Reflections on SSH Attacks 2019

Global Surveillance Awareness & Counter Measures

Efe Orhun - Managing Partner, CISSP
January 2020

Contents

Overview

Companies in the Small to Medium Business (SMB) segment often say they're too small to suffer cyber-attacks, they don't have technology or data of interest, and it seems unbelievable that nation states would be interested in them; this translate to a lack of investment in security process and technology and ultimately an increase in their cyber risk. DerivativeTech's own attack data demonstrate that not only are nation states and cybercriminals interested, they're highly active. The following paper analyzes the attacks DerivativeTech observed on a single SSH server in 2019. The server is hosted on a cloud hosting provider in the United States. All the attacks observed were inbound to a server on the U.S. soil.

Surprisingly across 2019, on this single server DerivativeTech observed 4170 distinct attacks, about 392.5 attacks per month, 13.08 attacks per day and 0.545 attacks per hour. Nation states and cybercriminals, with the help of automated tools, find it easier and easier to compromise systems. The reason may not be that you have data or technology of interest; it may simply be to see if it works, or to compromise your infrastructure and re-use it. The data supports this point, in that none of the attacks observed originate from TOR (The Onion Router) exit points; meaning they were potentially direct attacks from malicious, compromised hosts or via VPN masked hosts. You can see the details on the malicious and VPN masked hosts in Appendix I, II and III respectively.

Interestingly, there were some attacks originating from the "dark address space" or "darknet" – not to be confused with the "darkweb"; accessible via services like TOR, I2P, and Freenet. Dark address space is the area of the Internet's routable address space that's currently unused, with no active servers or services. On computer networks, darknet is the address space held in reserve for future network expansion. See details in Appendix IV.

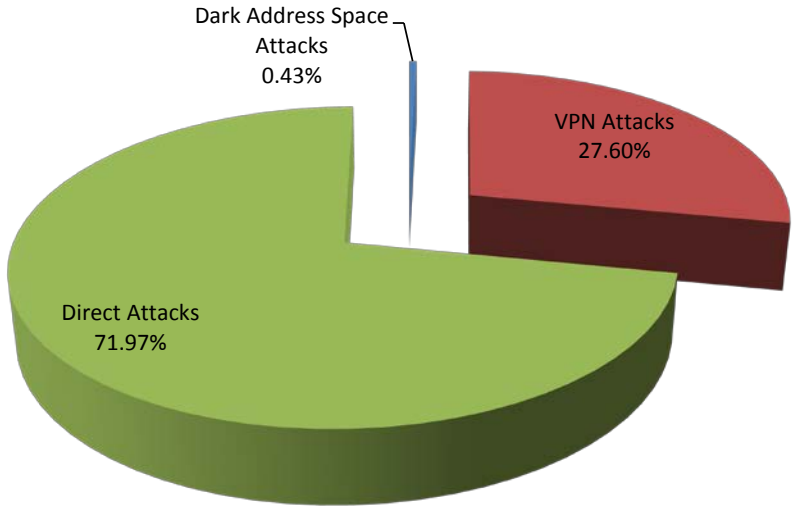


Chart 1 – Direct vs. Dark Address Space vs. VPN Based Attacks

Methodology

DerivativeTech uses its own automated tools to block and record attacks, and the attacking party is immediately scanned for fingerprinting using nmap and other custom tools are used to enrich the data features resulting in a massive data set for analysis.

The purpose of the study is twofold – to highlight the level and geographic segmentation of the attacks, to raise awareness of the alliances and nation states engaged in surveillance or potentially cybercrime. Various surveillance alliances works together to collect and share mass surveillance data. The macro insight is that collectively these alliances act as one global-surveillance entity, capable of spying on you and recording your activities on the Internet.

This paper will cover the top known alliances and the standalone countries that conduct their surveillance programs and show attack breakdowns. Standalone countries may have their own intelligence alliances, but they are not part of the NSA's network. The specific alliances covered in this report:

Alliances:

- 5-EYES
- 9-EYES
- 10-EYES
- 14-EYES
- Computer Network Operations Partners
- 3rd Party Agreement(s)
- NATO

Descriptions and coverage areas of these alliances are provided in their respective areas in the Attack Distribution by Alliance section.

Standalone Countries[1]:

- Russia
- China
- Iran

Attacks observed in this study are direct attacks coming to the system; we did not provide the detailed study of attribution conducted in this paper. Attribution typically comes from things like looking at the correlation of attack times, user name dictionaries used, frequency of attacks, adjacent hosts attacking in the same time frame and so forth; due to the complexity of vectors, it's typically challenging to get a conclusive result.

[1] Only reflects the major players of concern…

Why mention attribution? Just because an attack originates from a certain country doesn't mean that particular country conducted the attack; a compromised system can be used as a bounce host by any other actor on the Internet.

Given that both alliances and countries – in addition to cybercriminals - maintain annual quotas for compromising hosts and using them as staging points, bounce hosts and targets; it is quite likely that our distribution is accurate.

Overall Attack Timelines

Historically official holidays have been a common time for a significant uptake in attacks, this year the pattern changed, with relative stability across the holidays and other unusual activity peaks appearing.

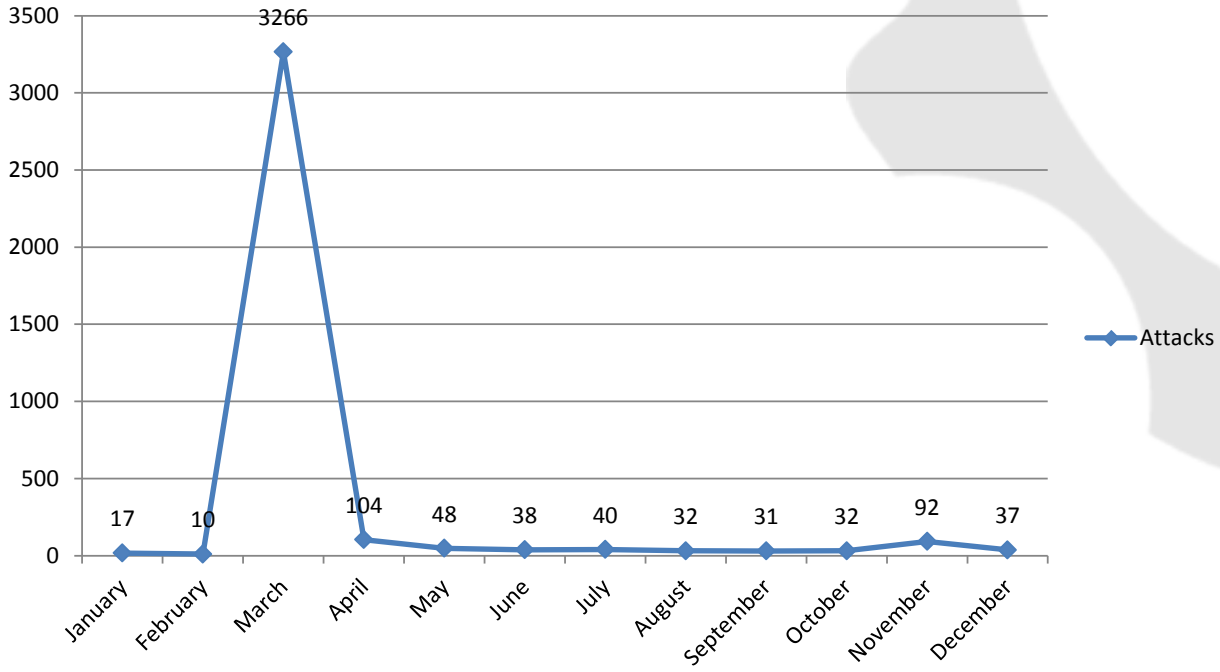


Chart 2 – Overall Attack Timelines

Most Active Attack Timeframes and Attackers

In March, April and November we observed the most active attack patterns. From an attribution perspective, it's not surprising to see the U.S. and China competing for first place.

Here are the geographic attribution breakdowns for each month:

- **March** – was an exceptional month with attacks by 112 countries about 3266 times. The usual suspects, the U.S. and China, led the pack:

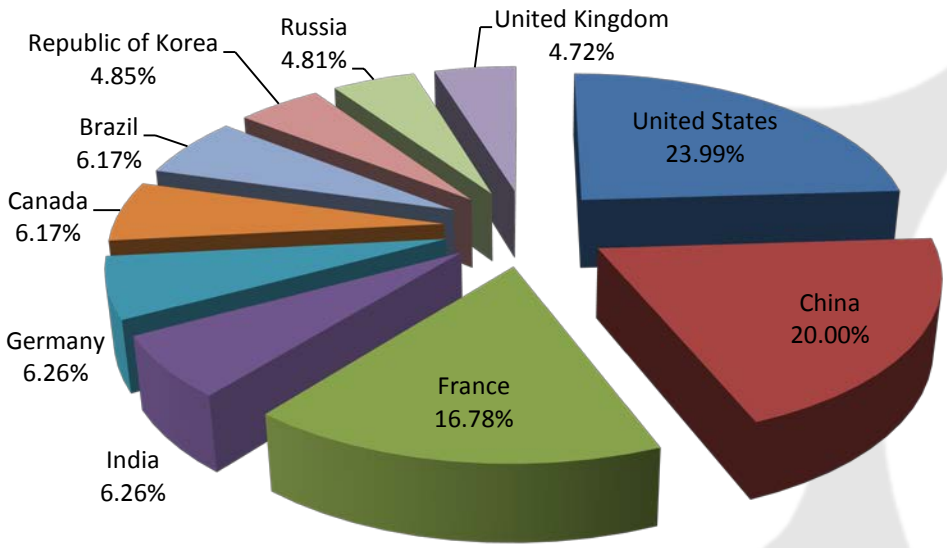


Chart 3 – Top 10 Attackers, March 2019

- **April**

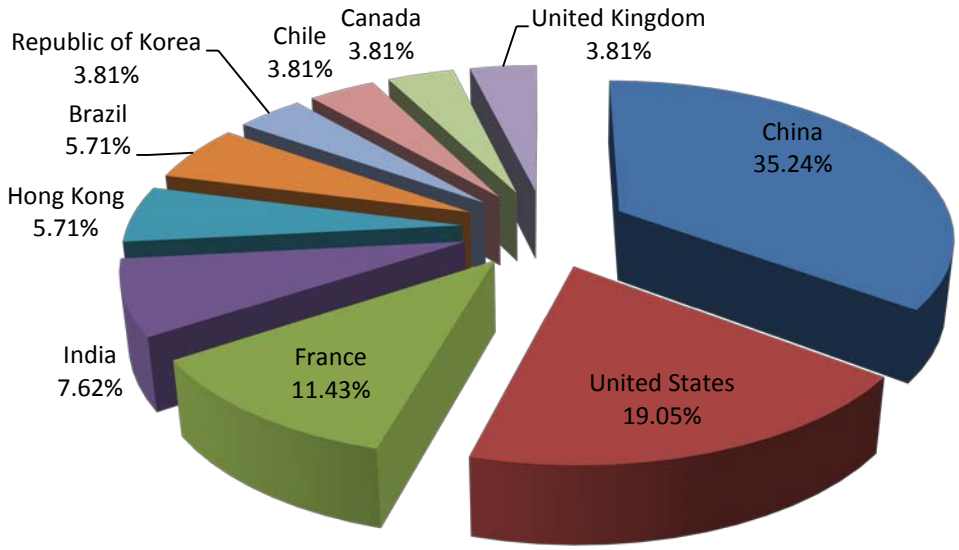


Chart 4 – Top 10 Attackers, April 2019

- **November**

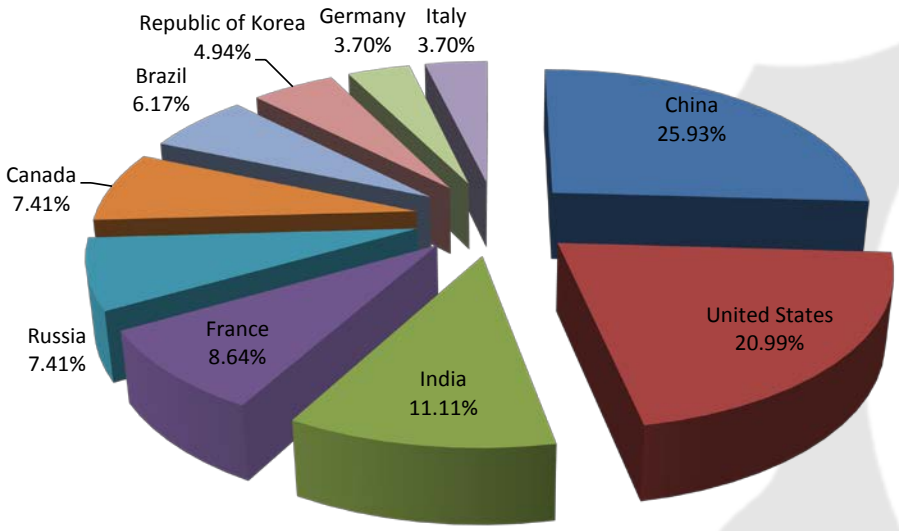


Chart 5 – Top 10 Attackers, November 2019

Top 20 Attackers

The U.S. and China also lead the top 20 attackers list, with this list of attackers making up about 82% of all attacks.

