



Praying Medic
@prayingmedic

Thread Reader App
87 tweets - 07 Mar 2019

[prayingmedic/status/1103772362778898432](https://twitter.com/prayingmedic/status/1103772362778898432)

1) This is my Q thread for March 7, 2019

Q posts can be found here:

qmap.pub

qanon.pub

Android apps:

bit.ly/Q_Drops



Q Alerts: QAnon Drop Notifications, Research +++ - Apps on Google Play

Q Alerts notifies you when Q Anon makes new drops on 8chan. It also allows you to search, browse and research QAnon posts. As a Q follower, Patriot and software dev by trade, throughout the day I fo...

<https://bit.ly/Q-alerts>

<https://bit.ly/Q-alerts>

My theme: Facebook = Lifelog



<https://nbs.twimg.com/media/D1Ff9Q-U4AAIcxZ.jpg>

2) Q has been educating us for almost a year on the deception behind tech companies like Facebook, Google and Twitter which function as publicly acceptable front organizations for the CI_A's domestic (illegal) spying operations.

This post has been broken into 5 sections.

FB RETURNING TO THE NEWS.
LIFELOG (DARPA) ENDS > FB BEGINS
LIFELOG (DARPA) TEAM TRANSFER > FB
WHAT (DARPA) TEAM MEMBERS PAST/PRESENT WORK FOR FB?
WHAT DIVISIONS?
LOCATE (3) PUBLIC.
(9) TOTAL (6_NON PUB).
BUILDING 8 EXPOSED (HERE) WHEN?
[4-11-18]
THINK SCRAMBLE [OFFLINE SCRUB] POST XBOX/PS CHAT LOGS DROP
[MS SHUTDOWN IMMEDIATELY POST DROP]
.....

<https://pbs.twimg.com/media/D1FgYTkU4AAvCpo.png>

3) DARPA is an acronym that stands for Defence Advanced Research Projects Agency. Their mission is the development of strategic technology for the Defense Department.

Here's their website: <https://www.darpa.mil/about-us/about-darpa>



For sixty years, DARPA has held to a singular and enduring mission: to make pivotal investments in breakthrough technologies for national security.

The genesis of that mission and of DARPA itself dates to the launch of Sputnik in 1957, and a commitment by the United States that, from that time forward, it would be the initiator and not the victim of strategic technological surprises. Working with innovators inside and outside of government, DARPA has repeatedly delivered on that mission, transforming revolutionary concepts and even seeming impossibilities into practical capabilities. The ultimate results have included not only game-changing military capabilities such as precision weapons and stealth technology, but also such icons of modern civilian society such as the Internet, automated voice recognition and language translation, and Global Positioning System receivers small enough to embed in myriad consumer devices.

DARPA explicitly reaches for transformational change instead of incremental advances. But it does not perform its engineering alchemy in isolation. It works within an innovation ecosystem that includes academic, corporate and governmental partners, with a constant focus on the Nation's military Services, which work with DARPA to create new strategic opportunities and novel tactical options. For decades, this vibrant, interlocking ecosystem of diverse collaborators has proven to be a nurturing environment for the intense creativity that DARPA is designed to cultivate.

<https://pbs.twimg.com/media/D1FX89UcAEANbD.png>

4) Q indicated that 9 former DARPA employees are currently working for Facebook. 3 names are publicly known. 6 are not publicly known. Regina Dugan, the former head of DARPA and one time Google employee is one name that is publicly known.



Ex-Darpa Head Regina Dugan Leaves Google for Facebook

Translation: One of Google's top research minds is headed for the company's arch-rival.

<https://www.wired.com/2016/04/regina-dugan-leaves-google-for-facebook/>



► **Q** (!!mG7VJxZNCI) 03/06/19 (Wed) 15:55:03 ID: 5b3d8f **(2)**
File (hide): [c8434c690a926ed...jpg](#) (58.75 KB, 511x429, 511:429,

<https://pbs.twimg.com/media/D1FI5eDU0AAaJ3v.png>

After all, who in their right mind would allow the government to spy on them 24/7/365?



<https://www.wired.com/2004/02/pentagon-kills-lifelog-project/>

PENTAGON KILLS LIFELOG PROJECT

THE PENTAGON CANCELED its so-called LifeLog project, an ambitious effort to build a database tracking a person's entire existence.

Run by Darpa, the Defense Department's research arm, LifeLog aimed to gather in a single place just about everything an individual says, sees or does: the phone calls made, the TV shows watched, the magazines read, the plane tickets bought, the e-mail sent and received. Out of this seemingly endless ocean of information, computer scientists would plot distinctive routes in the data, mapping relationships, memories, events and experiences.

LifeLog's backers said the all-encompassing diary could have turned into a near-perfect digital memory, giving its

<https://pbs.twimg.com/media/D1FoP-gU0AE:TwIM.png>

7) This is a 3-year-old article on Facebook's "Building 8" program.



What is Facebook's Secret Lab Working On?

Facebook has revealed the existence of a new group called "Building 8," dedicated to researching and developing exciting new hardware products. "We'll be investing hundreds of people and hundreds of ...

<https://www.inverse.com/article/14286-here-s-what-facebook-s-new-darpa-esque-building-8-lab-may-work-on>

<https://www.inverse.com/article/14286-here-s-what-facebook-s-new-darpa-esque-building-8-lab-may-work-on>

8) Because one of Facebook's goals is to create links between the human brain and the internet to advance applications of artificial intelligence, they've hired a team of neuroscientists.

<http://mindholocaust.is.the.nextholocaust.com/news/facebook-hiring-neuroscientists-to-build-mind-reading-network-a-social-one/>

9) More on Facebook's exploration of Artificial Intelligence.



How Facebook is taking mind reading from sci-fi to reality

The rumblings started months ago. Through a series of peculiar job listings and key hires, it became clear Facebook was up to something unlike anything it had ever pursued. Building 8, as the...

<https://www.theverge.com/2017/4/20/15375176/facebook-regina-dugan-interview-building-8-mind-reading-f8-...>

<https://www.theverge.com/2017/4/20/15375176/facebook-regina-dugan-interview-building-8-mind-reading-f8-2017>

10) Facebook claims to have reorganized its Augmented Reality/Virtual Reality (AR/VR) "Building 8" program.

Q says they have reorganized but their claim to have discontinued 'Building 8' is false. It was relocated to China.

  !mG7VJxZNCI 03/06/19 (Wed) 15:54:18 ID: 5b3d8f (2) No.5543889 Part 2

.....
**BUILDING 8 NEWS RELEASE "RESTRUCTURING BUILDING 8"
RELEASE?**
[12-14-18] > RIP
<https://techcrunch.com/2018/12/14/facebook-restructures-building-8-separating-projects-into-reality-labs-and-portal-groups/>
RIP = FALSE
REORG = TRUE
CHINA-CHINA-CHINA
CHINA-CHINA-CHINA
[OPEN ACCESS - PAY FOR PLAY]
.....

<https://pbs.twimg.com/media/D1FpyrtU0AIWskQ.png>

11) A December 2018 article claims that Facebook's Building 8 program has been discontinued.

Facebook Reality Labs and the Portal Group are reported to be assuming most of the research responsibilities.



Facebook restructures Building 8, separating projects into Reality Labs and Portal groups
Facebook is restructuring its experimental hardware efforts and giving its moonshot projects a home within its AR/VR research division. The restructuring, reported by Business Insider (paywalled), di...
<https://techcrunch.com/2018/12/14/facebook-restructures-building-8-separating-projects-into-reality-labs-and-portal-groups/>

<https://techcrunch.com/2018/12/14/facebook-restructures-building-8-separating-projects-into-reality-labs-and-portal-groups/>



The Building 8 brand is dead but the big change seems to be Facebook moving its more headline-grabbing experiments further away from its nearly ready-for-production ideas.

With some of the more experimental hardware projects at Facebook — like a computer brain interface, “soft” robotics and a project to “hear” through a skin-worn device — moving to Facebook Reality Labs, it’s clear that the organization once centered around AR/VR technologies is seeing its scope expand to more distant-reaching technologies that aren’t vaguely ready for consumer products yet.

Meanwhile, the Portal group seems to be where some of Facebook’s more in-reach consumer hardware products are living, with the newly released video chat device serving as the foundation. The leader of Building 8, Rafa Camargo, who took over after the departure of Regina Dugan, is the VP of the Portal team now.

<https://pbs.twimg.com/media/D1FqjOhV4AAZD9e.png>

12) What's the difference between AR (Augmented), VR (Virtual) And MR (Mixed) Reality?



What's the Difference Between AR, VR, and MR?

Discover the difference between augmented reality, virtual reality and mixed reality.

<https://www.fi.edu/difference-between-ar-vr-and-mr>

<https://www.fi.edu/difference-between-ar-vr-and-mr>



Augmented reality (AR) adds digital elements to a live view often by using the camera on a smartphone. Examples of augmented reality experiences include Snapchat lenses and the game Pokémon Go.

Virtual reality (VR) implies a complete immersion experience that shuts out the physical world. Using VR devices such as HTC Vive, Oculus Rift or Google Cardboard, users can be transported into a number of real-world and imagined environments such as the middle of a squawking penguin colony or even the back of a dragon.

In a **mixed reality (MR)** experience, which combines elements of both AR and VR, real-world and digital objects interact. Mixed reality technology is just now starting to take off with Microsoft's HoloLens one of the most notable early mixed reality apparatuses.

<https://pbs.twimg.com/media/D1FYQjVsAARZML.png>

13) Q wrote:

[OPEN ACCESS - PAY FOR PLAY]

Facebook's practice of granting unauthorized access to its user data is at the heart of a number of recent scandals.



Facebook's latest privacy scandal: What we know about the company's handling of user data
Another day, another Facebook privacy scandal. The latest: According to The New York Times Facebook gave tech companies special access to user's data.

<https://www.usatoday.com/story/tech/2018/12/19/facebooks-latest-privacy-scandal-what-we-know-now/2361257002/>

<https://www.usatoday.com/story/tech/2018/12/19/facebooks-latest-privacy-scandal-what-we-know-now/2361257002/>

14) Q suggests Facebook has granted access to user data on a pay-for-play basis.

Internal emails show that idea was discussed though there is not yet proof they followed through.



Facebook emails suggest company explored selling people's data despite pledges not to
Internal Facebook emails, some involving CEO Mark Zuckerberg, suggest it considered charging developers for access to users' personal information.

<https://www.usatoday.com/story/news/2018/12/05/facebook-emails-suggest-considered-selling-users-personal-data/2214513002/>

<https://www.usatoday.com/story/news/2018/12/05/facebook-emails-suggest-considered-selling-users-personal-data/2214513002/>

15) Q asked about the CI_A's legal authority to spy on US citizens. They have no such authority. Q suggested they use Google, Facebook, Twitter and other social media applications to circumvent domestic

spying laws.

► Q !lmG7VJxZNCI 03/06/19 (Wed) 15:54:18 ID: 5b3d8f (2) No.5543889

Part 3

.....
LAWS WHICH PREVENT C_A OPERATIONS INSIDE HOMELAND?
BULK DATA COLLECTION_NSA_HOMELAND?
BULK DATA COLLECTION_C_A_HOMELAND?
HOW DOES THE C_A AVOID LAW TRIGGER RE:
UMBRELLA_SPY_HOMELAND?
FACEBOOK [CHINA_BUILDING 8]
GOOGLE [CHINA_DRAGONFLY]
TWITTER [US_LEG_TRACK]
FACEBOOK TRACK USER GPS, VOICE & TEXT?
GOOGLE TRACK USER GPS, VOICE & TEXT?
TWITTER TRACK USER GPS?
[PHONE_PAD_MICROPHONE_ALGO_EMBED]
.....

