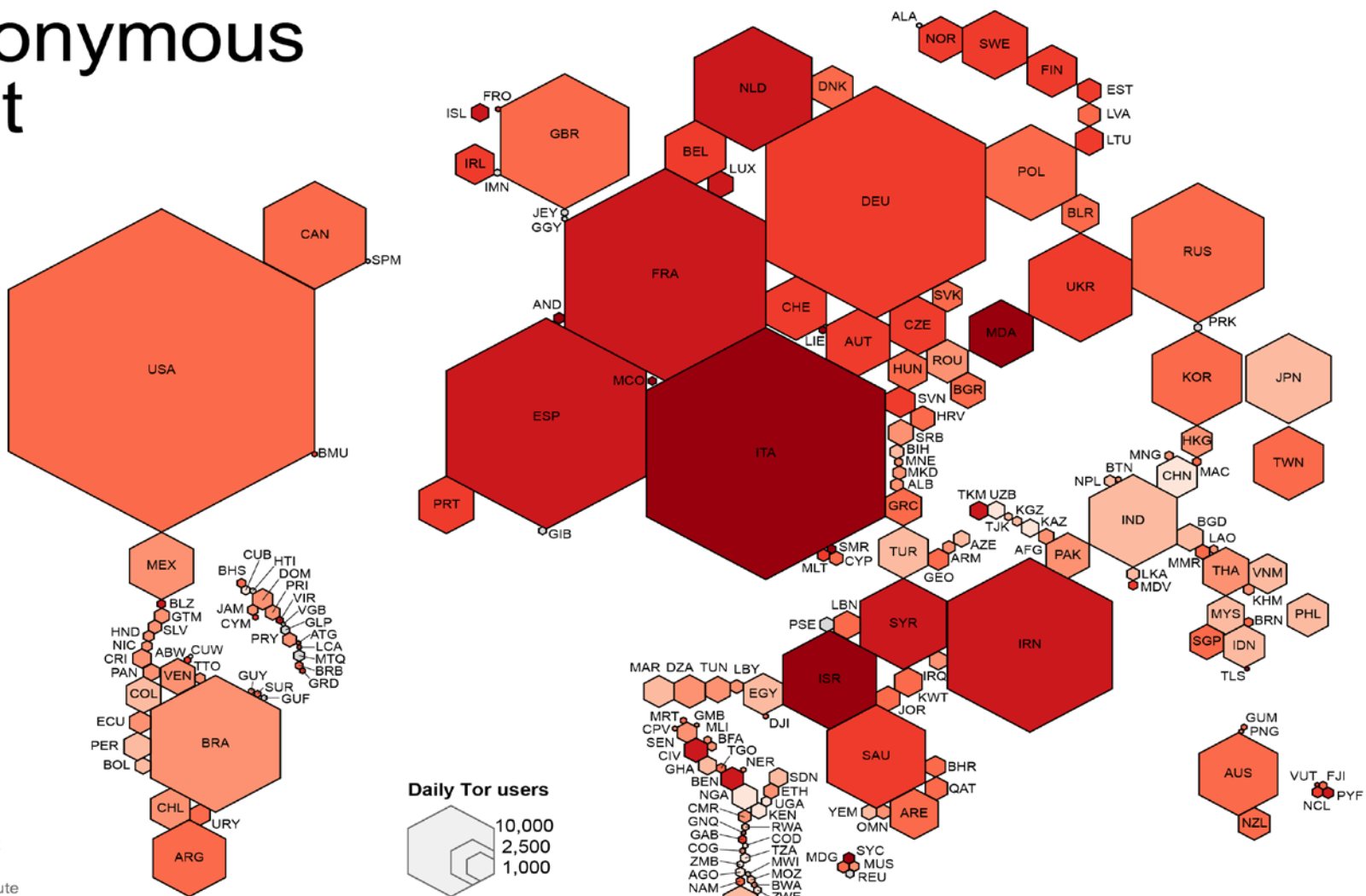
Daily Tor users
per 100,000
Internet users



Average number of
Tor users per day
calculated between
August 2012 and
July 2013

data sources:
Tor Metrics Portal
metrics.torproject.org
World Bank
data.worldbank.org

by Mark Graham
(@geoplace) and
Stefano De Sabbata
(@maps4thought)
Internet Geographies at
the Oxford Internet Institute
2014 • geography.oii.ox.ac.uk



US Court of Appeals: An IP address isn't enough to identify a pirate

Copyright owners will need more if they want a successful legal case

By William Gayde on August 29, 2018, 6:13 AM | 27 comments



Why it matters: Judge rules that copyright trolls need more than just an IP address if they want to go after copyright infringement. An IP is not enough proof to tie a person a crime.