Attacking Country	CC	Membership	Ranking
United States	US	FVEY, 9-EYES, 10-EYES, 14-EYES, 3rd Party, NATO	1
China	CN	Standalone	2
France	FR	9-EYES, 10-EYES, 14-EYES, 3rd Party, NATO	3
India	IN	10-EYES	4
Brazil	BR	Standalone	5
Canada	CA	FVEY, 9-EYES, 10-EYES, 14-EYES, 3rd Party, NATO	6
Germany	DE	14-EYES, CNO, 3rd Party, NATO	7
Republic of Korea	KR	10-EYES, CNO, 3rd Party	8
United Kingdom	GB	FVEY, 9-EYES, 10-EYES, 14-EYES, 3rd Party, NATO	9
Russia	RU	Standalone	10
Singapore	SG	10-EYES, 3rd Party	11
Indonesia	ID	Standalone	12
Netherlands	NL	9-EYES, 14-EYES, CNO, 3rd Party, NATO	13
Italy	IT	14-EYES, CNO, 3rd Party, NATO	14
Vietnam	VN	Standalone	15

Poland	PL	CNO, 3rd Party	16
Taiwan	TW	3rd Party	17
Hong Kong	HK	Standalone	18
Thailand	TH	10-EYES, 3rd Party	19
Colombia	CO	Standalone	20

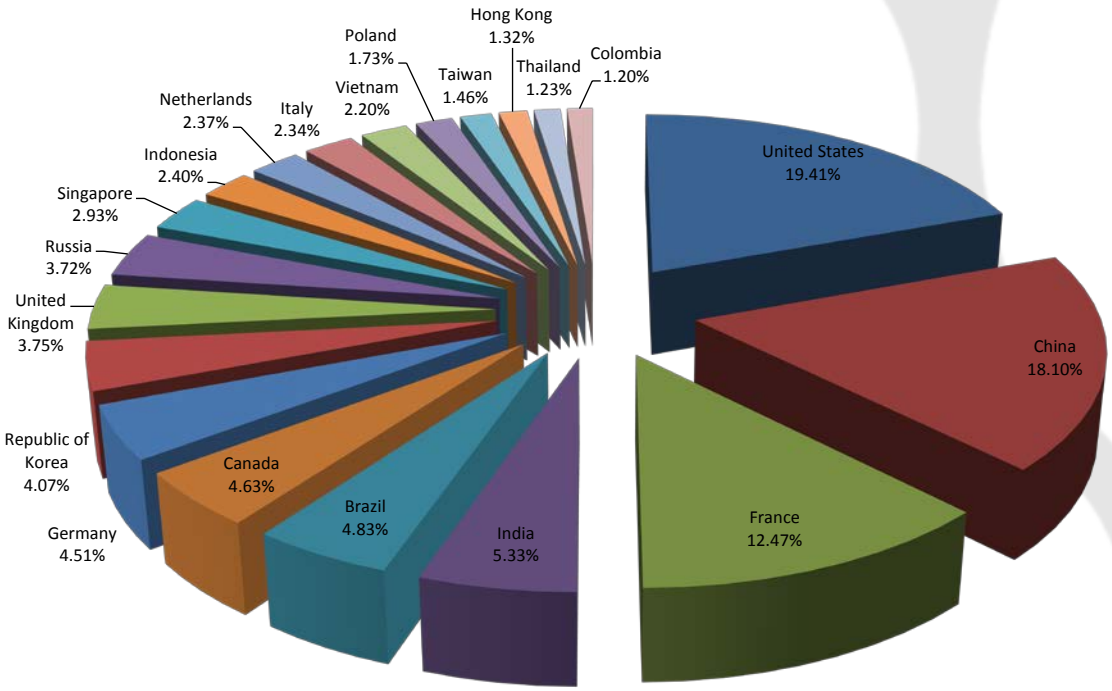


Chart 6 – Top 20 Attacking Countries

The U.S. and China (and Hong Kong) are almost head to head and account for 19.41% and 19.42% of the attacks respectively. Hong Kong is interesting, as the territory is divided between China and the Western powers; it is almost certain Hong Kong is a CNO country as well as a launch point for Chinese attacks; for the purposes of this section it is grouped with China.

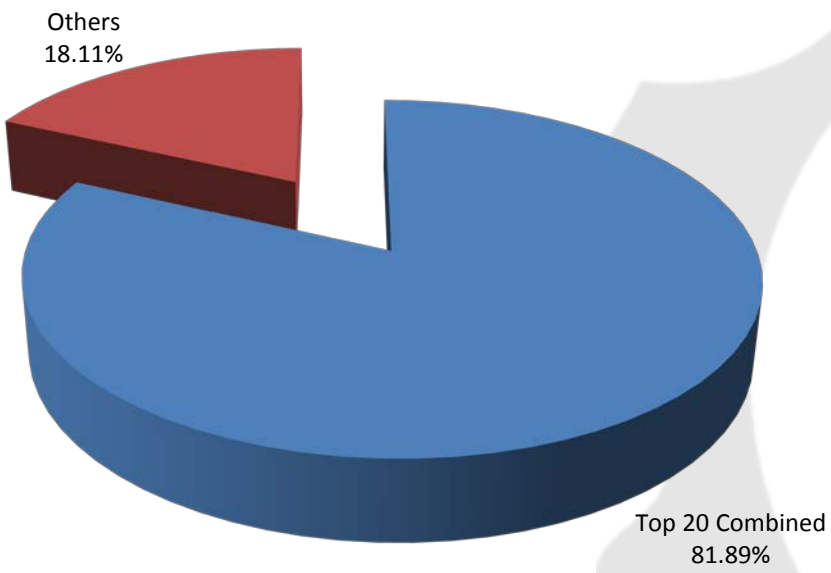


Chart 7 – Top 20 Attacking vs. Others

Attack Distribution by Alliance

Many, if not most, global citizens are currently under surveillance via one or more alliances or nation states. Managing cyber risk properly requires an awareness of surveillance in play during data use and transfer, and benefits from an understanding of the overlapping models and methods.

Coverage of the global surveillance alliances and nation states is provided below:

Alliances:

- 5-EYES
- 9-EYES
- 10-EYES
- 14-EYES
- Computer Network Operations Partners
- 3rd Party Agreement(s)
- NATO

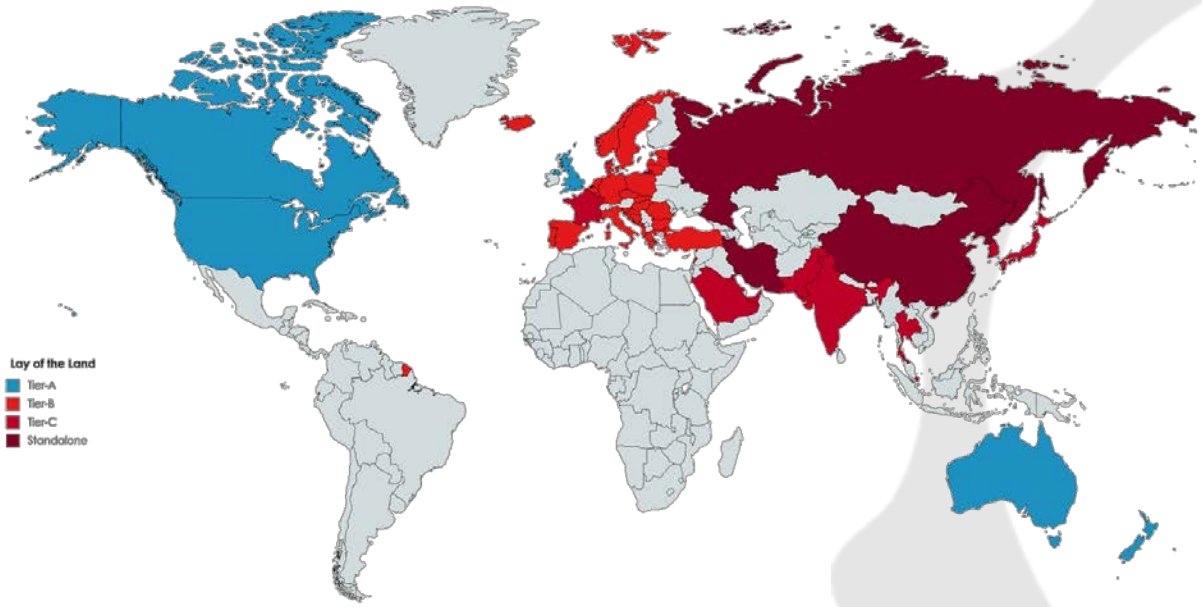


Image 1 – Alliance Members and Standalone Countries

Standalone Countries[2]:

- Russia
- China
- Iran

Covering the breadth and depth of surveillance activities goes beyond the scope of our analysis; regional operational centers, ocean cable taps, and satellite monitoring activities are just some examples of ways nation states gain unrestricted access to global information. Electrospaces.net illustrates the vastness of this information collection here, with a view from a reconstructed Global Interception Map:

[2] Only reflects the major players of concern…

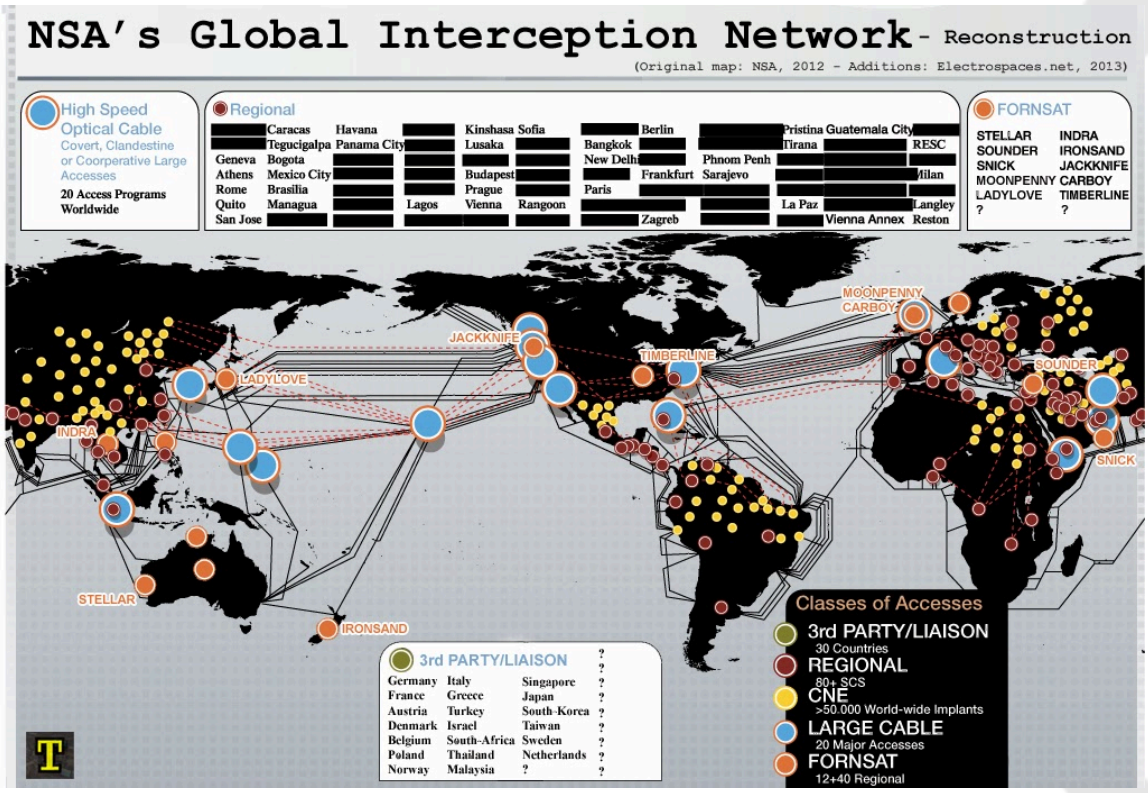


Image 2 - Reconstruction of the NSA global interception network map[3]

5-EYES Countries

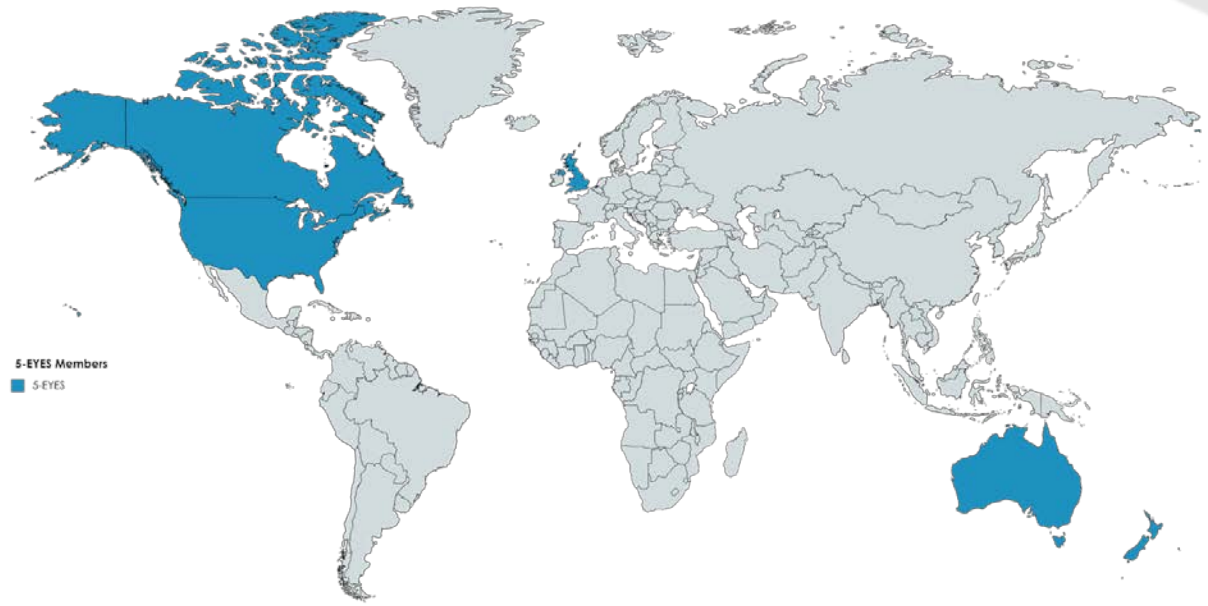


Image 3 – Five EYES Countries

[3] https://www.electrospaces.net/2013/12/nsas-global-interception-network.html

The Five Eyes (FVEY) is an Anglophone intelligence alliance comprising Australia, Canada, New Zealand, the United Kingdom and the United States. These countries are parties to the multilateral UKUSA Agreement, a treaty for joint cooperation in signals intelligence. [Source: Wikipedia]