<https://pbs.twimg.com/media/D1Fxz7DU0AEQuqg.png>

16) The CI_A's 1947 charter permits foreign surveillance but prohibits domestic spying. (Domestic surveillance is done by the NSA)

The Patriot act weakened domestic surveillance restrictions.

The CI_A tends to abuse its surveillance powers.



More About Intelligence Agencies (CIA/DNI) Spying

Central Intelligence Agency. Because of the excessive secrecy surrounding CIA operations, little is known about its domestic activities. In its 1947 charter, the CIA was prohibited from spying against...

🔗 <https://www.aclu.org/other/more-about-intelligence-agencies-ciadni-spying>

<https://www.aclu.org/other/more-about-intelligence-agencies-ciadni-spying>

MORE ABOUT INTELLIGENCE AGENCIES (CIA/DNI) SPYING



Central Intelligence Agency. Because of the excessive secrecy surrounding CIA operations, little is known about its domestic activities. In its 1947 charter, the CIA was prohibited from spying against Americans, in part because President Truman was afraid that the agency would engage in political abuse. But the law didn't stop the CIA from spying on Americans. During the 1960s, in clear violation of its statutory mission to co-ordinate foreign intelligence operations only, the CIA ventured into the domestic spying business through "Operation Chaos," in which it spied on as many as 7,000 Americans involved in the peace movement.

Unfortunately, the exposure of intelligence failings before the 9/11 attacks caused policy makers to promote "information sharing" among intelligence and law enforcement agencies as a cure-all, creating the likelihood that the CIA would increasingly operate domestically. Today we know that the CIA is a participant in FBI Joint Terrorism Task Forces, which engage in both foreign and domestic terrorism investigations. And the USA Patriot Act eased restrictions on the sharing of information the FBI collects in grand jury investigations and law enforcement wiretaps with the CIA. An ACLU lawsuit revealed that the CIA has also used National Security Letters to demand Americans' personal financial records without prior court approval. The CIA has acknowledged using National Security Letters "on a limited basis" to obtain financial information from U.S. companies. The history of the CIA's abuse of power and the continuing lack of public accountability over CIA operations make such revelations concerning to civil liberties advocates. The CIA's involvement in the NYPD intelligence activities targeting innocent Muslim communities in the Northeast reveal the CIA is once again treating Americans as suspected enemies.

<https://pbs.twimg.com/media/D1FzHHUVsAA0sSM.jpg>

17) Amazon, Facebook, Google and Twitter say they collect our data to enhance their "products" which will ultimately provide a better "user experience" but in reality, our data is being collected by the clown agency as a way to circumvent domestic spying laws.

▶ Q !!mG7VJxZNCI 03/06/19 (Wed) 15:54:18 ID: 5b3d8f (2) No.5543889

Part 4

.....

ALL FOR MARKETING PURPOSES AS PUBLICLY DISCLOSED?
WHO HAS ACCESS TO BULK TRACK DATA?

WHO HAS ACCESS TO BULK DATA?

IF NSA HAS ABILITY TO 'ABSORB' DATA STREAM UT IN-HOUSE TOOLS, DOES C_A HAVE ABILITY TO 'COLLECT' DATA STREAM FROM 'FUNDED' NETWORKED' OFFSHOOTS [BIG TECH]?

OFFSHOOTS NECESSARY TO AVOID C_A BREACH OF US DOMESTIC LAW?

AMAZON SERVER/CLOUD CONTRACT?

.....

<https://pbs.twimg.com/media/D1F1A9LUcAEXxm.png>

18) The CI_A wasn't content to be limited to foreign surveillance. It found ways to spy on US citizens & politicians.

As an example of their corruption & disregard for the law, they were caught under John Brennan's leadership illegally spying on Congress.

.....
AMAZON_SERVER/CLOUD_ROUTE_DATA 1-99 DOMESTIC?
C_A TASKED W/ GATHERING AND ANALYZING INFO ON FOREIGN
GOVS + INDIVS? SIGINT - COV
NSA TASKED W/ GATHERING AND ANALYZING INFO ON A GLOBAL
SCALE (INCLUDING DOMESTIC)? SIGINT - COV
WHAT FORMER US PRESIDENT WAS C_A DIRECTOR?

<http://www.thedrive.com/the-war-zone/25241/george-h-w-bush-saved-the-cia>

THINK C_A [BRENNAN] AUTH SPY CAMPAIGN US SENATE UNDER
HUSSEIN.

THINK C_A INSTALL CAMPAIGN US HOUSE & SENATE
INFILTRATION.

[PART 1 OF 9]

Q

<https://pbs.twimg.com/media/D1F14-hVYAAR06k.png>

19) George Herbert Walker Bush was CI_A director before becoming POTUS. This article extols him as a heroic patriot who reformed the tarnished image of the agency and restored our ability to trust our beloved clowns.



George Bush Saved The CIA

The CIA was mired in controversy and battling for its life before George Bush took over and turned it around with long-lasting reforms.

<http://www.thedrive.com/the-war-zone/25241/george-h-w-bush-saved-the-cia>

<http://www.thedrive.com/the-war-zone/25241/george-h-w-bush-saved-the-cia>

20) The CI_A's partnership with Amazon to build and maintain its cloud-based server shows cooperation (and perhaps collaboration) between the clown agency and the private companies that collect our data.



The Details About the CIA's Deal With Amazon

A \$600 million computing cloud built by an outside company is a "radical departure" for the risk-averse intelligence community.

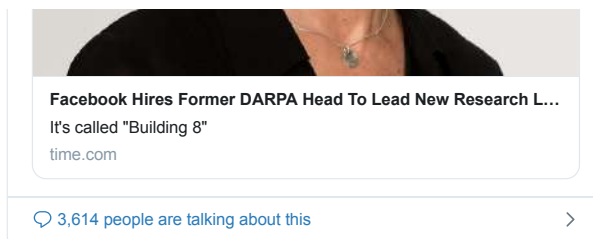
<https://www.theatlantic.com/technology/archive/2014/07/the-details-about-the-cias-deal-with-amazon/374632/>

<https://www.theatlantic.com/technology/archive/2014/07/the-details-about-the-cias-deal-with-amazon/374632/>

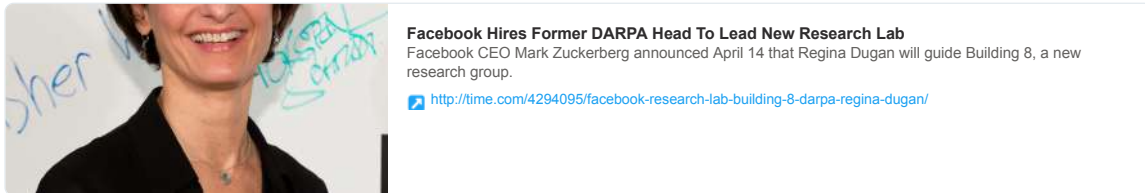
21) @Amyboo69 got a shoutout from Q after posting a link to an article about Regina Dugan being hired by Facebook.

Tweet:





Article:



<http://time.com/4294095/facebook-research-lab-building-8-darpa-regina-dugan/>



<https://pbs.twimg.com/media/D1F7oRzU8AAI3G3.png>

22) If the description and goals of Facebook and Lifelog [DARPA] were the same, and if senior team members went from DARPA to Facebook and if Lifelog was shut down on the same day Facebook was launched, then DARPA (Lifelog) = Facebook.

▶ Q [!mG7VJxZNCI] 03/06/19 (Wed) 21:38:12 ID: 27adf2 (2) No.5550175

<https://twitter.com/amyboo69/status/1103512061693161472>

Define 'Lifelog' [DARPA].

"an ontology-based (sub)system that captures, stores, and makes accessible the flow of one person's experience in and interactions with the world in order to support a broad spectrum of associates/assistants and other system capabilities". The objective of the LifeLog concept was "to be able to trace the 'threads' of an individual's life in terms of events, states, and relationships", and it has the ability to "take in all of a subject's experience, from phone numbers dialed and e-mail messages viewed to every breath taken, step made and place gone".

Define 'FB'.

The Facebook service can be accessed from devices with Internet connectivity, such as personal computers, tablets and smartphones. After registering, users can create a customized profile revealing information about themselves. Users can post text, photos and multimedia of their own devising and share it with other users as "friends". Users can use various embedded apps, and receive notifications of their friends' activities. Users may join common-interest groups.

Compare & Contrast.

DARPA senior employees > FB?

DARPA TERMINATES PROGRAM FEB 4, 2004.

FB FOUNDED FEB 4, 2004.

DARPA = FB

Q

<https://pbs.twimg.com/media/D1F8XJKUYAA019E.png>

23) The clown agency developed Lifelog with your money, took it private because no one would use it otherwise, made it cool by only allowing .edu email addresses to register (initially), killed off all competitors, and got Hollywood to promote its spying platform.

▶ Q [!mG7VJxZNCI] 03/06/19 (Wed) 21:58:23 ID: 5de4f4 (3) No.5550547 >>5550571 >>5550574 >>5550579 >>5550580 >>5550586 >>5550588

Logical thinking.

Did DARPA complete build/code (tax-payer funded) 'LifeLog' program?

After completion, was there fear the public wouldn't accept the adoption if known it was DoD/C_A backed?

Do you believe people would join a platform knowing it was under the control of the C_A and FED GOV?

No.

How do you lure the masses into entering all their personal info and private messages (i.e. their LIFE LOG) onto a new platform?

Do you make it cool?

How did FB 'supposedly' start and launch?

Ivy league only?

Develop a trend and/or following?

How do you keep the project running w/o 'public' taxpayer funds? [DoD reported LifeLog was **TERMINATED** to Congress/Senate OS]

Define 'Black Budget'.

Did HWOOD push?

Do people follow the 'stars'?

Competitors systematically attacked (myspace) to prevent comp?

THE LARGEST 'COLLECTIVE' SOCIAL MEDIA PLATFORM IN THE WORLD (BILLIONS LOGGED) IS OWNED AND OPERATED (COVERTLY) BY THE CENTRAL INTELLIGENCE AGENCY OF THE UNITED STATES OF AMERICA.

The More You Know.

Q

<https://pbs.twimg.com/media/D1F8j2rUcAAe75j.png>

24) The development of Facebook by the CI_A and DARPA bears an eerie resemblance to the storyline of the Jason Bourne film about a social media company called Deep Dream.



What Mark Zuckerberg Had To Do With 'Jason Bourne'

There is a lot going on in Jason Bourne, the newest film in the Bourne series. The movie, the fourth or fifth in the series (depends on your opinion of The Bourne Legacy) and the first in almost 10 y...

▶ <https://www.bustle.com/articles/175006-is-aaron-kalloor-based-on-mark-zuckerberg-in-jason-bourne-the-tech-...>

<https://www.bustle.com/articles/175006-is-aaron-kalloor-based-on-mark-zuckerberg-in-jason-bourne-the-tech-giant-seems-very-familiar>

25) Since the government developed the technology for Facebook, they limited legislation that would affect its utilization.

Zuckerberg was chosen as a charismatic, geeky puppet.

His task was to make Facebook go viral.

China knows facebook is CI_A malware.

>>5550547

Expand your thinking.

If covertly operated **[data accessible to project designators]** would they attempt to prevent any type of GOV regulations from being imposed?

Expand your thinking further.

Why was MZ chosen as CEO (public figure) tasked to expand growth?

Family tree of MZ?

Who is the wife of MZ?

Family tree of wife?

Why won't CHINA allow FB?

Situational awareness?

Do they know it's an individual collection asset program being covertly operated by the C_A?

Do they know it's been expanded to tap into the microphone of any device for listening and bulk data collection?

Do they know it's been expanded to tap into the GPS router of the device for RT tracking?

Do they know it's been expanded to tap into the camera function of the device in order to view/record all target designators?