After tracing infringement of its copyrights to a particular IP address, Cobbler Nevada, LLC **filed a lawsuit against the John Doe IP address** for direct and contributory copyright infringement.

[US Court] Copyright trolls need more than just an IP address if they want to go after copyright infringement. **An IP address is not enough proof to tie a person to a crime.**



Judge throws out mass John Doe porn copyright lawsuits

Porn studios can't determine who downloaded their movies from BitTorrent by using an IP address, the judge says

An IP address is not a specific person and may not even be a particular state.

Courts quash copyright trolls; recognize IP address is not a person

Justice finally served when judges can spell 'Internet,' tell assets from IP addresses



In 2012, federal judge in New York state denied the request of three porn studios to subpoena the names of users of 79 IP addresses.

Tracing IP address to file a lawsuit against the **unknown person's IP address** for illegal action, will not be accepted by the Courts.

...because **IP address is not enough proof to tie a person to a crime or illegal action.**



COUR DE JUSTICE
DE L'UNION
EUROPÉENNE

Court of Justice of the European Union Patrick Breyer v. Germany

**Court confirms that IP
addresses are personal data in
some cases**

**..collection and further processing of IP addresses
would be subject to EU data protection law**

IP Addresses at Odds with Jurisdiction

Why national jurisdiction becomes an
impediment in cyber attack attribution
and investigation?

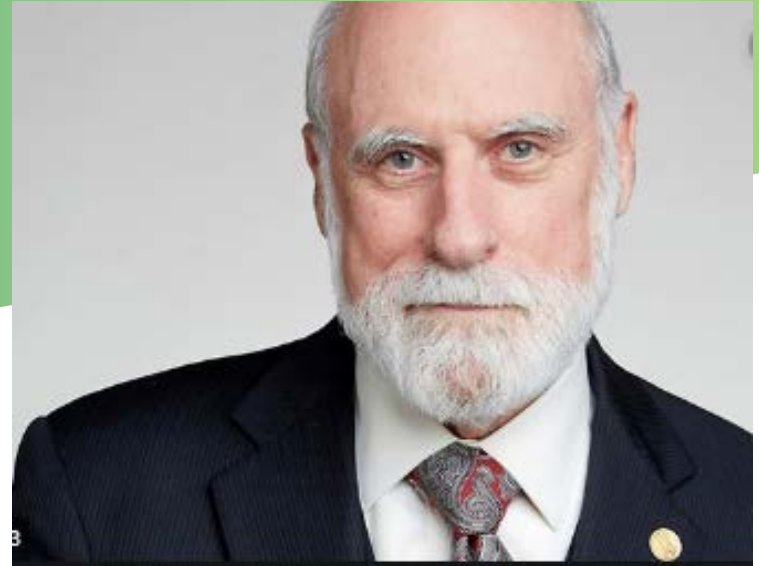
Jurisdictional Limitations

Jurisdictional limitations can hinder attribution in cross-border cybercrime investigations

To determine the actor responsible for a cyberattack, every time a law enforcement agency has to undertake an investigation that crosses borders

It must go through official channels to request help.

“ How do we collectively develop legal norms that apply in cyber space, while respecting the integrity of national jurisdictions?”



Challenges in Cyber Attribution

1. Hard to find strong evidences for reaching a correct conclusion about the sources of attacks
2. Investigation needs **metadata** connected to the attack including IP addresses, email data, hosting platforms, domain names. → **Fake metadata are generated**
3. **Untracable real IP Addresses** (easily hidden by VPN Software, Proxy Server, Tor Browser. Changing IP addresses, and using Public Wi-Fi)

Challenges in Cyber Attribution

4. Linking indications together. Technical, political, and all-source indicators are all tools used in determining cyber attribution.
5. Cyber attackers strongly deny evidences. Courts often relies on physical evidence.
6. Effective cyber attribution investigations cross -borders are being blocked by national jurisdiction

Stateless

Attribution

Toward International Accountability in Cyberspace



'Global Cyber Attribution Consortium'

- International experts provide independent investigation of major cyber incidents for the purpose of attribution.
- Avoid an appearance of bias and to protect transparency
- Work with victims with their cooperation to investigate cyber incidents
- Standardize methodological approaches



SHARE



IS IT TIME TO INSTITUTIONALIZE CYBER-ATTRIBUTION?

Posted on August 21, 2018 by [Karl Grindal](#), [Brenden Kuerbis](#), [Farzaneh Badii](#) and [Milton Mueller](#)



Authoritative attribution of cyberattacks to nation-state actors requires more than purely technical solutions. New institutions are needed to develop the credibility and procedural checks and balances that can take attribution beyond one nation pointing its finger at one of its adversaries. This white paper explores the attribution challenge, reviews proposed models for new institutions and sketches an agenda for future research.



Keywords—attribution; cybersecurity; forensics; governance; internet; transnational institution