Members of 5-EYES and their breakdown:

Member Country	CC	Membership	Ranking
United States	US	FVEY	1
Canada	CA	FVEY	6
United Kingdom	GB	FVEY	9
Australia	AU	FVEY	26
New Zealand	NZ	FVEY	66

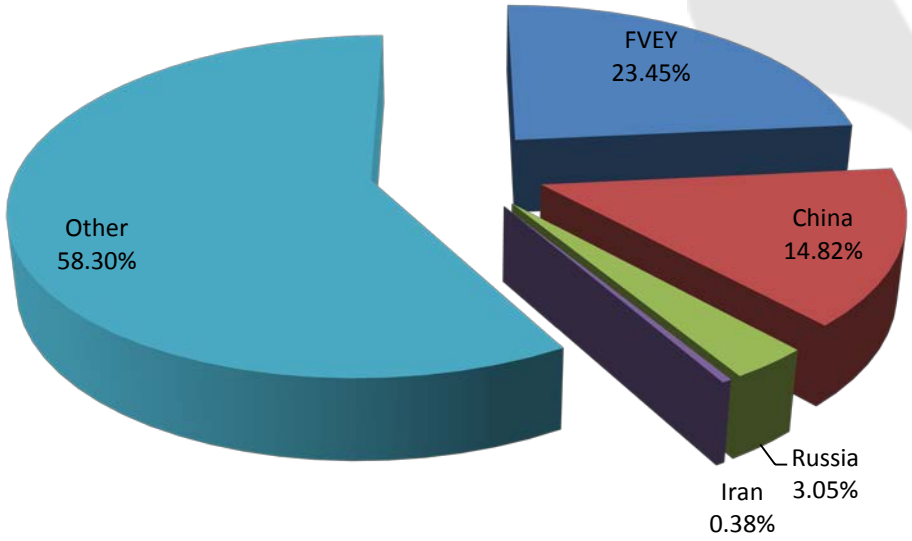


Chart 8 – 5-EYES versus China, Russia and Iran

9-EYES Countries

This is a European centric extension of 5-EYES, which adds Denmark, France, the Netherlands and Norway.

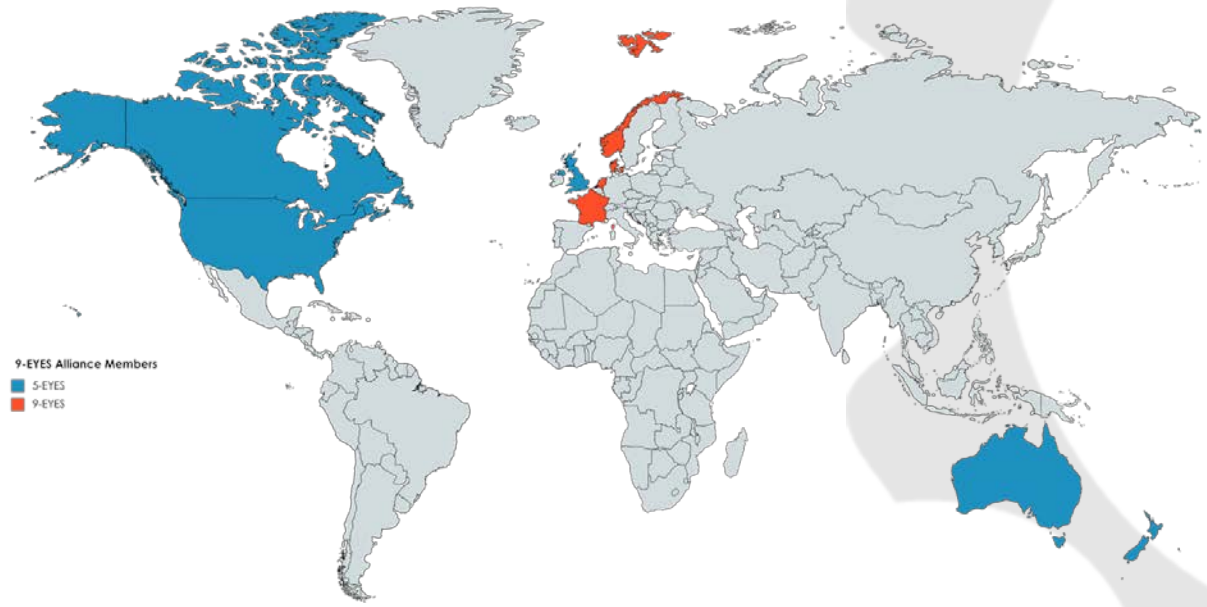


Image 4 – 9-EYES Countries

Members of 9-EYES and their breakdown:

Member Country	CC	Membership	Ranking
United States	US	9-EYES	1
France	FR	9-EYES	3
Canada	CA	9-EYES	6
United Kingdom	GB	9-EYES	9
Netherlands	NL	9-EYES	13
Australia	AU	9-EYES	26
Norway	NO	9-EYES	49
Denmark	DK	9-EYES	54
New Zealand	NZ	FVEY	66

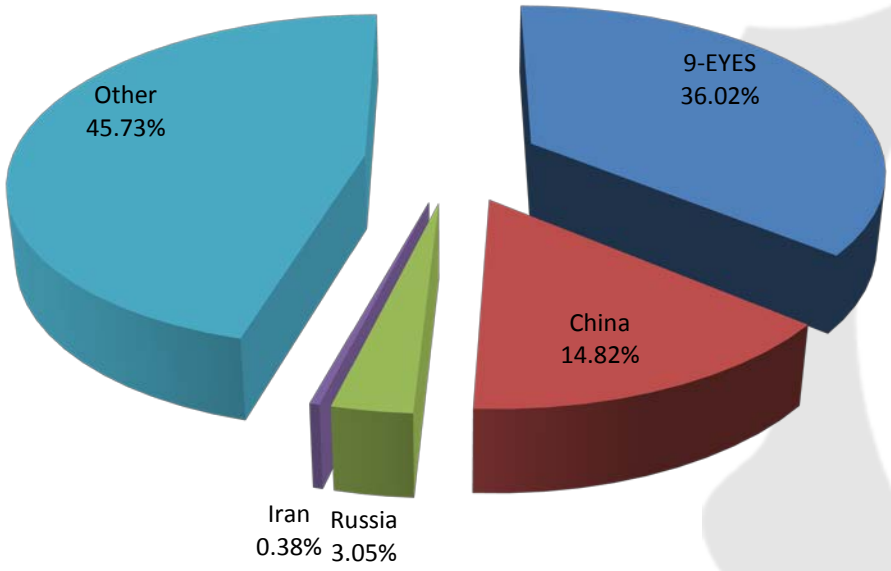


Chart 9 – 9-EYES versus China, Russia and Iran

10-EYES Countries

10-EYES is focused on the Asia Pacific and it includes 5-EYES countries plus Singapore, South Korea and most likely India and Thailand; also known as SIGINT Seniors Pacific (SSPAC).

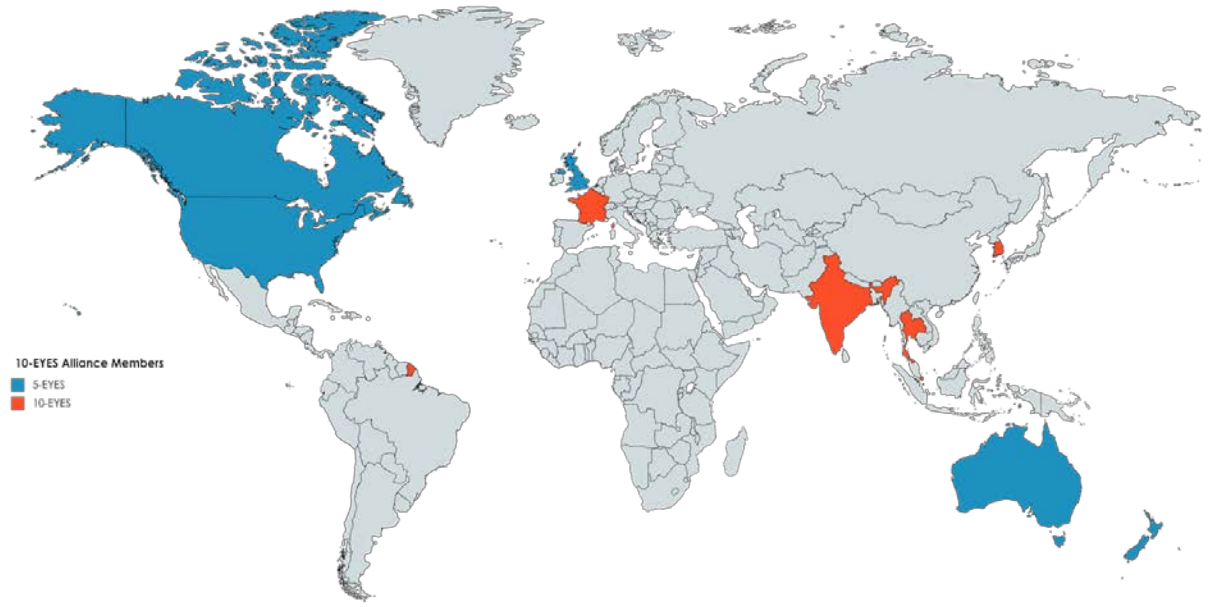


Image 5 – 10-EYES Countries

Members of 10-EYES and their breakdown:

Member Country	CC	Membership	Ranking
United States	US	10-EYES	1
France	FR	10-EYES	3
India	IN	10-EYES	4
Canada	CA	10-EYES	6
South Korea	KR	10-EYES	8
United Kingdom	GB	10-EYES	9
Singapore	SG	10-EYES	11
Thailand	HK	10-EYES	19
Australia	AU	10-EYES	26
New Zealand	NZ	10-EYES	66

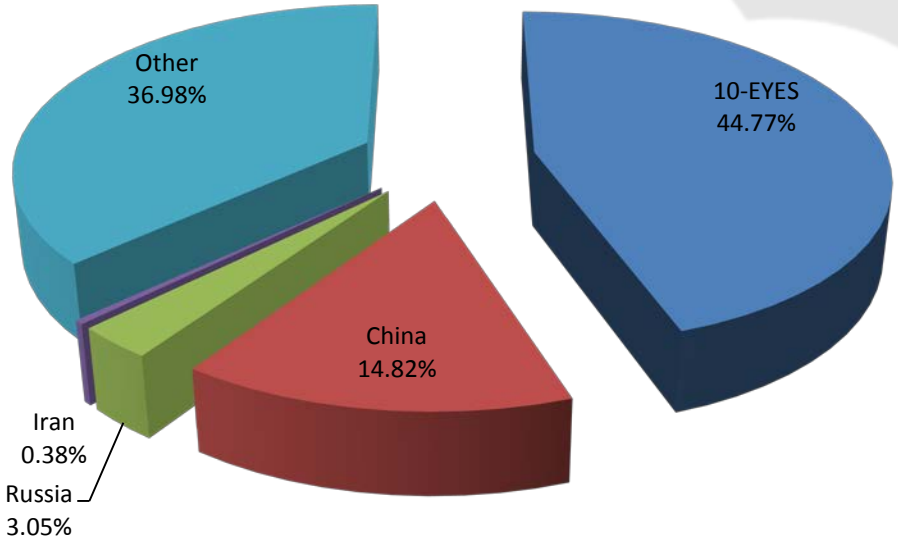


Chart 10 – 10-EYES versus China, Russia and Iran

14-EYES Countries

14-EYES is an extension of 9-EYES countries and includes Germany, Belgium, Italy, Sweden, Spain; this group is also European centric and also known as SIGINT Seniors Europe (SSEUR).