Q

<https://pbs.twimg.com/media/D1F-YRLVsAAorGI.png>

26) Zuckerberg married Priscilla Chan whose parents are Chinese citizens that fled Vietnam as boat refugees.

https://en.wikipedia.org/wiki/Priscilla_Chan

Priscilla Chan

From Wikipedia, the free encyclopedia

For other people named Priscilla Chan, see Priscilla Chan (disambiguation).

Priscilla Chan (born February 24, 1985) is an American pediatrician and philanthropist. She and her husband Mark Zuckerberg, the co-founder and CEO of Facebook, established the Chan Zuckerberg Initiative in December 2015, with a pledge to donate 99 percent of their Facebook shares, then valued at \$45 billion. She is a graduate of Harvard University and received her medical degree from the University of California, San Francisco (UCSF).

Early life

On February 24, 1985, Chan was born in Braintree, Massachusetts,^[2] and grew up in Quincy, Massachusetts, a suburb of Boston. Her parents were Hoa Chinese refugees who fled Vietnam in refugee boats.^{[3][4]} She grew up speaking Cantonese and served as an interpreter for her grandparents. She has two younger sisters.^[5] In 2003, she graduated as class valedictorian from Quincy High School, and was voted "class genius" by her classmates.^[6] According to a Facebook post by Mark Zuckerberg, Chan is a Buddhist.^[6]

Priscilla Chan



Priscilla Chan, in 2014.

Born	February 24, 1985 (age 34) ^[1] Braintree, Massachusetts, U.S.
Residence	Palo Alto, California, U.S.
Nationality	American
Citizenship	United States
Alma mater	Harvard University University of California, San Francisco

<https://pbs.twimg.com/media/D1GABK6VYAAcuhK.jpg>

27) The first long post in this series was [1 of 9]
The last one was [2 of 9].

► Q (!!mG7VJxZNCI) 03/06/19 (Wed) 22:09:07
ID: 5de4f4 (3) No.5550834 >>5550845

>>5550786

[2 of 9] complete.

Q

https://pbs.twimg.com/media/D1GA4u_UYAIK_hu.png

28) I'm not sure if future posts in this series will be strictly related to Facebook and DARPA or if we'll receive information about Twitter Google and Amazon.
(I suspect that we will.)

► Anonymous 03/06/19 (Wed) 22:12:15 ID: 459ca5 (8)

>>5550547

>>5550834

>>5550786

[PART 1 OF 9]

[2 of 9] Complete.

7 more to come.

All 9 related to Facebook/DARPA/China?

<https://pbs.twimg.com/media/D1GBKBKUyAIYgJ2.png>

29) Q isn't dropping this information just to amuse us.
He wants us to know that POTUS is taking measures to remove power from these pockets of control and return that power to we, the people.

► Q (!!mG7VJxZNCI) 03/06/19 (Wed) 22:16:14 ID: 4e2679
(3) No.5551010 >>5551015 >>5551017 >>5551020 >>5551033

<https://qz.com/1145669/googles-true-origin-partly-lies-in-cia-and-nsa-research-grants-for-mass-surveillance/>

[DARPA>GOOG]

Re-review past drops.

Major steps underway to challenge these control pockets.

Q

<https://pbs.twimg.com/media/D1GC5WzV4AAsAta.png>

30) Google was greatly helped when it first began by research grants from the government for mass

surveillance.



Google's true origin partly lies in CIA and NSA research grants for mass surveillance

The story of the deliberate creation of the modern mass-surveillance state includes elements of Google's surprising, and largely unknown, origin. It is a somewhat different creation story than the on...

<https://qz.com/1145669/googles-true-origin-partly-lies-in-cia-and-nsa-research-grants-for-mass-surveillance/>

<https://qz.com/1145669/googles-true-origin-partly-lies-in-cia-and-nsa-research-grants-for-mass-surveillance/>

31) They want us divided because when we're divided, we are weak.
An awake public is an empowered public and it is their greatest fear.

▶ Q !!mG7VJxZNCI 03/06/19 (Wed) 22:34:41 ID: 4e2679 (3) No.5551524 >>5551534 >>5551542 >>5551545
PEOPLE ARE PAWNS IN THEIR SICK GAME OF GLOBAL DOMINATION.
PEOPLE ARE DIVIDED TO PREVENT A RISING OF THE PEOPLE.
PEOPLE ARE DIVIDED AND TAUGHT TO FIGHT THEMSELVES INSTEAD OF THE RULING CLASS.
RACE VS RACE
RELIGION VS RELIGION
POLITICAL VS POLITICAL
CLASS VS CLASS
SEX VS SEX
WHEN YOU ARE DIVIDED, YOU ARE WEAK.
WHEN YOU ARE WEAK, YOU HAVE NO POWER.
WHEN YOU HAVE NO POWER, YOU HAVE NO CONTROL.
STAY STRONG, PATRIOTS.
STAY UNITED, NOT DIVIDED.
YOU ARE WHAT MATTERS.
YOU, AWAKE, IS THEIR GREATEST FEAR.
Q

<https://pbs.twimg.com/media/D1Giti4UcAAiv-3.jpg>

32) Snowden became a hero for exposing the NSA's spy tools but he first worked for the CI_A.

Why didn't he expose CI_A surveillance tools if he's primarily interested in freedom from surveillance?

Once a clown always a clown.

The NSA's loss is the CI_A's gain.

▶ Q !!mG7VJxZNCI 03/06/19 (Wed) 22:23:50 ID: 4e2679 (3) No.5551229 >>5551245 >>5551248 >>5551250 >>5551257
<https://www.iqt.org/our-history/>
Why did @Snowden only engage and attack the NSA?
If @Snowden really cared about privacy/citizenship awareness, why didn't he expose the C_A's main programs?
@Snowden was priv to DARPA, IQT, and NSA SURV / COV programs.
Why did @Snowden only focus on NSA?
Where did @Snowden work prior to NSA?
ASK YOURSELF A VERY SIMPLE QUESTION, WOULD YOU RELEASE (GO LIVE) TO THE PUBLIC
ACROSS THE MEDIA ALL HIGHLY CLASSIFIED MATERIAL (NSA) PRIOR TO.....GETTING
TO YOUR END DESTINATION?
OR, WOULD YOU LOGICALLY TRAVEL TO YOUR END DESTINATION, THEN RELEASE PUBLICLY?
WAS RUSSIA THE PLANNED LOCATION?
WHY RUSSIA?
WHY DID CHINA (HKG) LET HIM OUT OF THE COUNTRY?
WAS THERE A 'RED' SECURITY ALERT PUT OUT TO PREVENT PASSPORT TRAVEL ACROSS ALL
NATIONS?
WHY DID CHINA GRANT ACCESS TO TRAVEL W/ THE BLOCK IN PLACE?
WHY RUSSIA?
RUSSIA RUSSIA RUSSIA
Q

<https://pbs.twimg.com/media/D1GkpkJUYAA6ipZ.png>

33) The CI_A paints Russia as a perpetual villain.

Russia was Snowden's destination.

CI_A clears Snowden through Hong Kong & Russia w/ China help when global security hold is placed on his passport.

CI_A creates a story that he's "stranded" in Russia

CI_A abandon's Snowden.

► Q !UW.yye1fxo Feb 18 2018 20:41:03 # 104

@SNOWDEN
 WHERE ARE YOU?
 NOT RUSSIA.
 [EYES ON]
 YOU ARE NOW A LIABILITY.
 HELPING @JACK?
 PROJECT DEEPTDREAMv2[A]].
 WE WILL NEVER FORGET.
 ES FAILED.
 WHERE IS ES?
 JOHN PERRY BARLOW.
 DEFINE THE END?
 THE DAY OF RECKONING IS UPON US.
 JOHN 3:16
 Q

<https://pbs.twimg.com/media/D1GoxC9U8AEdiv.png>

► Q !UW.yye1fxo 01/27/18 (Sat) 11:41:44 ID: 5997a0 (4) No.180445 >>180458 >>180461

>>180316
 HK allowed his passport to clear customs WITH THE CLOWNS IN AMERICA
 AND DEPT OF DEFENSE PUTTING A NAT SEC HOLD WW?
 How does he clear customs?
 How does he end up in Russia?
 Coincidence?
 Who was the 1st agency he worked for?
 Who taught him the game?
 Who assigned him w/ foreign ops?
 Why is this relevant?
 Future unlocks past.
 Watch the news.
 Spider web.
 Stop taking the sleeping pill.
 Q

<https://pbs.twimg.com/media/D1GpZ9KU4AA2p1d.jpg>

34) Mark Zuckerberg announced a sudden decision to make Facebook a more "privacy-focused" platform.

► Anonymous 03/06/19 (Wed) 22:46:44 ID: 11b8d2 (2) No.5551830 >>5551858 >>5551871 >>5551899 >>5551985

File (hide): 31fb3712bd781ce...,png (554.97 KB, 933x1005, 311:335, ClipboardImage.png) (h) (u)

File (hide): 6108b07c3b79308...,png (267.88 KB, 653x386, 653:386, 6108b07c3b79308ee4d06417cb...,png) (h)



WATCH guy behind Zeeborg:
 Shadowman, Handler, Programmer



CNN.COM
 Zuckerberg: Mueller team interviewed Facebook staff - CNN Video
<https://www.cnn.com/videos/cnn/2018/04/18/facebook-robert-mueller-interview-mark-zuckerberg-sngall>

<https://twitter.com/SputnikInt/status/1103531723986485248>

Mark Zuckerberg outlines new plan to build 'privacy-focused' Facebook <https://sptnkne.ws/kSJj>
 12:44 AM - 7 Mar 2019

https://pbs.twimg.com/media/D1Gr6JU8AE_5IX.jpg

35) Zuckerberg knows heavy government regulation is coming if Facebook doesn't fold under the weight of corruption first or be bankrupted by class action lawsuits.

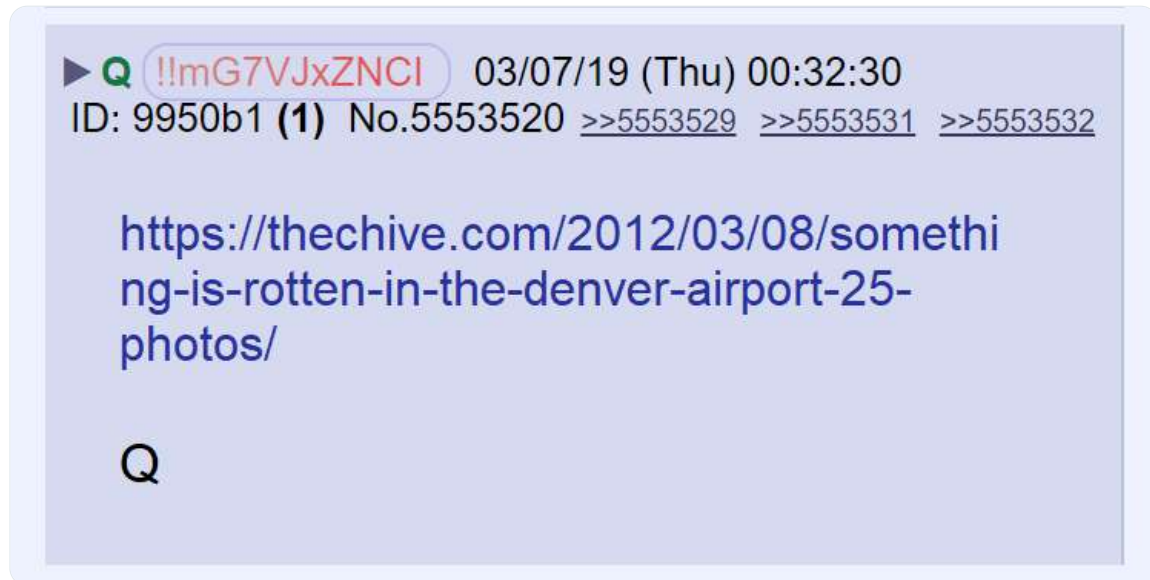
► Q !!mG7VJxZNCI 03/06/19 (Wed) 23:41:31
 ID: 1e3478 (2) No.5552746 >>5552751 >>5552753

>>5551830

Trying to get ahead of something?
 What a coincidence.
 Q

<https://pbs.twimg.com/media/D1GtGgiUYAEVVM2.png>

36) Q posted a link.