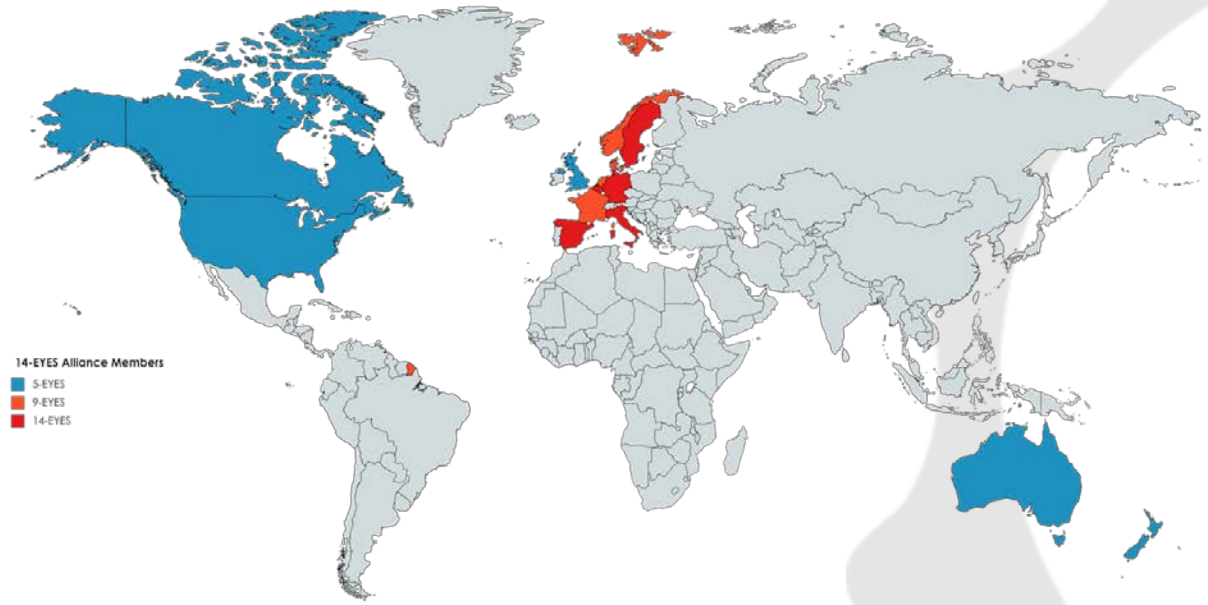


Image 6 – 14-EYES Countries

Members of 14-EYES and their breakdown:

Member Country	CC	Membership	Ranking
United States	US	14-EYES	1
France	FR	14-EYES	3
Canada	CA	14-EYES	6
Germany	DE	14-EYES	7
United Kingdom	GB	14-EYES	9
Netherlands	NL	14-EYES	13
Italy	IT	14-EYES	14
Spain	ES	14-EYES	23
Australia	AU	14-EYES	26
Sweden	SE	14-EYES	30
Belgium	BE	14-EYES	37
Norway	NO	14-EYES	49
Denmark	DK	14-EYES	54
New Zealand	NZ	14-EYES	66

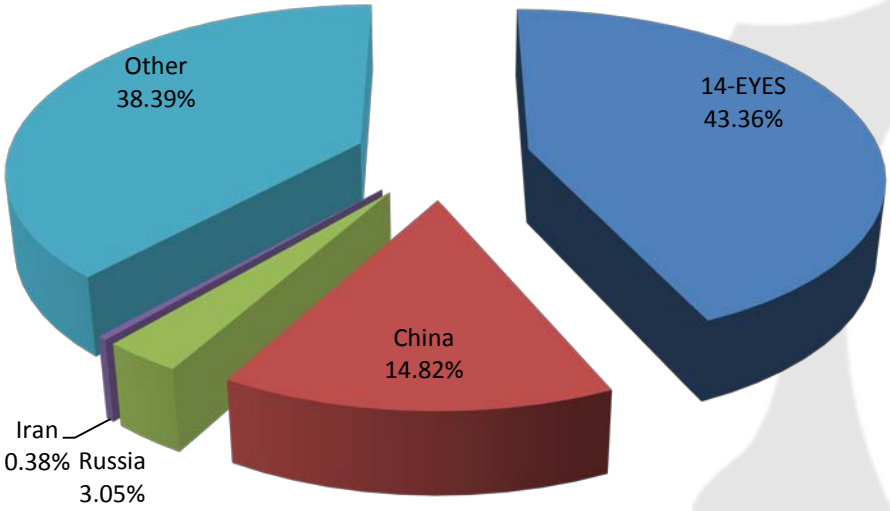
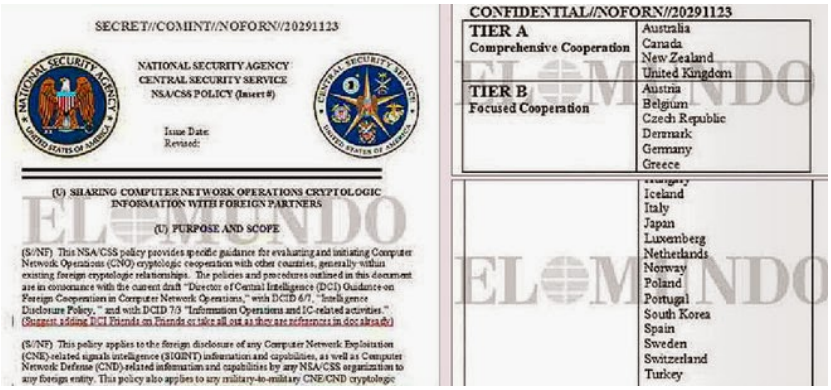


Chart 11 – 14-EYES versus China, Russia and Iran

Computer Network Operation (CNO) Countries

CNO countries also bear examining as they represent another category of partnership on the surveillance continuum. On October 30, the Spanish newspaper El Mundo[4] published an undated document showing cooperation with various countries on four different levels.



SECRET//COMINT//NOFORN//20291123

NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
NSA/CSS POLICY (Insert #)

Issue Date:
Revised:

(U) SHARING COMPUTER NETWORK OPERATIONS CRYPTOLOGIC INFORMATION WITH FOREIGN PARTNERS

(U) PURPOSE AND SCOPE

(S//NF) This NSA/CSS policy provides specific guidance for evaluating and initiating Computer Network Operations (CNO) cryptologic cooperation with other countries, generally within existing foreign cryptologic relationships. The policies and procedures outlined in this document are in concordance with the current draft "Director of Central Intelligence (DCI) Guidance on Foreign Cooperation in Computer Network Operations," with DCID 6/7, "Intelligence Disclosure Policy," and with DCID 7/3 "Information Operations and IC-related activities."
(Suggest adding DCI Friends on Friends or take all out as they are references in doc already)

(S//NF) This policy applies to the foreign disclosure of any Computer Network Exploitation (CNE)-related signals intelligence (SIGINT) information and capabilities, as well as Computer Network Defense (CND)-related information and capabilities by any NSA/CSS organization to any foreign entity. This policy also applies to any military-to-military CNE/CND cryptologic

CONFIDENTIAL//NOFORN//20291123

TIER A Comprehensive Cooperation	Australia Canada New Zealand United Kingdom
TIER B Focused Cooperation	Austria Belgium Czech Republic Denmark Germany Greece
	Iceland Italy Japan Luxemberg Netherlands Norway Poland Portugal South Korea Spain Sweden Switzerland Turkey

Image 7 – Document Published by El Mundo

[4] El CNI facilitó el espionaje masivo de EEUU a España - https://www.elmundo.es/espana/2013/10/30/5270985d63fd3d7d778b4576.html

According to El Mundo, NSA documents explain the "specific guidance for evaluating and initiating Computer Network Operations (CNO) cryptologic cooperation with other countries, generally within existing foreign cryptologic relationships". This covers all telephonic and electronic surveillance operations, and indicates that the results would be shared with allied countries. The documents suggest that the Spanish intelligence services are working hand in hand with the NSA, as are other foreign agencies. And if there was any doubt about who holds the upper hand, the NSA documents make clear that any collaboration was always to serve the needs of protecting American interests.

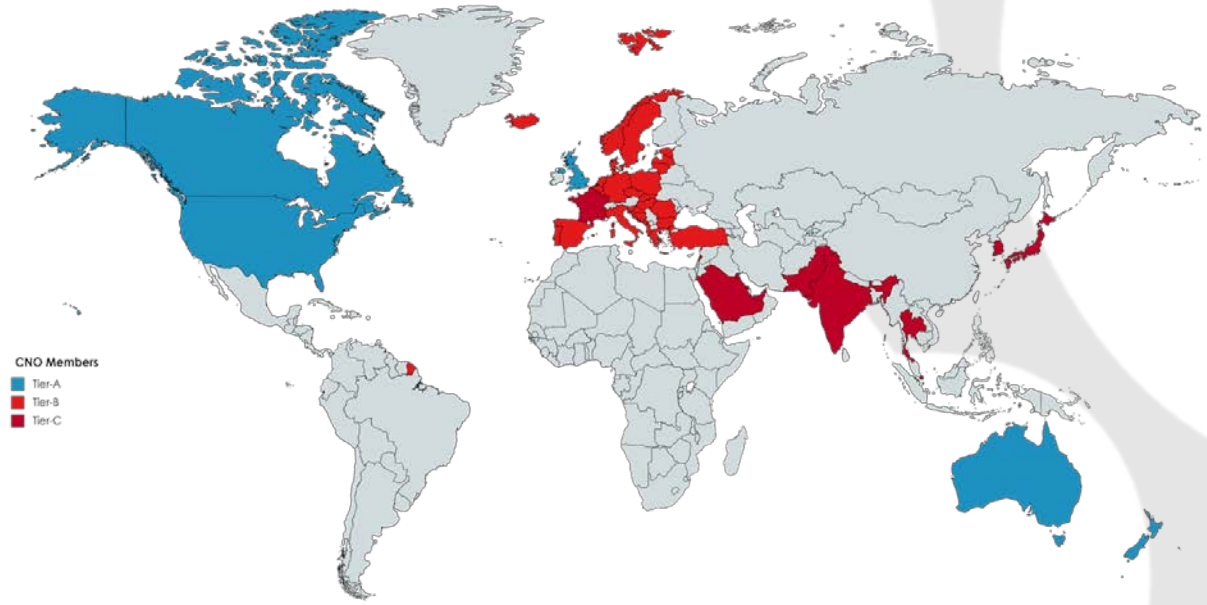


Image 8 – CNO Countries

There are multiples levels in CNO cooperation[5]:

- Tier-A - Comprehensive Cooperation – Includes Five Eyes
- Tier-B - Focused Cooperation - Mostly European CNO countries listed below a.k.a Third Party
- Tier-C – Limited Cooperation - consists of countries such as France, Israel, India and Pakistan (there are potentially others)
- Tier-D – Exceptional Cooperation - countries that the US considers to be hostile to its interests.

Disclaimer: The full list is not known and the data constructed here is gathered based on documents leaked in the public domain; some of the entities that are marked as standalone nation states in our

[5] In May 2014, the list with the "Tier A" and "Tier B" countries was also published in Greenwald's book *No Place To Hide*, where he ignores the fact that the document was about CNO cooperation and simply assumes that the "Tier B" countries are the same as those with 3rd Party status.*

study (other than the obvious ones; Russia, China, Iran, Republic of North Korea) may indeed be part of a CNO partnership or a 3rd Party Agreement.

Tier-A CNO members and their attack breakdown:

Member Country	CC	Membership	Ranking
Germany	DE	CNO	7
Republic of Korea	KR	CNO	8
Netherlands	NL	CNO	13
Italy	IT	CNO	14
Poland	PL	CNO	16
Spain	ES	CNO	23
Japan	JP	CNO	25
Hungary	HU	CNO	28
Sweden	SE	CNO	30
Greece	GR	CNO	34
Belgium	BE	CNO	37
Austria	AT	CNO	39
Czechia	CZ	CNO	41
Switzerland	CH	CNO	44
Norway	NO	CNO	49
Denmark	DK	CNO	54
Turkey	TR	CNO	55
Luxembourg	LU	CNO	68
Iceland	IS	CNO	70
Bosnia and Herzegovina	BA	CNO	116

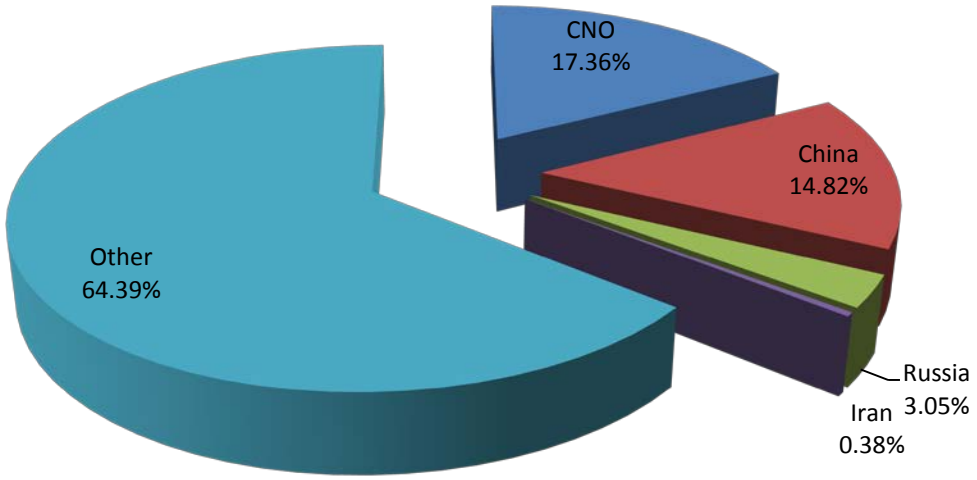


Chart 12 – CNO versus China, Russia and Iran

NATO Countries

The North Atlantic Treaty Organization (NATO) consists of 29 member states – members of NATO are typically involved as a partner in NSA's Worldwide SIGINT/Defense Cryptologic Platform.

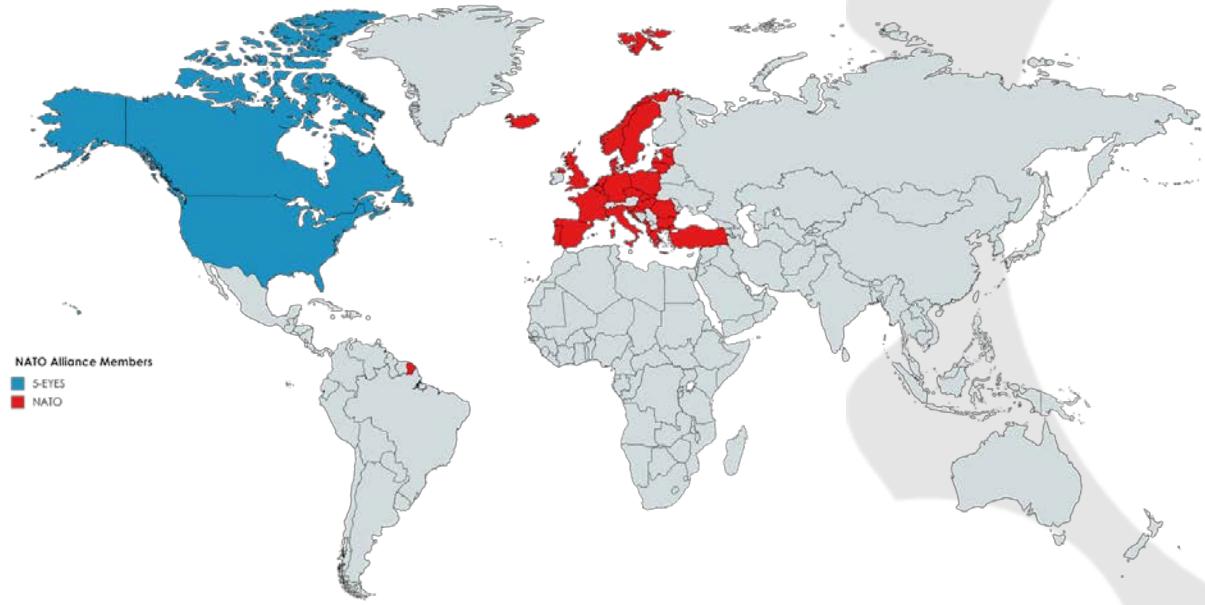


Image 9 – NATO Countries

Members of NATO and their attack breakdown:

Member Country	CC	Membership	Ranking
United States	US	NATO	1
France	FR	NATO	3
Canada	CA	NATO	6
Germany	DE	NATO	14
United Kingdom	GB	NATO	9
Netherlands	NL	NATO	13
Italy	IT	NATO	14
Poland	PL	NATO	16
Spain	ES	NATO	23
Hungary	HU	NATO	28
Greece	GR	NATO	34
Romania	RO	NATO	36
Belgium	BE	NATO	37
Czechia	CZ	NATO	40
Bulgaria	BG	NATO	43

Norway	NO	NATO	49
Denmark	DK	NATO	54
Turkey	TR	NATO	55
Portugal	PT	NATO	59
Latvia	LV	NATO	64
Luxembourg	LU	NATO	68
Iceland	IS	NATO	70
Slovakia	SK	NATO	78
Croatia	HR	NATO	80

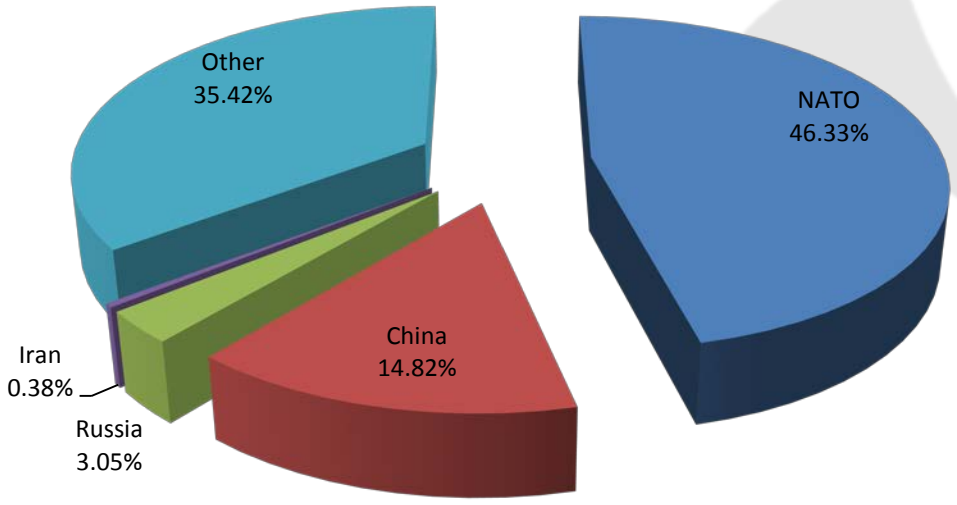


Chart 13 – NATO versus China, Russia and Iran

Conclusion

Nation state surveillance and signals intelligence (SIGINT) operations are alive and well – the quest for information and gaining footholds for launching attacks will continue to be an on-going effort.

Compared to all the attacks coming from the SIGINT alliance countries, direct attacks coming from Russia and Iran are seemingly not so significant and direct attacks from North Korea are non-existent; China is still a substantial player in launching direct and indirect attacks.

What's interesting in all this is that the U.S. attacks its own computing resources more than any country in the World.

So you might think what can I do with a report like this? Well, first and foremost it is awareness of your operating environment. Second, understand geo-intellectual-property risks to your business. Whether you are in friendly or in an unfriendly territory you are subject to monitoring. Based on the evidence this monitoring goes beyond the needs for national security, but also acts as a means for industrial espionage.

In a statement issued, the US director of national intelligence, James Clapper, said: "It is not a secret that the intelligence community collects information about economic and financial matters, and terrorist financing.

We collect this information for many important reasons: for one, it could provide the United States and our allies early warning of international financial crises which could negatively impact the global economy. It also could provide insight into other countries' economic policy or behavior which could affect global markets."[6]

As a business if you want to protect your financial viability, intellectual property and your customer privacy it's time to deepen your defense strategy, protect your assets, and mature your information security program.

Perimeter defense is a great start; however, you may be blocking the countries you are not doing business with, but what if the country you are in is the country is initiating the most attacks?

You need more than just a perimeter - you need defense in-depth[7]. Here are DerivativeTech's recommendations on how to establish a defense in depth baseline:

1. **Understand your attack surface and minimize it** – routine checks of the perimeter are needed, so that the attack surface is properly understood. What is needed for operations vs. what is not needs to be properly documented and monitored.

2. **Detect incoming threats** – this could be something as simple as Fail2Ban or a sophisticated deep packet inspection firewall; it depends on your budget and operational needs, but in this day and age you need to know who is at your door.

3. **Alerting mechanism** – you may be detecting incoming threats, but if you are not alerted it may not be worth it; granted the volume of attacks can be overwhelming and this takes us to the next one,

[6] NSA accused of spying on Brazilian oil company Petrobras - https://www.theguardian.com/world/2013/sep/09/nsa-spying-brazil-oil-petrobras

[7] Depending on the size of the organization a proper incident response policy, playbooks and team should be established. This describes the outline for handling routine network based incidents.

4. **Automated response** – setting thresholds on the incoming attacks and responding automatically is the ultimate way to handle these attacks; for example creating tickets for potential incidents, blocking the attacking IP addresses for a period of time or indefinitely, attacking back to the attacker. Attacking back to the attacker is not always the best response due to cumbersome attribution process – avoid this unless you're confident in your attribution. Simple open source tools and Python are your best friends.

References

1. **Five Eyes, 9-Eyes and many more -** https://www.electrospaces.net/2013/11/five-eyes-9-eyes-and-many-more.html
2. **14-Eyes are 3rd Party partners forming the SIGINT Seniors Europe -** https://www.electrospaces.net/2013/12/14-eyes-are-3rd-party-partners-forming.html
3. **NSA's Foreign Partnerships -** https://www.electrospaces.net/2014/09/nsas-foreign-partnerships.html
4. **Canada and the Five Eyes Intelligence Community -** http://web.archive.org/web/20140319230059/http://www.cdfai.org/PDF/Canada%20and%20the%20Five%20Eyes%20Intelligence%20Community.pdf
5. **NSA's global interception network** - https://austinangck2809.blogspot.com/2013/12/nsa-global-interception-network.html
6. **El CNI facilitó el espionaje masivo de EEUU a España** - https://www.elmundo.es/espana/2013/10/30/5270985d63fd3d7d778b4576.html
7. **Paper 1: Echelon and its role in COMINT** - https://www.heise.de/tp/features/Paper-1-Echelon-and-its-role-in-COMINT-3449041.html
8. **No Place to Hide (Glenn Greenwald)** - https://en.wikipedia.org/wiki/No_Place_to_Hide_%28Greenwald_book%29
9. **ECHELON** - http://web.archive.org/web/20160312133841/http://www.billhance.com/USA/echelon.htm
10. **Embassy Spy Network** - https://www.duncancampbell.org/content/embassy-spy-centre-network

Appendix I – Top 10 Attacking Autonomous System Numbers

What is ASN? An autonomous system number is a unique identifier that is globally available and allows its autonomous system to exchange routing information with other systems[8].

Country	Country Code	Organization	ASN
United States	US	DIGITALOCEAN-ASN - DigitalOcean	AS14061
France	FR	OVH S.A.S	AS16276
China	CN	CNNIC-TENCENT-NET-AP Shenzhen Tencent Computer Systems Company Limited	AS45090
China	CN	CHINANET-BACKBONE No.31	AS4134
Republic of Korea	KR	KIXS-AS-KR Korea Telecom	AS4766
United States	US	MICROSOFT-CORP-MSN-AS-BLOCK - Microsoft Corporation	AS8075
France	FR	Online S.A.S	AS12876
United States	US	COMCAST-7922 - Comcast Cable Communications	AS7922
China	CN	CHINA169-BACKBONE CNCGROUP China169 Backbone	AS4837
China	CN	CNNIC-BAIDU-AP Beijing Baidu Netcom Science and Technology Co.	AS38365

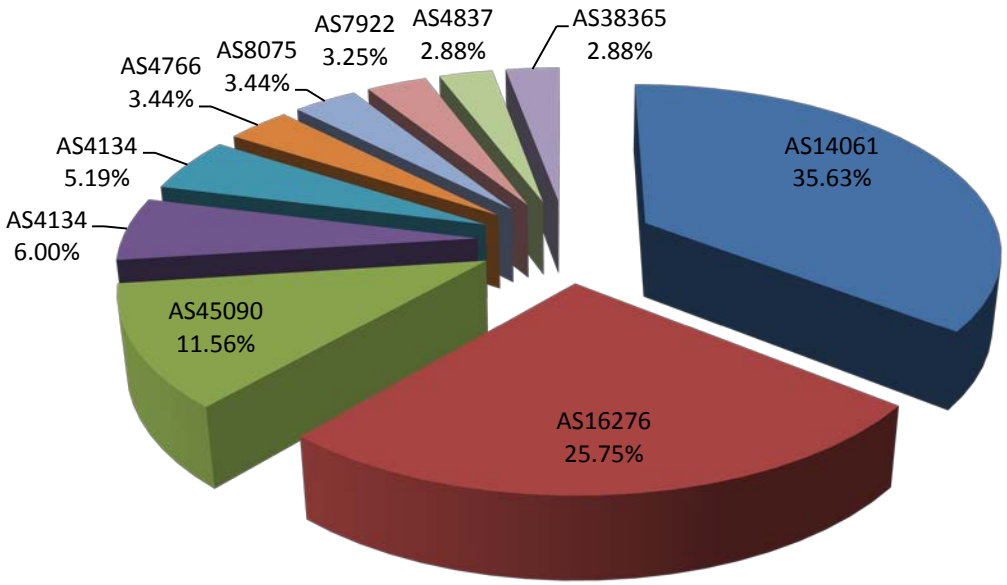


Chart 14 – Top 10 Attacking Autonomous Service Numbers

[8] ASN - https://en.wikipedia.org/wiki/Autonomous_System_Number

Looking at the list of organizations with the attacking ASN(s); 3 names jump out based on their geo-diversity:

1. **DIGITALOCEAN-ASN – DigitalOcean**
   U.S. based internet and cloud service provider also it hosts VPN service providers; verified VPN endpoints engaged in attacks. Looking at the global breakdown of Digital Ocean's attacking IPs, they are quite diverse:

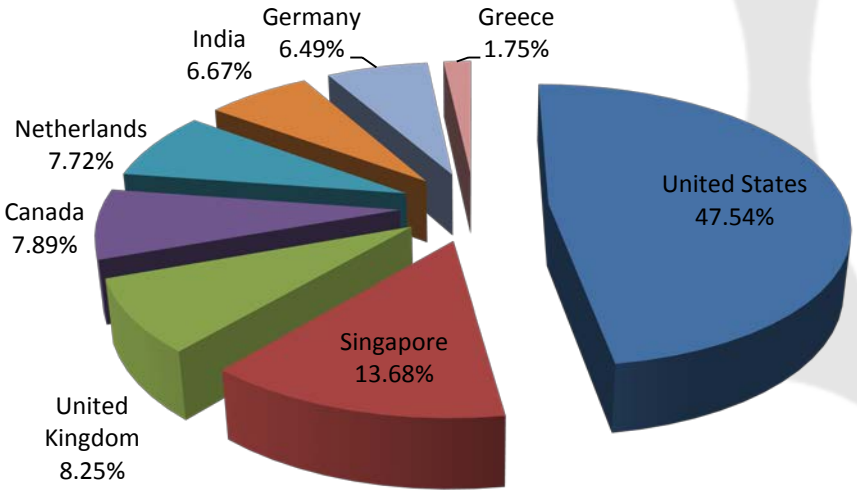


Chart 15 – AS14061 DIGITALOCEAN-ASN – DigitalOcean based Attacks Global Breakdown