<https://pbs.twimg.com/media/D1GwQeUU8AAgEq-.png>

37) You can never unsee some things.
Symbolism will be their downfall.

(Did the elites actually build an underground bunker below the Denver airport?)



Something is rotten in the Denver airport (13 Photos)

Something stinks in the Denver International Airport. It has been rumored that a 5 building bunker exists below the airport and the POTUS has been ushered there in moments of Pending DOOM.

<https://thehive.com/2012/03/08/something-is-rotten-in-the-denver-airport-25-photos/>

<https://thehive.com/2012/03/08/something-is-rotten-in-the-denver-airport-25-photos/>

38) Notable:
One of the images is of a stone marker for a time capsule.
The dedication was done on March 19, 1994.
The [-21] day countdown ends this year on March 19th.
Coincidence?



<https://pbs.twimg.com/media/D1GxSAhVAAAcuzA.jpg>

39) We are part of an operation like none in history. A communications operation that assists in a mass awakening resulting in billions of people being set free from the power of corruption.

July 4, 2019, will be a memorable day.

► Q !ImG7VJxZNCI 03/06/19 (Wed) 21:13:37 ID: 27adf2 (2) No.5549666 >>5549676 >>5549680 >>5549681

File (hide): e8f3bec87a15325...jpg (77.9 KB, 640x480, 4:3, 27264602991_ed3a1e66d0_z.jpg) (h) (u)



<https://www.youtube.com/watch?v=B5T7Gr5cJbM>

Never, in our history, has a communications project such as this taken place.

>Return Power Back to the People

>Truth, Transparency, and Equal Justice Under the Law.

We hold these truths to be self-evident, that all men (& women) are created equal, that they are endowed by their Creator with certain unalienable Rights, that among these are Life, Liberty and the pursuit of Happiness. — That to secure these rights, Governments are instituted among Men (& Women), deriving their just powers from the consent of the governed, — That whenever any Form of Government becomes destructive of these ends, it is the Right of the People to alter or to abolish it, and to institute new Government, laying its foundation on such principles and organizing its powers in such form, as to them shall seem most likely to effect their Safety and Happiness. Prudence, indeed, will dictate that Governments long established should not be changed for light and transient causes; and accordingly all experience hath shewn that mankind are more disposed to suffer, while evils are sufferable than to right themselves by abolishing the forms to which they are accustomed. But when a long train of abuses and usurpations, pursuing invariably the same Object evinces a design to reduce them under absolute Despotism, it is their right, it is their duty, to throw off such Government, and to provide new Guards for their future security. —

"Freedom is never more than one generation away from extinction. We didn't pass it to our children in the bloodstream. It must be fought for, protected, and handed on for them to do the same." - Reagan

United We Stand.
July 4, 2019.
WWG1WGA!!!
Q

<https://pbs.twimg.com/media/D1Gyk-XUYAAXwkD.jpg>

40) Q's link.



<https://www.youtube.com/embed/B5T7Gr5oJbM>

41) Our friend [@michaelbeatty3](#) caught the Hannity radio show yesterday. Hannity's sources say justice is coming.



Miguelifornia
[@michaelbeatty3](#)



Listening to Hannity Radio in my car just now.
Sean seems calm, confident & at peace.
He mentioned 3 different times....
"My sources are telling me all will be
well and that justice is finally coming"

IT'S COMING#WWG1WGA #QAnon #DarkToLight

♡ 11.8K 11:16 PM - Mar 6, 2019

💬 9,189 people are talking about this





 **Miguelifornia**

@michaelbeatty3

Following



Listening to Hannity Radio in my car just now.

Sean seems calm, confident & at peace. He mentioned 3 different times....

"My sources are telling me all will be well and that justice is finally coming"

IT'S COMING

[#WWG1WGA](#) [#QAnon](#) [#DarkToLight](#)



4:16 PM - 6 Mar 2019

<https://pbs.twimg.com/media/D1Gz0POVsAAocBN.png>

42) Q has heard Hannity has credible sources.

Two pens?

Note the filename: IMG_45EXE.PNG

Executive Order coming?

Q !!mG7VJxZNCI 03/06/19 (Wed) 18:05:15 ID: efd49b (1) No.5546235 >>5546242 >>5546246

File (hide): a0e664b506b6f52...png (3.26 MB, 1125x2436, 375:812, IMG_45EXE.PNG) (h) (u)

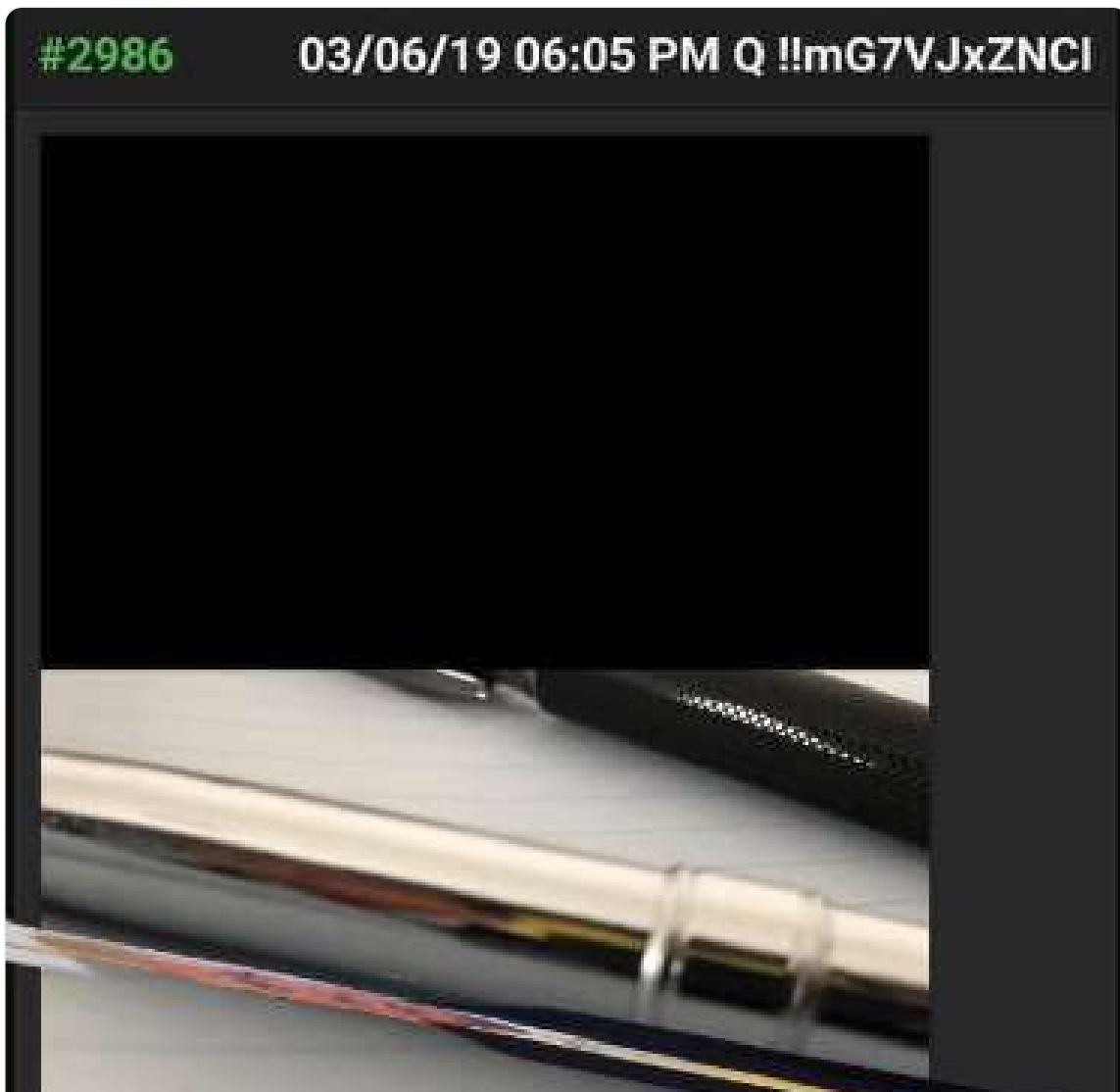


<https://twitter.com/michaelbeatty3/status/1103434110310146048>

We hear his source(s) are 'very' credible.
Q

<https://pbs.twimg.com/media/D1G0N7rU8AYQIsI.jpg>

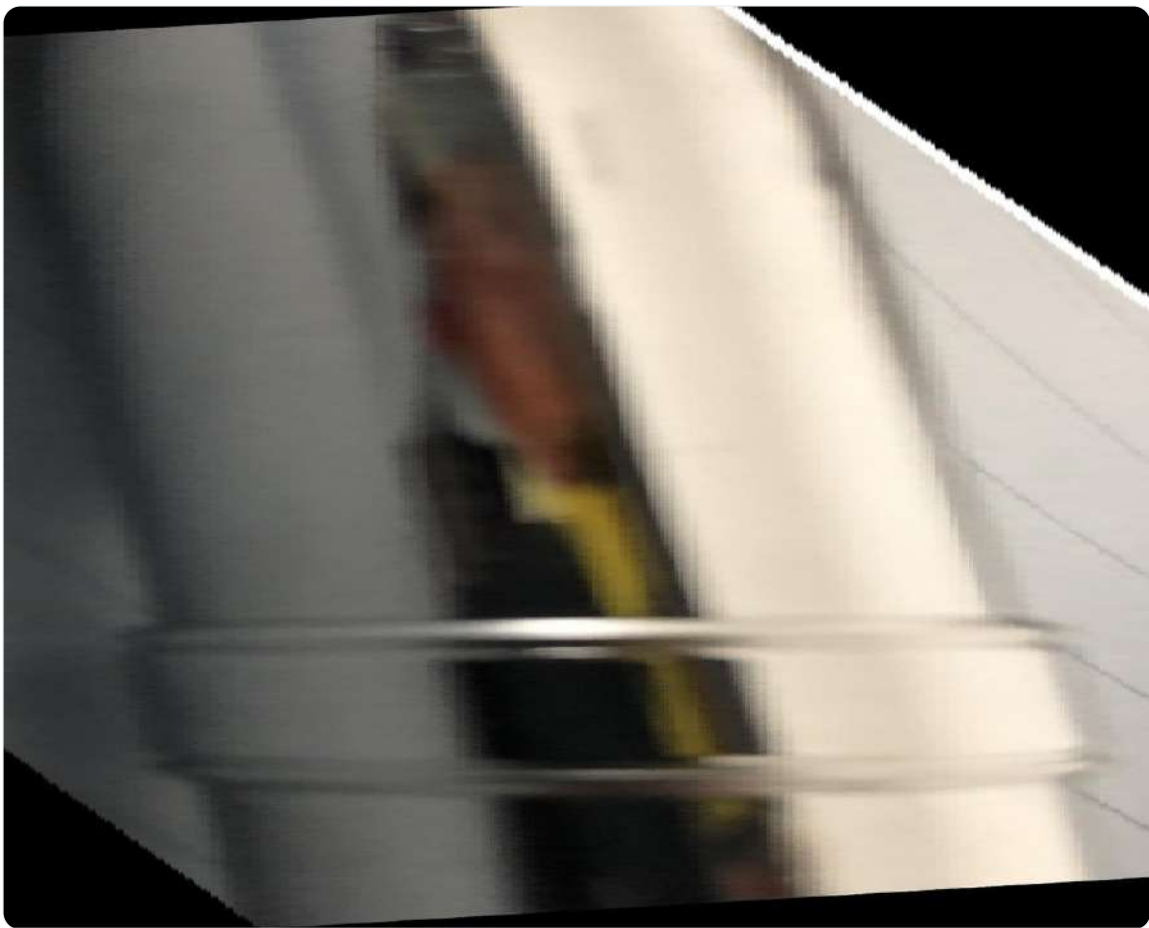
43) Many attempts have been made to figure out what the reflection in the pen is. Images that attempt to show POTUS in the reflection ignore the fact that he would have to be laying or standing sideways due to the orientation of the pen.





<https://pbs.twimg.com/media/D1G1DZKU0AALxB5.png>

44) I rotated and stretched the image and this is what I came up with.
But again, the orientation of the pen creates a problem.



<https://pbs.twimg.com/media/D1G1wvFU4AgDq5W.jpg>

45) An interesting possibility (I'm not putting any money on it.)

► Anonymous 03/06/19 (Wed) 21:36:33 ID: b02434 (1) No.5550145 >>>5550234
File (hash): 181f1bba6019ad5... .jpeg (697.75 KB, 2323x1822, 2323:1822, F4540D09E8D32-52CF-808A3.../009) (b) (u)

2. Mont Blanc Ball Point

TechMarch.com

The mastery master piece which was created by collaboration between Mont Blanc and the Van der Grinten & Arpel's carries the glory of most expensive ball point pen of the world. The cost of the pen is USD 730,000. This pen is a master piece and has a wonderful jewelry art on it.

Is Q+ namefagging at this point? ;)

Going back to cross reference FISA judges and WH.

HAND AND FACE

WHITE SHIRT CUFF

ARM

DRAPE

TRUMP GIVES OVAL OFFICE NEW LOOK WITH GOLD DRAPES

<https://pbs.twimg.com/media/D1G2DZrUDAY-eko.jpg>

46) It's easy to become obsessed with minor details.
The 40,000 ft view shows us that POTUS is with us.
He's one of us.
He's giving us insider information no other President would dare to.
Feel proud, patriot.
WWG1WGA



<https://pbs.twimg.com/media/D1G4y8jUcAMUqfE.jpg>

47) @Davidwmiller91 posted a graphic showing @USAttyHuber's meeting with AG William Barr this week and the related place on Q's countdown.

BigD
@Davidwmiller91

IT'S HAPPENING!!! #QAnon #WWG1WGA #TrustThePlan
#EnjoyTheShow #ByeCrookedHillary #TheGreatAwakening

5,625 1:16 AM - Mar 8, 2019

4,926 people are talking about this



BigD

@Davidwmiller91

Following



IT'S HAPPENING!!!

#QAnon #WWG1WGA #TrustThePlan
#EnjoyTheShow #ByeCrookedHillary
#TheGreatAwakening



6:16 PM - 7 Mar 2019

<https://pbs.twimg.com/media/D1HDynJUcAI3XgU.png>

48) AG Barr meeting with Huber and IG Horowitz precedes the release of the IG's next report.

[-30]
[-45]
[-60]
[-90]
-Blockade removal ['Scaramucci' model]
-[RR] removal [Goodbye #2 [#1 _ oversight of Mueller]
-[Ohr] removal
-[1-4] removal
-Barr install
-Barr (w/ Whitaker) review [RR] notes re: strong reservations to DECLAS due to sources & methods + Foreign CLAS (irreparable harm) > OIG review prior to executing order
-Barr (w/ Whitaker) pull DECLAS review assignment from OIG [cite: executive order from POTUS does not require special oversight - DOJ/FBI (Wray) fully capable in reviewing and commenting re: OP integrity (sources & methods) etc.]
-Barr executes order to DECLAS + provide members of H committee long requested supplemental documentation in C setting [scope memo + CLAS] as required by US Law.
-Whitaker remain DOJ senior staff
-Barr meeting Huber & OIG
-OIG report
-House D's threaten subpoena of Barr/Whitaker re: DECLAS, SC report, Huber, etc....
-House D's use subpoena power to Acts 1, 2, and 3. [spill +30]
-Meeting w/ NK > DENUC plan/process > sanctions lift meets subj A, B food for people (aid)
UK/AUS narrative shift re: in_country spy campaign v. POTUS (hops 1 to 2; 2 to 3; 3 to 4; 4 to target)
-D sky is falling push to public (scare to control)(projection)
-Public Awakening
-Narrative damage control
-Placeholders active
-Wall discussion end (public awareness of D's)
-Red/Green Castle per orig plan
Dark to Light.
<https://www.youtube.com/watch?v=G2qIXXafxCQ>
Q

<https://pbs.twimg.com/media/D1HFCfNUcAEVhTr.png>

49) Q Responded.

<https://www.nbcsandiego.com/news/local/Source-Leaked-Documents-Show-the-US-Government-Tracking-Journalists-and-Advocates-Through-a-Secret-Database-506783231.html>



Richard Blumenthal ✓

@SenBlumenthal

Follow



Why is the Department of Homeland Security reportedly building secret dossiers on journalists & immigration lawyers? Apparent profiling mirrors the behavior of autocrats. I will be demanding answers.



Leaked Documents Show the Government Tracking Journalists

The documents detail an intelligence-gathering effort by the United States and Mexican authorities, targeting more than 50 people including journalists, an attorn...

[nbc.com](https://nbc.com/news/politics-government/leaked-documents-show-the-government-tracking-journalists)

10:33 AM - 7 Mar 2019

<https://pbs.twimg.com/media/D1HHndZU4AI0F9U.png>

51) Corrupt journalists and those attempting to subvert justice will face a much bigger battle in the future.

The leak was plugged.

► Q !!mG7VJxZNCI 03/07/19 (Thu) 21:07:53 ID: f9e971
(2) No.5568772 >>5568777 >>5568785 >>5568790

<https://twitter.com/SenBlumenthal/status/1103710332994887682>

Glimpse of something much bigger to come?
Actions have consequences.
Remember, it goes both ways.
Nobody is safe.
Leak was plugged.

Q

<https://pbs.twimg.com/media/D1HIPxmU0AExrH9.png>

52) In January Q suggested that many legal FISA warrants were currently active against those who illegally spied on the President.

FISA goes both ways.

► Q !!mG7VJxZNCI 01/06/19 (Sun) 11:34:40 ID: e73272 (2)
No.4628579 >>4628585 >>4628586 >>4628588 >>4628590 >>4628591

How many AUTH FISA UMBRELLA SURV warrants targeting those who illegally targeted [] are currently active?
Upstream collection can be very revealing.
When you no longer control the levers of POWER, do FVEY ('Allies') buckle & cooperate in order to preserve and maintain their future?
Germany losing stranglehold on EU?
The future will not repeat the past.
The clock is ticking.
Q

https://pbs.twimg.com/media/D1HI_geU0AE3RIW.png

53) After the November election, Q said we got what we needed.
Investigations that started in the House would be continued in the Senate.

Q !mG7VJxZNCI No.424
Nov 7 2018 00:55:31 (EST)

2444

<https://twitter.com/realDonaldTrump/status/1060022696703070208>

We got what we needed.
Thank you, Patriots!
Senate means everything.
Think Judges (SC) & Cabinet.
DECLAS overrides all potential House blockades.
POTUS has ultimate authority.
Shift to Senate Judiciary (oversight) from House to now occur (stronger position and held in reserve for this scenario).
Lower chamber (House) used as 2-year starter.
Upper chamber (Senate) will be used next 2-year closer.
<https://www.judiciary.senate.gov/about/jurisdiction>
Military planned.
No impact re: ongoing investigations
Team is stronger [PRO].
Q

https://www.scribd.com/document/401345263/Log-to-Ag-Barr-03-07-2019-Fisa#from_embed

House > Senate

Q

<https://pbs.twimg.com/media/D1HNORIU4AAwyS3.jpg>

54) Senate Judiciary Chair Lindsey Graham requested all documents & comms shared with the intelligence gang of 8 regarding the Russia investigation and docs related to the Carter Page FISA application be delivered to him by...

March 21st.

UNITED STATES SENATE
COMMITTEE ON INTELLIGENCE
WASHINGTON, DC 20540-5000

March 7, 2019

The Honorable William P. Barr
Attorney General
U.S. Department of Justice
950 Pennsylvania Ave. NW
Washington, D.C. 20530

Dear Attorney General Barr:

Through the Foreign Intelligence Surveillance Act (FISA), Congress granted the Executive the ability to seek classified evidence to conduct surveillance on Americans from a special, secret source that meets behind closed doors. Given the nature of these sources and the need to protect them, the public's confidence in the FISA process is based on assurances, such as those set forth in the 2001 Woods provisions, that FISA applications will undergo rigorous review before being referred to the Foreign Intelligence Surveillance Court (FISC). Only through strict adherence to procedures like those set forth in the Woods memo and production by the government to the FISC of all material and relevant facts, can the public continue to have confidence in FISA.

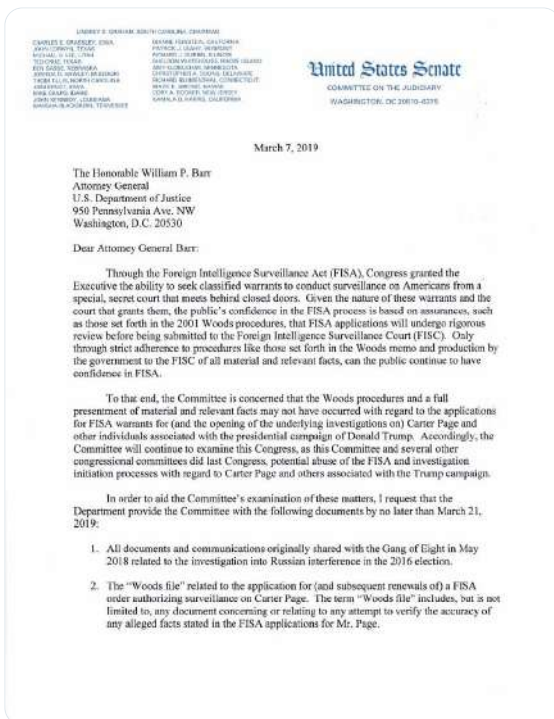
To that end, the Committee is concerned that the Woods provisions and a full presentation of material and relevant facts may not have occurred with regard to the application for FISA warrants for (and the opening of the underlying investigation on) Carter Page and other individuals associated with the presidential campaign of Donald Trump. Accordingly, the Committee will continue to examine this Congress, as this Committee and several other congressional committees did last Congress, potential abuse of the FISA and investigation instance processes with regard to Carter Page and others associated with the Trump campaign.

In order to aid the Committee's examination of these matters, I request that the Department provide the Committee with the following documents by no later than March 21, 2019:

1. All documents and communications originally shared with the Gang of Eight in May 2018 related to the investigation into Russian interference in the 2016 election.
2. The "Woods file" related to the application for (and subsequent issuance of) a FISA order authorizing surveillance on Carter Page. The term "Woods file" includes, but is not limited to, any document concerning or relating to any attempt to verify the accuracy of any alleged facts stated in the FISA applications for Mr. Page.