Attacking countries and their alliance memberships:

Country	CC	Membership	Ranking
United States	US	FVEY, 9-EYES, 10-EYES, 14-EYES, 3rd Party, NATO	1
Singapore	SG	10-EYES, 3rd Party	2
United Kingdom	GB	FVEY, 9-EYES, 10-EYES, 14-EYES, 3rd Party, NATO	3
Canada	CA	FVEY, 9-EYES, 10-EYES, 14-EYES, 3rd Party, NATO	4
Netherlands	NL	9-EYES, 14-EYES, CNO, 3rd Party, NATO	5
India	IN	10-EYES	6
Germany	DE	14-EYES, CNO, 3rd Party, NATO	7
Greece	GR	CNO, 3rd Party, NATO	8

2. **OVH S.A.S**
   France based internet and cloud service provider also hosts VPN service providers; verified VPN endpoints engaged in attacks. Looking at the global breakdown of OVH S.A.S's attacking IPs display more geo-diversity than DigitalOcean's:

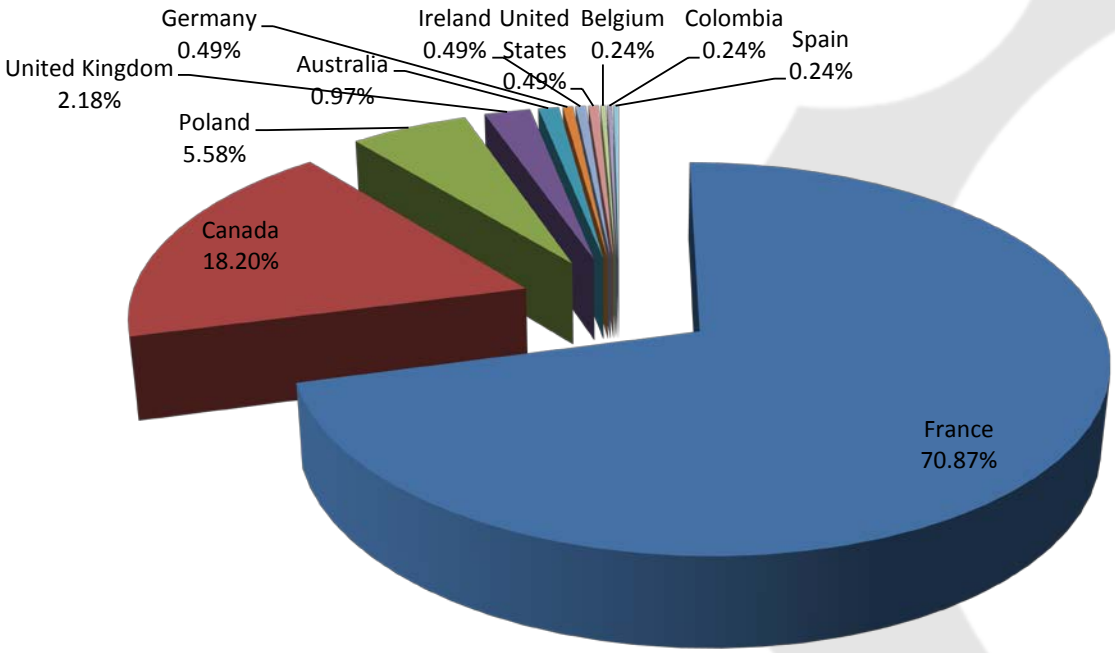


Chart 16 – AS16276 OVH S.A.S based Attacks Global Breakdown

Attacking countries and their alliance memberships:

Country	CC	Membership	Ranking
France	FR	9-EYES, 10-EYES, 14-EYES, 3rd Party, NATO	1
Canada	CA	FVEY, 9-EYES, 10-EYES, 14-EYES, 3rd Party, NATO	2
Poland	PL	CNO, 3rd Party	3
United Kingdom	GB	FVEY, 9-EYES, 10-EYES, 14-EYES, 3rd Party, NATO	4
Australia	AU	FVEY, 9-EYES, 10-EYES, 14-EYES	5
Germany	DE	14-EYES, CNO, 3rd Party, NATO	6
Ireland	IE	Standalone	7
United States	US	FVEY, 9-EYES, 10-EYES, 14-EYES, 3rd Party, NATO	8
Belgium	BE	14-EYES, CNO, 3rd Party, NATO	9
Colombia	CO	Standalone	10
Spain	ES	14-EYES, CNO, 3rd Party, NATO	11

3. Microsoft Corporation

Microsoft is one of the top 3 cloud vendors with Microsoft Azure – based on our scans these hosts are not VPN endpoints, but rather client machines that are attacking systems.

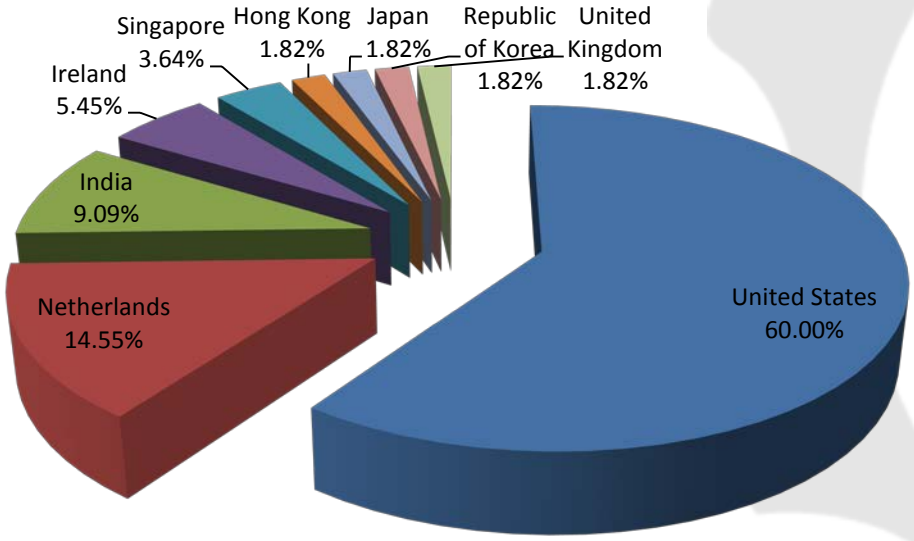


Chart 17 – AS8075 Microsoft Corporation based Attacks Global Breakdown

Attacking countries and their alliance memberships:

Country	CC	Membership	Ranking
United States	US	FVEY, 9-EYES, 10-EYES, 14-EYES, 3rd Party, NATO	1
Netherlands	NL	9-EYES, 14-EYES, CNO, 3rd Party, NATO	2
India	IN	10-EYES	3
Ireland	IE	Standalone	4
Singapore	SG	10-EYES, 3rd Party	5
Hong Kong	HK	Standalone (Potential CNO)	6
Japan	JP	CNO, 3rd Party	7
Republic of Korea	KR	10-EYES, CNO, 3rd Party	8
United Kingdom	GB	FVEY, 9-EYES, 10-EYES, 14-EYES, 3rd Party, NATO	9

Other ASN(s) mainly chose to attack from their own operating countries namely, China and Korea. One other interesting entity is Amazon Inc…

Amazon Web Services (AWS)

Amazon is the leading cloud infrastructure service provider and has a massive global footprint. Corporations as well as governments heavily utilize it for various purposes. Below reflects the geo-

diversity of AWS infrastructure – using AWS one can initiate an ephemeral virtual machine and surface anywhere; this is also true for other cloud service providers…

The beauty is unlike TOR attribution is relatively easier; AWS will still not disclose the name of the attacker to you, but they will notify them and take other actions if necessary.

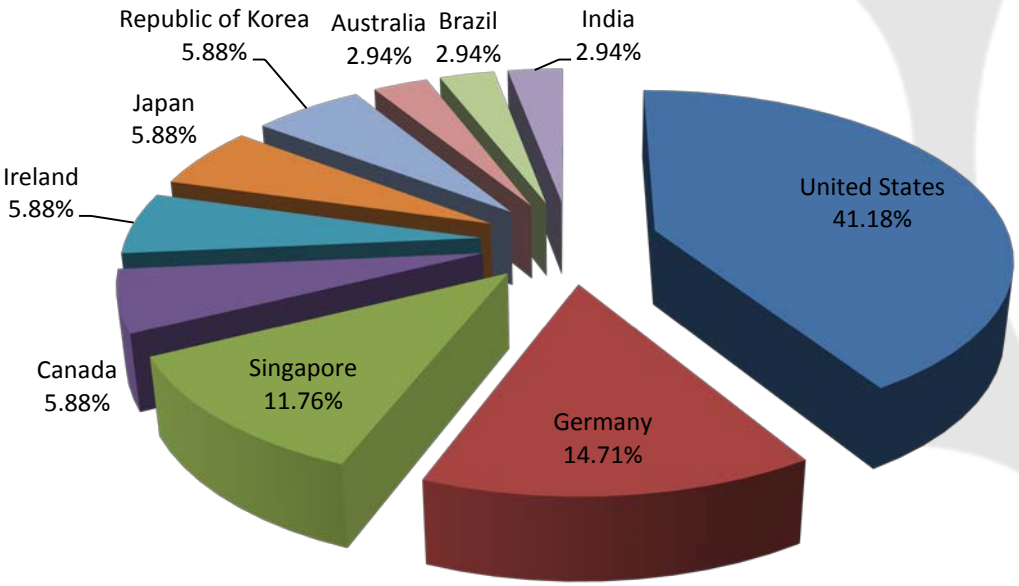


Chart 18 – AS16509, AS14618 Amazon AWS based Attacks Global Breakdown

Attacking countries and their alliance memberships:

Country	CC	Membership	Ranking
United States	US	FVEY, 9-EYES, 10-EYES, 14-EYES, 3rd Party, NATO	1
Germany	DE	14-EYES, CNO, 3rd Party, NATO	2
Singapore	SG	10-EYES, 3rd Party	3
Canada	CA	FVEY, 9-EYES, 10-EYES, 14-EYES, 3rd Party, NATO	4
Ireland	IE	Standalone	5
Netherlands	NL	9-EYES, 14-EYES, CNO, 3rd Party, NATO	6
India	IN	10-EYES	7
Ireland	IE	Standalone	8
Japan	JP	CNO, 3rd Party	9
Republic of Korea	KR	10-EYES, CNO, 3rd Party	10
Australia	AU	FVEY, 9-EYES, 10-EYES, 14-EYES	11
Brazil	BR	Standalone	12
India	IN	10-EYES	13

Appendix II – VPN vs. Direct Attacks

Approximately 30% of the attacks observed came through a VPN service.

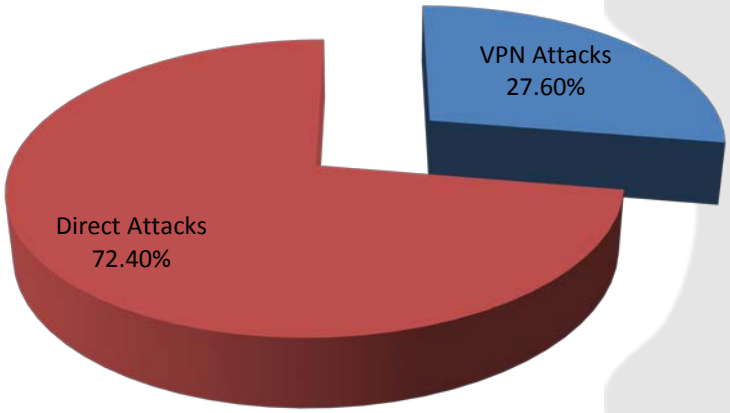


Chart 19 – VPN vs. Direct Attacks

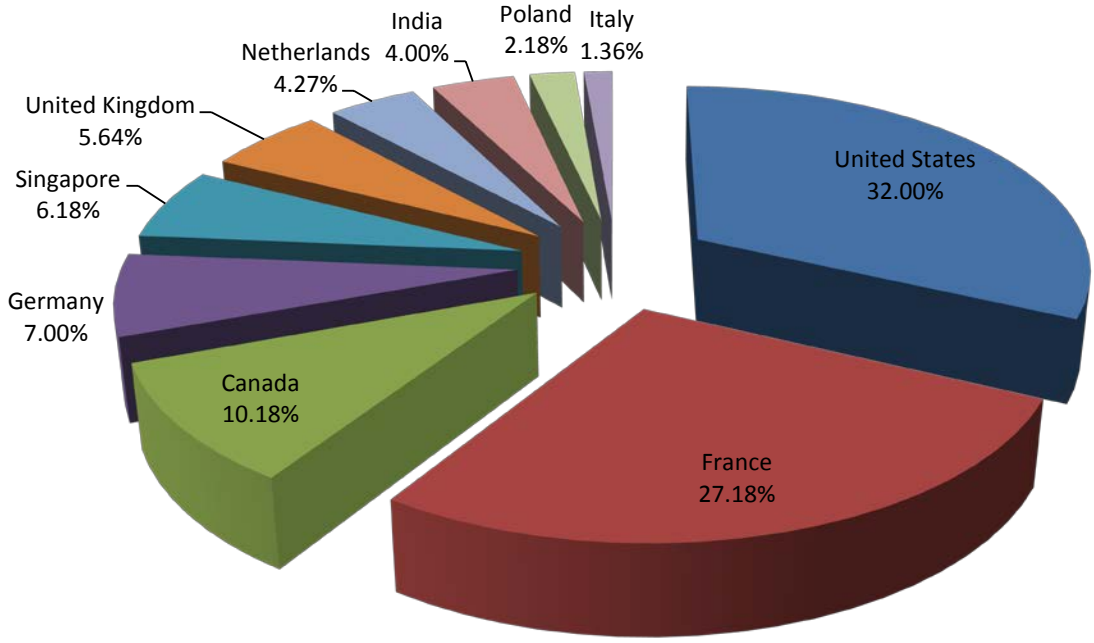


Chart 20 – Top 10 Countries Using VPN

Top 10 Countries with VPN Endpoints:

Country	CC	Membership	Ranking
United States	US	FVEY, 9-EYES, 10-EYES, 14-EYES, 3rd Party, NATO	1
France	FR	9-EYES, 10-EYES, 14-EYES, 3rd Party, NATO	2
Canada	CA	FVEY, 9-EYES, 10-EYES, 14-EYES, 3rd Party, NATO	3
Germany	DE	14-EYES, CNO, 3rd Party, NATO	4
Singapore	SG	10-EYES, 3rd Party	5
United Kingdom	GB	FVEY, 9-EYES, 10-EYES, 14-EYES, 3rd Party, NATO	6
Netherlands	NL	9-EYES, 14-EYES, CNO, 3rd Party, NATO	7
India	IN	10-EYES	8
Poland	PL	CNO, 3rd Party	9
IT	IT	14-EYES, CNO, 3rd Party, NATO	10

Appendix III – Top 10 Countries on Other Attack List(s)

The major players are the same based on other public lists, just the order is different.

Country	CC	Membership	Ranking
China	CN	Standalone	1
France	FR	9-EYES, 10-EYES, 14-EYES, 3rd Party, NATO	2
United States	US	FVEY, 9-EYES, 10-EYES, 14-EYES, 3rd Party, NATO	3
India	IN	10-EYES	4
United Kingdom	GB	FVEY, 9-EYES, 10-EYES, 14-EYES, 3rd Party, NATO	5
Republic of Korea	KR	10-EYES, CNO, 3rd Party	6
Vietnam	VN	Standalone	7
Russia	RU	Standalone	8
Brazil	BR	Standalone	9
Canada	CA	FVEY, 9-EYES, 10-EYES, 14-EYES, 3rd Party, NATO	10

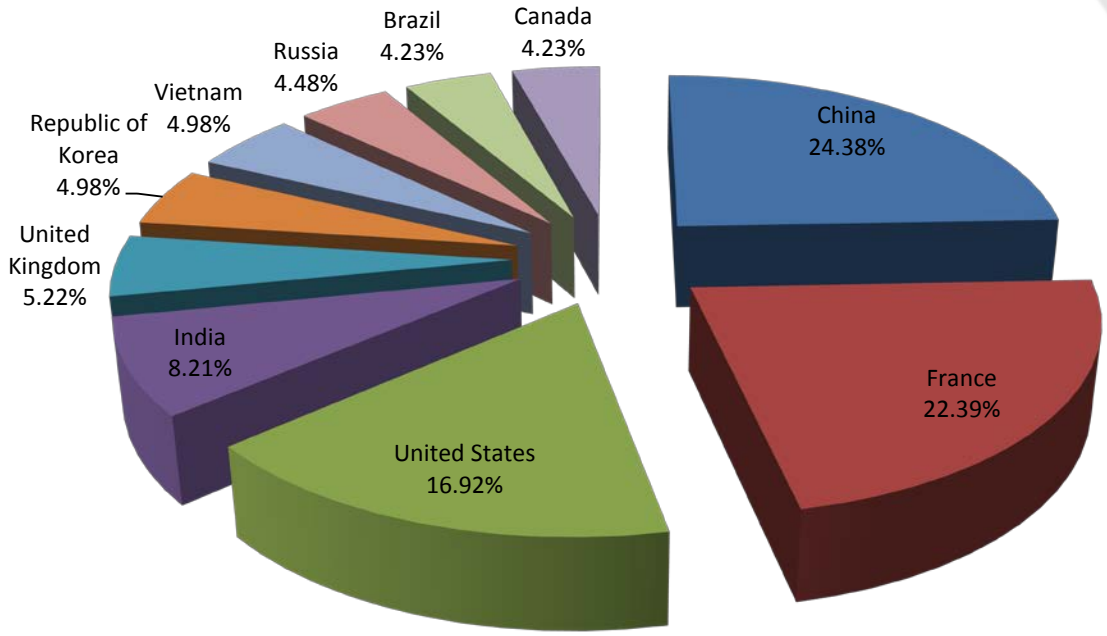


Chart 21 – Top 10 Countries on Other Attack Lists

Appendix IV – Attacks Originating from Dark Address Space

Dark address space, which is sometimes referred to as "darknet," is the area of the Internet's routable address space that's currently unused, with no active servers or services. On computer networks, darknet is the address space held in reserve for future network expansion – we especially see this used in cloud service providers to support their ephemeral services.

Often when DoS and other cyber-attacks occur, blocks of Internet address space, including darknet space, briefly appear in global routing tables and are used to launch a cyber-attack, or send spam, before being withdrawn without a trace.

In our study we observed the following countries invoked their dark address spaces.

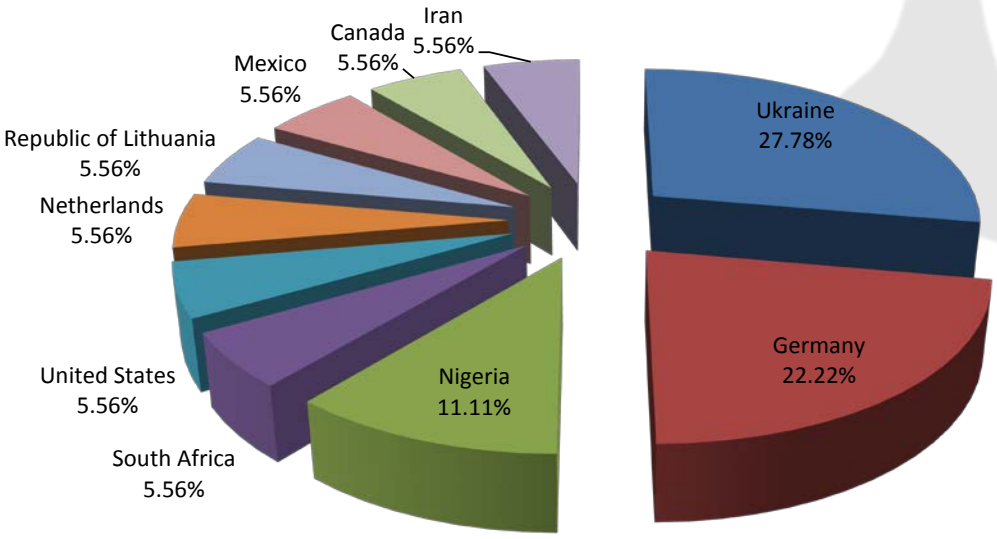


Chart 22 – Dark Address Space Attack Geo-distribution

Country breakdown:

Country	CC	Membership	Ranking
Ukraine	UA	Standalone (Potential CNO)	1
Germany	DE	14-EYES, 3rd Party, NATO	2
Nigeria	NG	Standalone	3
South Africa	ZA	Standalone	4
United States	US	FVEY, 9-EYES, 10-EYES, 14-EYES, 3rd Party, NATO	5
Netherlands	NL	9-EYES, 14-EYES, CNO, 3rd Party, NATO	6
Republic of Lithuania	LT	Standalone (Potential CNO)	7
Mexico	MX	Standalone	8
Canada	CA	FVEY, 9-EYES, 10-EYES, 14-EYES, 3rd Party, NATO	9
Iran	IR	Standalone	10

Looking at the possible associations of these “dark address space” addresses:

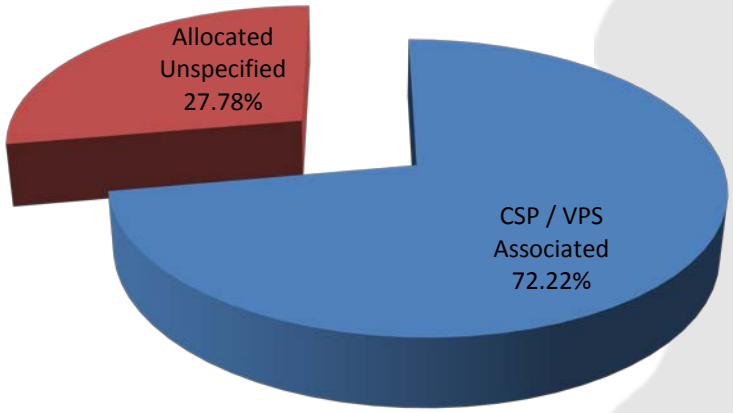


Chart 23 – Possible Dark Address Space Culprits

Appendix IV – Top Level User Names Observed

The below are the user names observed the most during attacks:

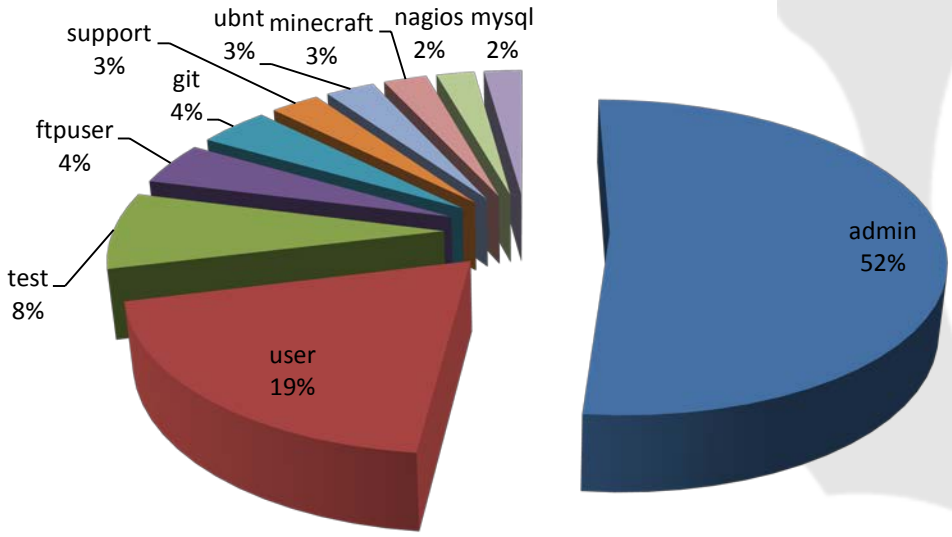


Chart 24 – Top 10 User Names Observed

Top 10 User Names Observed for the Top 10 Attackers

User name dictionaries could be an interesting component in understanding the attacker. For example some of the attacks observed originating from the U.S. were heavy in Chinese names; this could mean the following:

1. The attacking host was compromised by pro-Chinese hackers and they were too lazy to change their user name dictionary before they initiated attack.
2. It was a false flag operation by the alliance countries
3. It was targeted given that our region contains an overwhelming number of Chinese-American nationals.

Regardless of what it meant, wanted to highlight some potential reasons some of the things you may be observing in your own systems.

As a reminder here are the top 10 attacking countries:

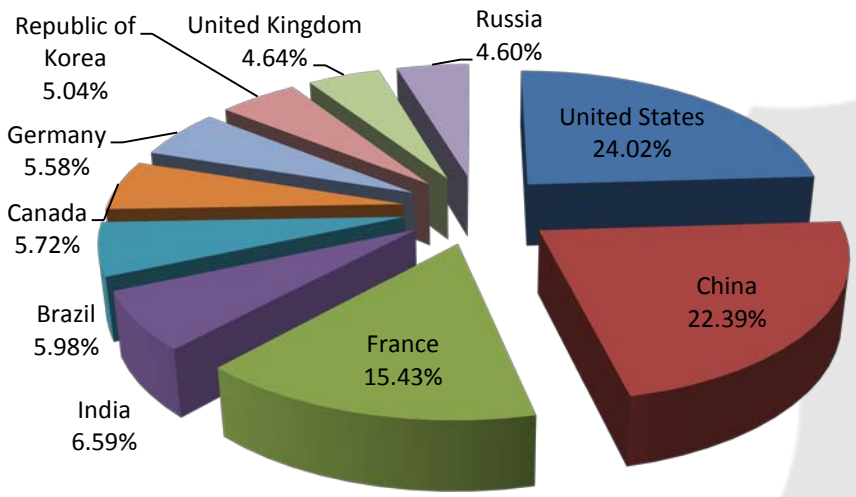


Chart 25 – Top 10 Attackers

Now let's take a look at the observed user name breakdown per attacker.