Log to Ag Barr 03-07-2019 (Fisa)
Log to Ag Barr 03-07-2019 (Fisa) - Read online for free. Log to Ag Barr 03-07-2019 (Fisa)
https://www.scribd.com/document/401345263/Log-to-Ag-Barr-03-07-2019-Fisa#from_embed

https://www.scribd.com/document/401345263/Log-to-Ag-Barr-03-07-2019-Fisa#from_embed



https://pbs.twimg.com/media/D1HNk_ZUwAA99JY.jpg

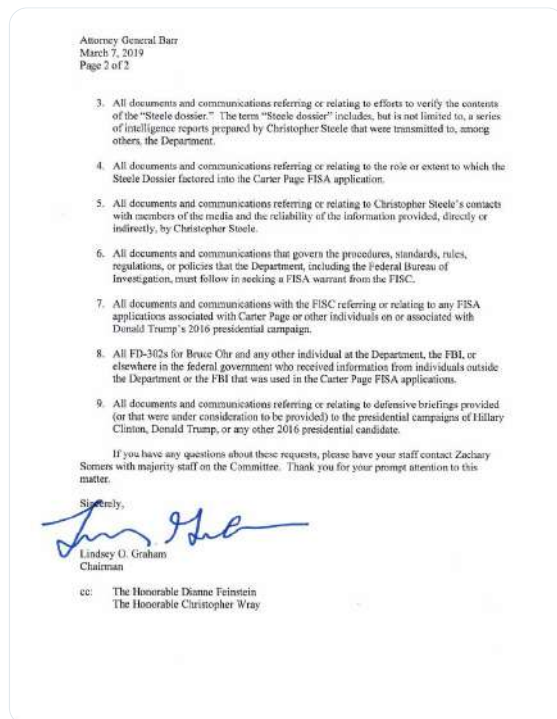
55) Graham activated.



<https://pbs.twimg.com/media/D1HQVQWVsAEfCPB.jpg>

56) POTUS and Q are helping Make India (and the world) Great Again.

[#MIGA](#)



<https://pbs.twimg.com/media/D1HNnG-VAAAFIj5.jpg>

► Q [!!mG7VJxZNCI](#) 03/07/19 (Thu) 21:28:54 ID: 285835 (3)



We stand
TOGETHER in this
FIGHT.
WWG1WGA!!!
Q

<https://pbs.twimg.com/media/D1HSZmcUcAE051C.jpg>

57) Q posted a link to a Bing search about Facebook and said parts 3-9 are coming soon.

► Q [!!mG7VJxZNCI](#) 03/07/19 (Thu) 21:45:10 ID: d6e0f4 (1)
No.5569577 >>[5569588](#) >>[5569591](#) >>[5569592](#) >>[5569593](#) >>[5569595](#)

[http://www.bing.com/news/search?
q=facebook&qft=interval%3d%227%22
&form=PTFTNR](http://www.bing.com/news/search?q=facebook&qft=interval%3d%227%22&form=PTFTNR)

[Parts 3-9 coming soon]

Q

<https://pbs.twimg.com/media/D1HTbkFV4Al2dmN.png>

58) Nothing to see here.

<https://www.bing.com/news/search?q=facebook&qft=interval%3d%227%22&form=PTFTNR>



Mark Zuckerberg Wants Facebook to Emulate China's WeChat. Can It?

SAN FRANCISCO — As Mark Zuckerberg begins shifting Facebook to private messaging and away from public sharing and open conversations, the vision he has sketched out for the ...

[nytimes.com](#) | 5h



Facebook Vows To Quash Anti-Vaccine Misinformation

Facebook announced on Thursday it is taking steps to combat the spread of anti-vaccine information across the social media platform by reducing the distribution of misleading medi...

[NPR](#) | 4h



Facebook's shift to ephemeral messaging raises big questions for its advertising business and could trigger a

Mark Zuckerberg just announced in a blog post that Facebook would shift its focus from public posts to private ephemeral communication on its messaging apps. The 3,200-word post...

[Business Insider](#) | 3h



Facebook Announces Plan to Curb Vaccine Misinformation

Facebook announced Thursday its first policy to combat misinformation about vaccines, following in the footsteps of Pinterest and YouTube. The social network is adopting an ...

[nytimes.com](#) | 4h



Facebook looks to stem the spread of anti-vaccine misinformation

Facebook has a problem with more than just fake news. Add vaccine misinformation on the social network to the list. Revealed Thursday: The social network says it will reduce ...

[USA Today](#) | 9h



Facebook says it will take action against anti-vaccine content. Here's how it plans to do it.

In an effort to curb anti-vaccination conspiracy theories and misinformation, Facebook announced Thursday it will no longer recommend the offending pages and groups, and will ...

[The Washington Post](#) | 4h



Facebook Messenger had a vulnerability that could let hackers see who you contact

A previously reported Facebook vulnerability was similarly found in the company's Messenger product, according to security research group Imperva. Nearly a year ago, Imperva...

[The Verge](#) | 10h



Facebook will downrank anti-vax content on News Feed and hide it on Instagram

After indicating that it was exploring its options for fighting the potentially deadly rise of anti-vaccination content on its platform last month, Facebook is making a plan of attack. Facebo...

[TechCrunch](#) | 9h



Facebook announces plans to block anti-vaccination content

Facebook is cracking down on the spread of vaccine misinformation, the company announced Thursday. The changes come as tech giants are facing criticism for their role in discriminat...

[CBS News](#) | 5h



Facebook says it will dramatically improve privacy. But it hasn't fully delivered on past promises.

Mark Zuckerberg insisted this week that he's serious about privacy — so much so that he's planning to transform Facebook into a more refined social experience. But the social networ...

[The Washington Post](#) | 5h



A Patched Bug Left Facebook Messenger Conversations Exposed to Hackers, Researcher Says

A Facebook bug allowed hackers to target a person through their web browser, and find out exactly who they were conversing with on Facebook Messenger, according to a blog post...

[Fortune](#) | 5h



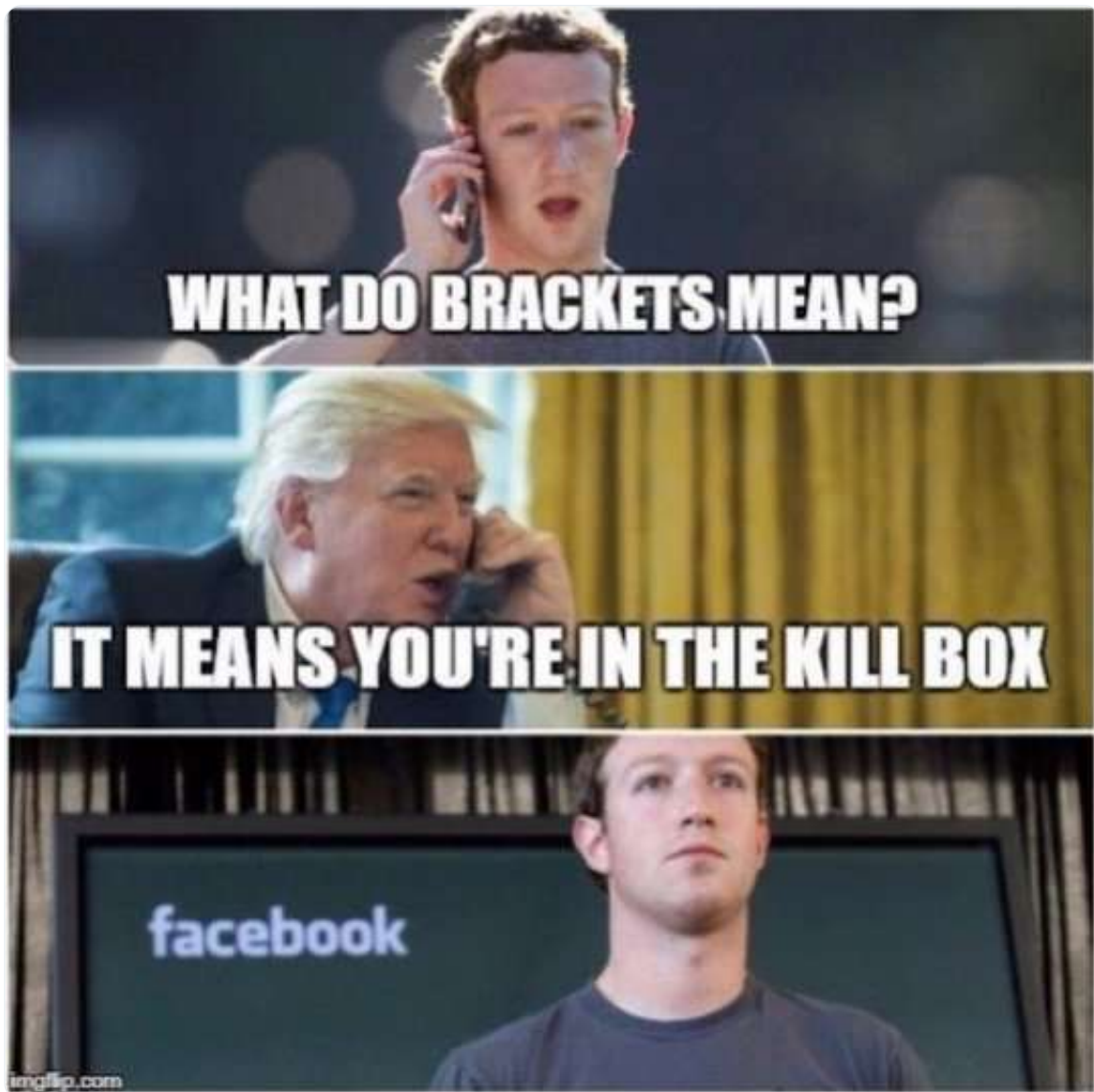
Facebook and Instagram will hide pages that spread 'vaccine misinformation'

I'd like to think that everyone who reads TMW knows that vaccines work. That they don't cause autism, as demonstrated time and time again. That autism doesn't need the extra...

[thenextweb.com](#) | 6h

<https://pbs.twimg.com/media/D1HU7ukUYAMUuk0.jpg>

59) [MZ]



<https://pbs.twimg.com/media/D113PPNVYAAk0GZ.jpg>

60) An anon did a deep dig into Vault 7—the public release by Wikileaks of the CIA's spy tools. The following tweets will explain the anon's post and connect some dots from past posts by Q.

61) The anon begins by explaining his train of thought.

What does Snowden have to do with Facebook and the inability to turn off or delete a spying program installed on an electronic device?

Keking out right now. Pretty sure I found something. Rip me apart if I'm wrong though. So many shills on here. You're missing crumbs. Look here, not [here]. Responding to post 2996 Q says, "how is that possible for a 'supposed' non_gov entity?"

How is it possible that FB tracks data even when the app is deleted? In post 2993 (3/7/109) Q is calling out @Snowden. So I used the filter to find posts relating to WikiLeaks. Q's post from July 31, 2018 is a screenshot of the Wikileaks Vault 7... released MARCH 7. Sounds confusing just trying to show you my thought process, stay with me, it makes sense.

"Unlike bullets, bombs or missiles, most CIA malware is designed to live for days or even years after it has reached its 'target'. CIA malware does not "explode on impact" but rather permanently infests its target. In order to infect target's device, copies of the malware must be placed on the target's devices, giving physical possession of the malware to the target. To exfiltrate data back to the CIA or to await further instructions the malware must communicate with CIA Command & Control (C2) systems placed on internet connected servers. But such servers are typically not approved to hold classified information, so CIA command and control systems are also made unclassified." FROM VAULT 7

Links below that direct you to user forums on how to not leave a digital fingerprint that can be associated with the CIA, and how to construct an imitation fingerprint. Using Facebook as their 'fingerprint' they are able to install malware on peoples' phones, tablets, and computers which relay all data back to a central server using HIVE.

<https://pbs.twimg.com/media/D1l6qLdVYAAGcfK.png>

62) And why on March 7th did Q bringing this to our attention?

I'll use this article as a reference.



Wikileaks: CIA Hacking Tools Revealed - Daniel Solis Report

Source: WikiLeaks, Vault 7 Published: 7. 3. 2017 Contents • Press Release • Analysis • Examples • Frequently Asked Questions Press Release Today, Tuesday 7 March 2017, WikiLeaks begins its ...

► <https://danielsolis.cz/wikileaks-cia-hacking-tools-revealed/>

<https://danielsolis.cz/wikileaks-cia-hacking-tools-revealed/>

Press Release

Today, Tuesday 7 March 2017, WikiLeaks begins its new series of leaks on the U.S. Central Intelligence Agency. Code-named "Vault 7" by WikiLeaks, it is the largest ever publication of confidential documents on the agency.

The first full part of the series, "Year Zero", comprises 8,761 documents and files from an isolated, high-security network situated inside the CIA's **Center for Cyber Intelligence** in Langley, Virginia. It follows an introductory disclosure last month of **CIA targeting French political parties and candidates in the lead up to the 2012 presidential election**.

Recently, the CIA lost control of the majority of its hacking arsenal including malware, viruses, trojans, weaponized "zero day" exploits, malware remote control systems and associated documentation. This extraordinary collection, which amounts to more than several hundred million lines of code, gives its possessor the entire hacking capacity of the CIA. The archive appears to have been circulated among former U.S. government hackers and contractors in an unauthorized manner, one of whom has provided WikiLeaks with portions of the archive.

<https://pbs.twimg.com/media/D1l8PI-VYAAbXn.png>

63) Anon did a search of Wikileaks posts and found one from last July about the release of Wikileaks Vault 7—which explains how the CI_A's spying tools have fallen into the hands of bad actors.

Vault 7 was released exactly one year earlier on March 7, 2018.

► **Anonymous** 07/30/18 (Mon) 22:13:20 ID: 987024 (6) No.2367152 >>2367162 >>2367164
>>2367210 >>2367363 >>2367415 >>2367604 >>2367750
File (hide): 741fca4ddb87e96...png (59.4 KB, 279x512, 279:512, 2018-07-31_1-12-08.png) (h) (u)



Vault 7: CIA Hacking Tools Revealed

A series of leaks on the U.S. Central Intelligence Agency Code-named "Vault 7" by WikiLeaks, it is the largest ever publication of confidential documents on the agency.

7 March 2017

>>2366811

► Q !CbboFOtcZs 07/30/18 (Mon) 22:14:44
ID: 6632ee (1) No.2367164 >>2367173 >>2367175

>>2367152

Track last.
JA offline cause.
Q

<https://pbs.twimg.com/media/D11-xNUVsAlwWMn.jpg>

64) Q calls out Snowden and asks why he didn't release the CI_A spy tools.

► Q !ImG7VJxZNCI 03/06/19 (Wed) 22:23:50 ID: 4e2679 (3) No.5551229 >>5551245 >>5551248 >>5551250 >>5551257
<https://www.iqt.org/our-history/>

Why did @Snowden only engage and attack the NSA?
If @Snowden really cared about privacy/citizenship awareness, why didn't he expose the C_A's main programs?
@Snowden was priv to DARPA, IQT, and NSA SURV / COV programs.
Why did @Snowden only focus on NSA?
Where did @Snowden work prior to NSA?

ASK YOURSELF A VERY SIMPLE QUESTION, WOULD YOU RELEASE (GO LIVE) TO THE PUBLIC
ACROSS THE MEDIA ALL HIGHLY CLASSIFIED MATERIAL (NSA) PRIOR TO.....GETTING
TO YOUR END DESTINATION?
OR, WOULD YOU LOGICALLY TRAVEL TO YOUR END DESTINATION, THEN RELEASE PUBLICLY?
WAS RUSSIA THE PLANNED LOCATION?
WHY RUSSIA?
WHY DID CHINA (HKG) LET HIM OUT OF THE COUNTRY?
WAS THERE A 'RED' SECURITY ALERT PUT OUT TO PREVENT PASSPORT TRAVEL ACROSS ALL
NATIONS?
WHY DID CHINA GRANT ACCESS TO TRAVEL W/ THE BLOCK IN PLACE?
WHY RUSSIA?
RUSSIA RUSSIA RUSSIA
Q

<https://pbs.twimg.com/media/D1l8mBqVAAAQ3l8.png>

65) Q asks: Why is there no way to turn off or delete spying malware installed on electronic devices if the software was (supposedly) developed by a non-government entity?

► Q [!!mG7VJxZNCI](#) 03/07/19 (Thu) 00:07:05 ID: 1e3478 (2)
No.5553154 >>5553158 >>5553168 >>5553171 >>5553173 >>5553174

>>5552800

Other articles prior to posts.

Privacy push to cover for past/future 'exposure' issue re:
data release non_marketing.

There is no privacy.

There is no way to turn off (even through app deletion) their
ability to extract info.

How is that possible for a 'supposed' non_gov entity?

Phone co's involved?

Phone_wipe resolve?

Q

<https://pbs.twimg.com/media/D1l8rS1U8AI-eX4.png>

66) The first part of the Vault 7 article explains the nature of the problem:

The CI_A created a massive hacking & malware division that lacks necessary oversight and is on questionable legal grounds. Once created, spying malware is quickly pirated and sold to bad actors.

CIA loses control of its global spy tool arsenal	➡	Recently, the CIA lost control of the majority of its hacking arsenal including malware, viruses, trojans, weaponized "zero day" exploits, malware remote control systems and associated documentation. This extraordinary collection, which amounts to more than several hundred million lines of code, gives its possessor the entire hacking capacity of the CIA. The archive appears to have been circulated among former U.S. government hackers and contractors in an unauthorized manner, one of whom has provided WikiLeaks with portions of the archive.
"Year Zero" is a report covering the scope of the CIA's malware & hacking capabilities	➡	"Year Zero" introduces the scope and direction of the CIA's global covert hacking program, its malware arsenal and dozens of "zero day" weaponized exploits against a wide range of U.S. and European company products, include Apple's iPhone, Google's Android and Microsoft's Windows and even Samsung TVs, which are turned into covert microphones.
The CIA competes with NSA for preeminence & budget	➡	Since 2001 the CIA has gained political and budgetary preeminence over the U.S. National Security Agency (NSA). The CIA found itself building not just its now infamous drone fleet, but a very different type of covert, globe-spanning force — its own substantial fleet of hackers. The agency's hacking division freed it from having to disclose its often controversial operations to the NSA (its primary bureaucratic rival) in order to draw on the NSA's hacking capacities.
CIA creates a massive malware & hacking division without congressional oversight	➡	By the end of 2016, the CIA's hacking division, which formally falls under the agency's Center for Cyber Intelligence (CCI) , had over 5000 registered users and had produced more than a thousand hacking systems, trojans, viruses, and other "weaponized" malware. Such is the scale of the CIA's undertaking that by 2016, its hackers had utilized more code than that used to run Facebook. The CIA had created, in effect, its "own NSA" with even less accountability and without publicly answering the question as to whether such a massive budgetary spend on duplicating the capacities of a rival agency could be justified.
Does the CIA have legal authority to do what it is currently doing?	➡	In a statement to WikiLeaks the source details policy questions that they say urgently need to be debated in public, including whether the CIA's hacking capabilities exceed its mandated powers and the problem of public oversight of the agency. The source wishes to initiate a public debate about the security, creation, use, proliferation and democratic control of cyberweapons.

<https://pbs.twimg.com/media/D1JEJ1zV4AACJyq.jpg>

67) CI_A has malware that fakes out users.

We believe the TV is off but it's recording conversations and sending them to a server.

Is that how Facebook's app continues to send geolocation and record conversations even after it's been uninstalled and the phone wiped clean?

CIA malware & hacking tools are developed by the Engineering and Development group.



"Weeping angel" infiltrates Samsung TVs and has a "fake off" mode feature that records voice while a user thinks the device is inactive. Recordings are sent to a CIA server.



As of October of 2014, the CIA was looking into infecting vehicle control systems.



The CIA's MDB develops malware for smart phones to record from microphones & cameras and to collect audio and text comms.



CIA malware targets iPhone, Android, smart TVs

CIA malware and hacking tools are built by EDG (Engineering Development Group), a software development group within CCI (Center for Cyber Intelligence), a department belonging to the CIA's DDI (Directorate for Digital Innovation). The DDI is one of the five major directorates of the CIA (see this [organizational chart](#) of the CIA for more details).

The EDG is responsible for the development, testing and operational support of all backdoors, exploits, malicious payloads, trojans, viruses and any other kind of malware used by the CIA in its covert operations world-wide.

The increasing sophistication of surveillance techniques has drawn comparisons with George Orwell's 1984, but "Weeping Angel", developed by the CIA's **Embedded Devices Branch (EDB)**, which infests smart TVs, transforming them into covert microphones, is surely its most emblematic realization.

The attack against **Samsung smart TVs** was developed in cooperation with the United Kingdom's **MIS/BTSS**. After infestation, Weeping Angel places the target TV in a "Fake-Off" mode, so that the owner falsely believes the TV is off when it is on. In "Fake-Off" mode the TV operates as a bug, recording conversations in the room and sending them over the Internet to a covert CIA server.

As of October 2014 the CIA was also looking at **infecting the vehicle control systems used by modern cars and trucks**. The purpose of such control is not specified, but it would permit the CIA to engage in nearly undetectable assassinations.

The CIA's Mobile Devices Branch (MDB) developed **numerous attacks to remotely hack and control popular smart phones**. Infected phones can be instructed to send the CIA the user's geolocation, audio and text communications as well as covertly activate the phone's camera and microphone.

Despite iPhone's minority share (14.5%) of the global smart phone market in 2016, a specialized unit in the CIA's Mobile Development Branch produces malware to infest, control and exfiltrate data from **iPhones and other Apple products running iOS, such as iPads**. CIA's arsenal includes **numerous local and remote "zero days"** developed by CIA or obtained from GCHQ, NSA, FBI or purchased from cyber arms contractors such as Baitshop. The disproportionate focus on iOS may be explained by the popularity of the iPhone among social, political, diplomatic and business elites.

<https://pbs.twimg.com/media/D1JHaGdVYAIQbv.jpg>

68) The CI_A can infiltrate any operating system, device or network. They don't report vulnerabilities but exploit them and in doing so, they allow bad actors to exploit them as well.

CIA malware bypasses encrypted messaging services



The CIA has developed a wide array of hacking tools to infiltrate all devices, operating systems and isolated networks.



The CIA is required to report vulnerabilities to software companies for security reasons but they don't. They allow themselves access and in doing so, they allow bad actors the same access.



These techniques permit the CIA to bypass the encryption of WhatsApp, Signal, Telegram, Wiebo, Confide and Cloackman by hacking the "smart" phones that they run on and collecting audio and message traffic before encryption is applied.

CIA malware targets Windows, OSx, Linux, routers

The CIA also runs a very substantial effort to infect and control **Microsoft Windows users** with its malware. This includes multiple local and remote weaponized "zero days", air gap jumping viruses such as "Hammer Drill" which infects software distributed on CD/DVDs, **infectors for removable media such as USBs**, systems to **hide data in images** or in covert disk areas ("Brutal Kangaroo") and to **keep its malware infestations going**.

Many of these infection efforts are pulled together by the CIA's **Automated Implant Branch (AIB)**, which has developed several attack systems for automated infestation and control of CIA malware, such as "Assassin" and "Medusa".

Attacks against Internet infrastructure and webservers are developed by the CIA's **Network Devices Branch (NDB)**.

The CIA has developed automated multi-platform malware attack and control systems covering Windows, Mac OS X, Solaris, Linux and more, such as EDB's "HIVE" and the related "Cutthroat" and "Swindle" tools, which are **described in the examples section below**.

CIA 'hoarded' vulnerabilities ("zero days")

In the wake of Edward Snowden's leaks about the NSA, the U.S. technology industry secured a commitment from the Obama administration that the executive would disclose on an ongoing basis — rather than hoard — serious vulnerabilities, exploits, bugs or "zero days" to Apple, Google, Microsoft, and other US-based manufacturers.