1. United States

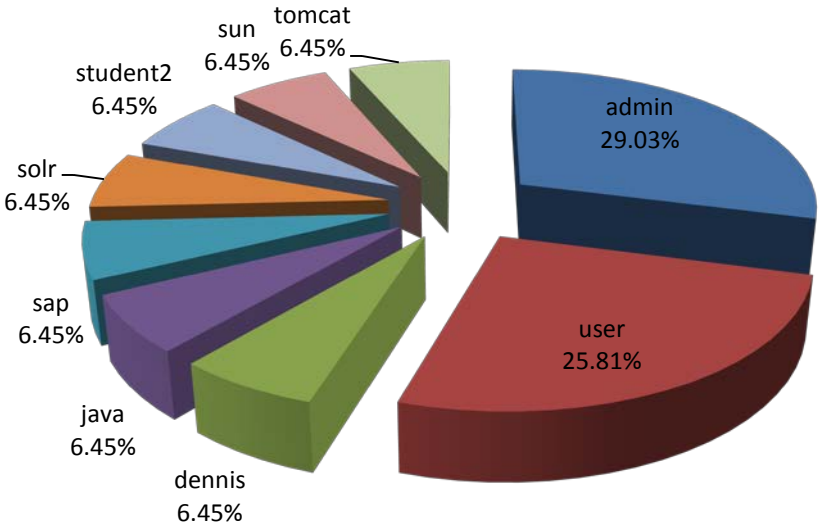


Chart 26 – User Names Observed in Attacks Originating from the United States

2. China

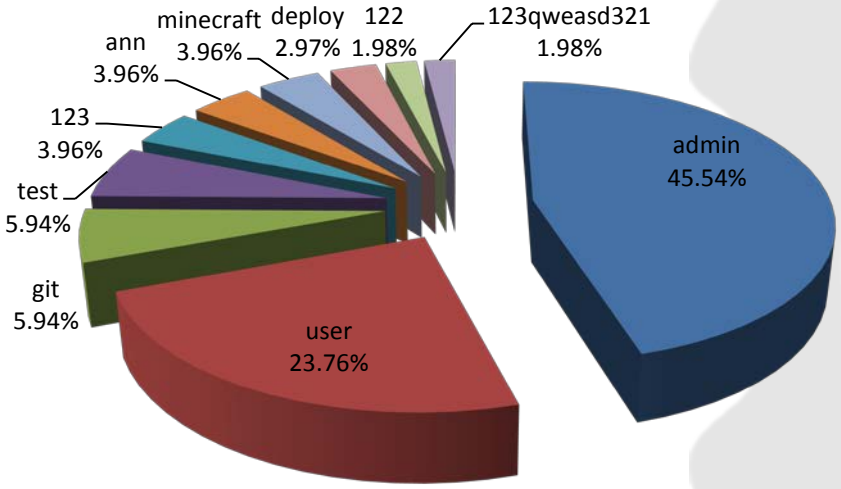


Chart 27 – User Names Observed in Attacks Originating from China

3. France

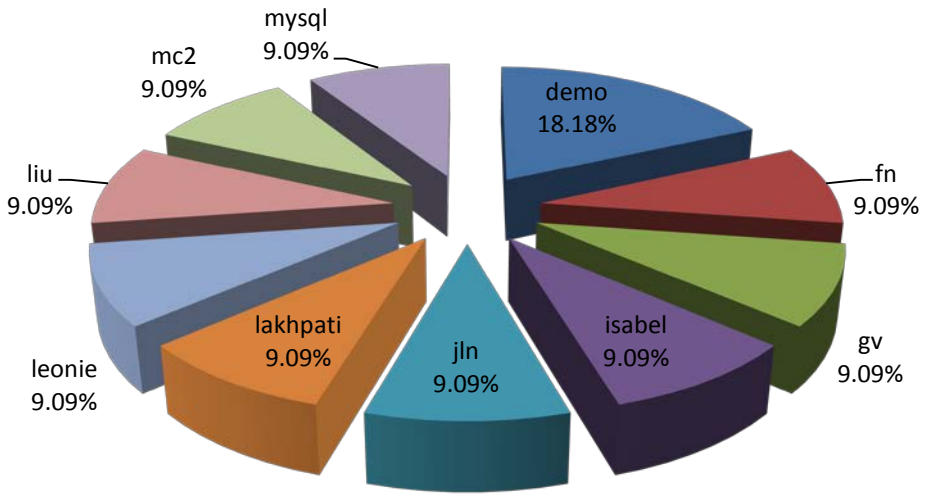


Chart 28 – User Names Observed in Attacks Originating from France

4. *India*

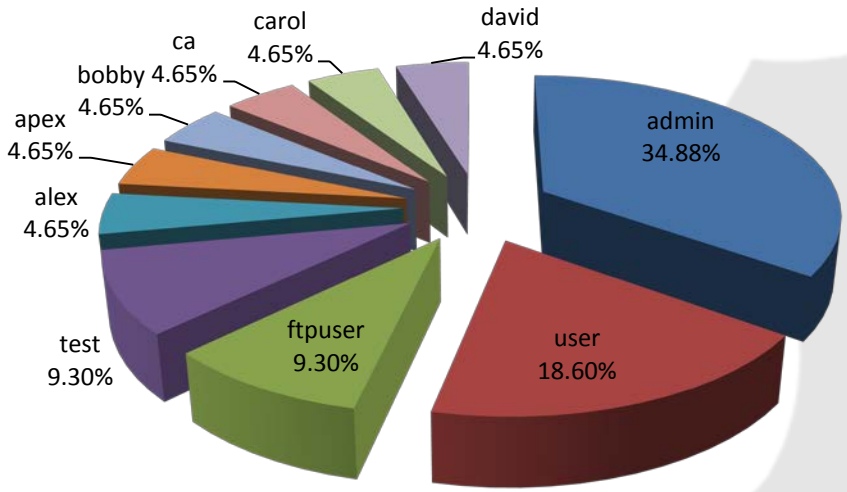


Chart 29 – User Names Observed in Attacks Originating from India

5. *Brazil*

Notice “zhangwei” is in the user name dictionary coming from Brazil…

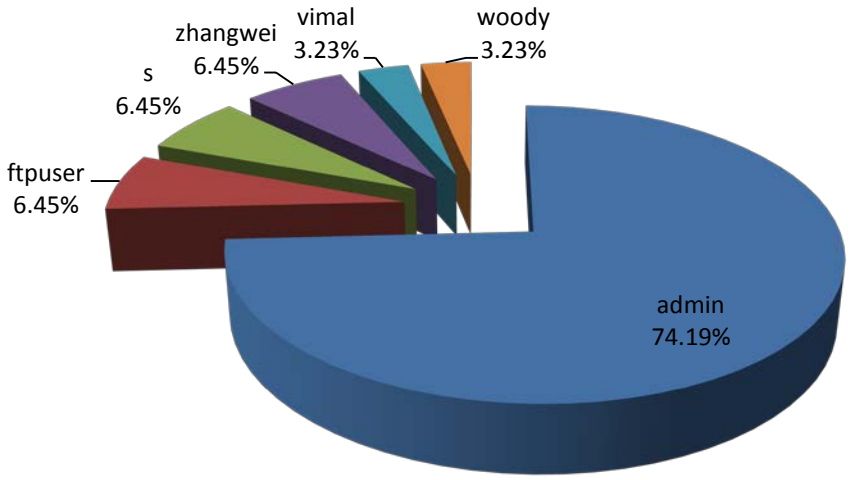


Chart 30 – User Names Observed in Attacks Originating from Brazil

6. *Canada*

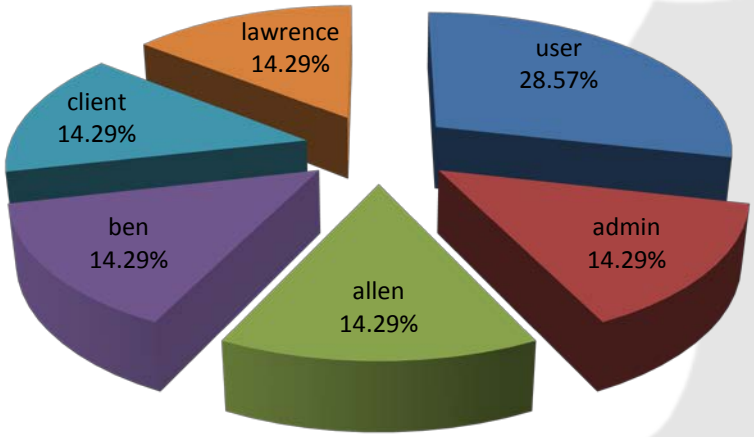


Chart 31 – User Names Observed in Attacks Originating from Canada

7. *Germany*

Notice the alphabetical order in the user name dictionary coming from Germany in the aggregate attacks… Germans are methodical as always…

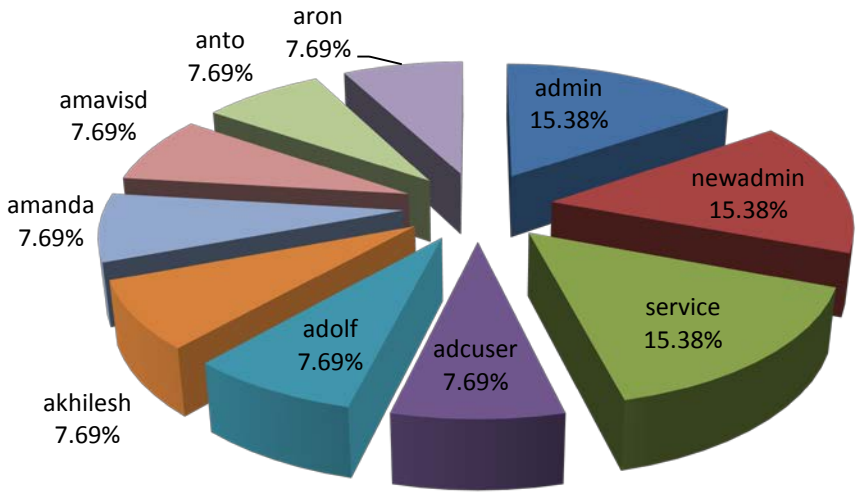


Chart 32 – User Names Observed in Attacks Originating from Germany

8. South Korea

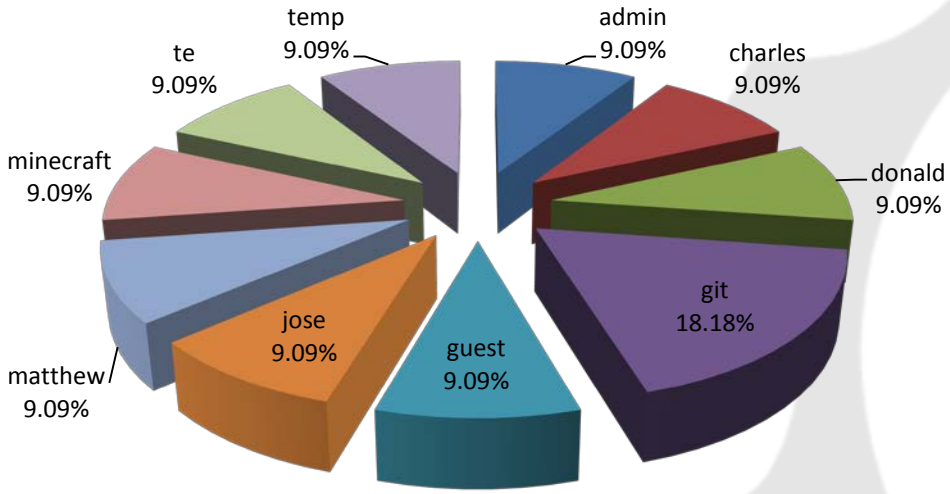


Chart 33 – User Names Observed in Attacks Originating from South Korea

9. United Kingdom

No user names were observed from United Kingdom.

10. Russia

Notice “ming” is in the user name dictionary coming from Russia…

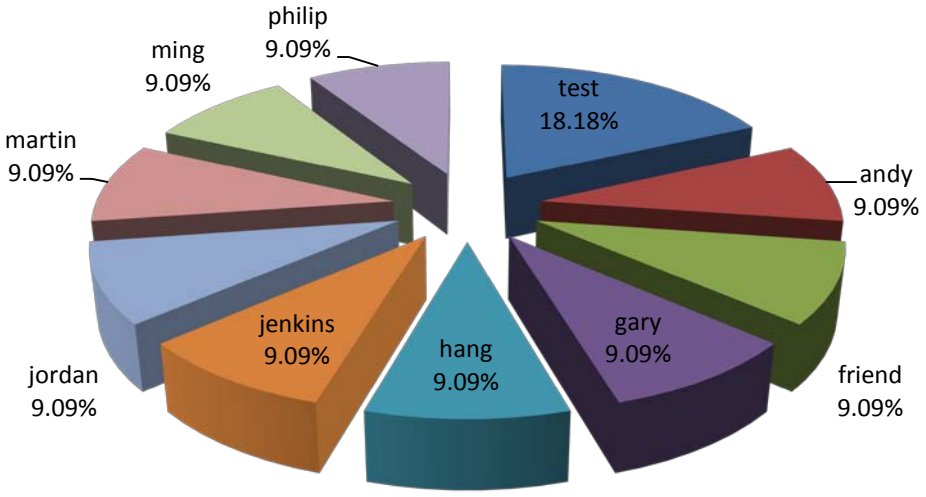


Chart 34 – User Names Observed in Attacks Originating from Russia