Serious vulnerabilities not disclosed to the manufacturers places huge swathes of the population and critical infrastructure at risk to foreign intelligence or cyber criminals who independently discover or hear rumors of the vulnerability. If the CIA can discover such vulnerabilities so can others.

<https://pbs.twimg.com/media/D1JK-jyUcAAWecE.jpg>

69) Last year, Q reported that the President's Twitter account was hacked by the CI_A.

This report confirms that it can (and has) been done.

"Year Zero" documents show that the CIA breached the Obama administration's commitments. Many of the vulnerabilities used in the CIA's cyber arsenal are pervasive and some may already have been found by rival intelligence agencies or cyber criminals.

As an example, specific CIA malware revealed in "Year Zero" is able to penetrate, infest and control both the Android phone and iPhone software that runs or has run presidential Twitter accounts. The CIA attacks this software by using undisclosed security vulnerabilities ("zero days") possessed by the CIA but if the CIA can hack these phones then so can everyone else who has obtained or discovered the vulnerability. As long as the CIA keeps these vulnerabilities concealed from Apple and Google (who make the phones) they will not be fixed, and the phones will remain hackable.

<https://pbs.twimg.com/media/D1JOrRrVsAAAZiU.png>

70) Q's report on the CI_A hacking POTUS Twitter account.



Anonymous ID:WBXFvlgI Thu 02 Nov 2017 17:07:18

Flash Traffic:

Three letter agency embedded tracking/up-channel into POTUS' Twitter to specifically target through specialized geo and send his location.

We anticipated this (see post a few hours ago).

It has begun.

Perhaps more posts to follow as expected imminent departure.

Q



Anonymous ID:VXi4Bx/o Thu 02 Nov 2017 17:11:43

No.147688276

Quoted By: >>147688399 >>147689362

>>147687684

Let's be clear - you're telling us POTUS is currently under attack by our own intelligence agencies?



Anonymous ID:WBXFvlgI Thu 02 Nov 2017 17:19:28

No.147689362

Quoted By: >>147689878 >>147689883 >>147690249 >>147690258

>>147688276

Let's be real clear.

The CIA just attacked the Command and Chief which was immediately detected by NSA/MI and alerted to POTUS.

Re-review all my crumbs including today/yesterday/weekend.

What does this mean?

What actions are immediately occurring?

If this leaks, or the immediate action ongoing at Langley, you'll have your verification ahead of schedule.

Q

<https://pbs.twimg.com/media/D1JOzxLUcAAC9Uz.png>

71) Because classifying its spy tools would expose operators to the risk of prosecution, the CI_A opted to leave its malware unclassified making it easy to steal and resell.

Because classifying its spy tools would expose operators to risk of prosecution, the CIA's surveillance malware is not classified or patented making these programs easy to pirate.



How the CIA dramatically increased proliferation risks

In what is surely one of the most astounding intelligence own goals in living memory, the CIA structured its classification regime such that for the most market valuable part of "Vault 7" — the CIA's weaponized malware (implants + zero days), Listening Posts (LP), and Command and Control (C2) systems — the agency has little legal recourse.

The CIA made these systems unclassified.

Why the CIA chose to make its cyberarsenal unclassified reveals how concepts developed for military use do not easily crossover to the 'battlefield' of cyber 'war'.

To attack its targets, the CIA usually requires that its implants communicate with their control programs over the Internet. If CIA implants, Command & Control and Listening Post software were classified, then CIA officers could be prosecuted or dismissed for violating rules that prohibit placing classified information onto the Internet. Consequently the CIA has secretly made most of its cyber spying/war code unclassified. The U.S. government is not able to assert copyright either, due to restrictions in the U.S. Constitution. This means that cyber 'arms' manufacturers and computer hackers can freely "pirate" these 'weapons' if they are obtained. The CIA has primarily had to rely on obfuscation to protect its malware secrets.

<https://pbs.twimg.com/media/D1JSQPcV4AARxp7.jpg>

72) The anon's post picks up here at the mention of "fires".

Intelligence agencies today will use the word 'fire' when injecting or implanting a program to mimic the military's jargon for a weapon being fired.

Conventional weapons such as missiles may be fired at the enemy (i.e into an unsecured area). Proximity to or impact with the target detonates the ordnance including its classified parts. Hence military personnel do not violate classification rules by firing ordnance with classified parts. Ordnance will likely explode. If it does not, that is not the operator's intent.

Over the last decade U.S. hacking operations have been increasingly dressed up in military jargon to tap into Department of Defense funding streams. For instance, attempted "malware injections" (commercial jargon) or "implant drops" (NSA jargon) are being called "fires" as if a weapon was being fired. However the analogy is questionable.

Unlike bullets, bombs or missiles, most CIA malware is designed to live for days or even years after it has reached its 'target'. CIA malware does not "explode on impact" but rather permanently infests its target. In order to infect target's device, copies of the malware must be placed on the target's devices, giving physical possession of the malware to the target. To exfiltrate data back to the CIA or to await further instructions the malware must communicate with CIA Command & Control (C2) systems placed on internet connected servers. But such servers are typically not approved to hold classified information, so CIA command and control systems are also made unclassified.

A successful 'attack' on a target's computer system is more like a series of complex stock maneuvers in a hostile take-over bid or the careful planting of rumors in order to gain control over an organization's leadership rather than the firing of a weapons system. If there is a military analogy to be made, the infestation of a target is perhaps akin to the execution of a whole series of military maneuvers against the target's territory including observation, infiltration, occupation and exploitation.

<https://pbs.twimg.com/media/D1JTBMLUcAEmgBy.png>

73) A malware program once implanted usually waits for instructions from command and control (C2) Because the CI_A's programs are not classified, the command and control systems are also unclassified.

Conventional weapons such as missiles may be fired at the enemy (i.e into an unsecured area). Proximity to or impact with the target detonates the ordnance including its classified parts. Hence military personnel do not violate classification rules by firing ordnance with classified parts. Ordnance will likely explode. If it does not, that is not the operator's intent.

Over the last decade U.S. hacking operations have been increasingly dressed up in military jargon to tap into Department of Defense funding streams. For instance, attempted "malware injections" (commercial jargon) or "implant drops" (NSA jargon) are being called "fires" as if a weapon was being fired. However the analogy is questionable.

Unlike bullets, bombs or missiles, most CIA malware is designed to live for days or even years after it has reached its 'target'. CIA malware does not "explode on impact" but rather permanently infests its target. In order to infect target's device, copies of the malware must be placed on the target's devices, giving physical possession of the malware to the target. To exfiltrate data back to the CIA or to await further instructions the malware must communicate with CIA Command & Control (C2) systems placed on internet connected servers. But such servers are typically not approved to hold classified information, so CIA command and control systems are also made unclassified.

A successful 'attack' on a target's computer system is more like a series of complex stock maneuvers in a hostile take-over bid or the careful planting of rumors in order to gain control over an organization's leadership rather than the firing of a weapons system. If there is a military analogy to be made, the infestation of a target is perhaps akin to the execution of a whole series of military maneuvers against the target's territory including observation, infiltration, occupation and exploitation.

<https://pbs.twimg.com/media/D1JT654U0AEPVeT.png>

74) CI_A operators avoid detection and implicate foreign actors or other entities by leaving behind false digital fingerprints.

Evading forensics and anti-virus

A series of standards lay out CIA malware infestation patterns which are likely to assist forensic crime scene investigators as well as Apple, Microsoft, Google, Samsung, Nokia, Blackberry, Siemens and anti-virus companies attribute and defend against attacks.

"Tradecraft DO's and DON'Ts" contains CIA rules on how its malware should be written to avoid fingerprints implicating the "CIA, US government, or its witting partner companies" in "forensic review". Similar secret standards cover the **use of encryption to hide CIA hacker and malware communication** (pdf), **describing targets & exfiltrated data** (pdf) as well as **executing payloads** (pdf) and **persisting** (pdf) in the target's machines over time.

CIA hackers developed successful attacks against most well known anti-virus programs. These are documented in **AV defeats**, **Personal Security Products**, **Detecting and defeating PSPs** and **PSP/Debugger/RE Avoidance**. For example, Comodo was defeated by **CIA malware placing itself in the Window's "Recycle Bin"**. While Comodo 6.x has a **"Gaping Hole of DOOM"**.

CIA hackers discussed what the NSA's "Equation Group" hackers did wrong and **how the CIA's malware makers could avoid similar exposure**.

<https://pbs.twimg.com/media/D1JWAsYUwAERGqN.png>

75) The anon noted that in some cases, CI_A chooses to leave digital fingerprints behind implicating Facebook. through programs like UMBRAGE, Fine Dining, Improvise and HIVE.

UMBAGE

The CIA's hand crafted hacking techniques pose a problem for the agency. Each technique it has created forms a "fingerprint" that can be used by forensic investigators to attribute multiple different attacks to the same entity.

This is analogous to finding the same distinctive knife wound on multiple separate murder victims. The unique wounding style creates suspicion that a single murderer is responsible. As soon one murder in the set is solved then the other murders also find likely attribution.

The CIA's **Remote Devices Branch's UMBAGE group** collects and maintains a **substantial library** of attack techniques 'stolen' from malware produced in other states including the Russian Federation.

With UMBAGE and related projects the CIA cannot only increase its total number of attack types but also misdirect attribution by leaving behind the "fingerprints" of the groups that the attack techniques were stolen from.

UMBAGE components cover keyloggers, password collection, webcam capture, data destruction, persistence, privilege escalation, stealth, anti-virus (PSP) avoidance and survey techniques.

Fine Dining

Fine Dining comes with a standardized questionnaire i.e menu that CIA case officers fill out. The questionnaire is used by the agency's OSB (**Operational Support Branch**) to transform the requests of case officers into technical requirements for hacking attacks (typically "exfiltrating" information from computer systems) for specific operations. The questionnaire allows the OSB to identify how to adapt existing tools for the operation, and communicate this to CIA malware configuration staff. The OSB functions as the interface between CIA operational staff and the relevant technical support staff.

Among the list of possible targets of the collection are 'Asset', 'Liason Asset', 'System Administrator', 'Foreign Information Operations', 'Foreign Intelligence Agencies' and 'Foreign Government Entities'. Notably absent is any reference to extremists or transnational criminals. The 'Case Officer' is also asked to specify the environment of the target like the type of computer, operating system used, Internet connectivity and installed anti-virus utilities (PSPs) as well as a list of file types to be exfiltrated like Office documents, audio, video, images or custom file types. The 'menu' also asks for information if recurring access to the target is possible and how long unobserved access to the computer can be maintained. This information is used by the CIA's 'JQIMPROVISE' software (see below) to configure a set of CIA malware suited to the specific needs of an operation.

Improvise (JQIMPROVISE)

'Improvise' is a toolset for configuration, post-processing, payload setup and execution vector selection for survey/exfiltration tools supporting all major operating systems like Windows (Bartender), MacOS (JukeBox) and Linux (DanceFloor). Its configuration utilities like Margarita allows the NOC (Network Operation Center) to customize tools based on requirements from 'Fine Dining' questionnaires.

HIVE

HIVE is a multi-platform CIA malware suite and its associated control software. The project provides customizable implants for Windows, Solaris, MikroTik (used in internet routers) and Linux platforms and a Listening Post (LP)/Command and Control (C2) infrastructure to communicate with these implants.

<https://pbs.twimg.com/media/D1JXUmRUwAAja2Z.png>

76) The anon noticed a lot of use of words like "bombs" and "packets of data."

► **keystone i found the keystone** **Anonymous** 03/07/19 (Thu) 17:31:08 ID: 9a6a8f (2) No.5565314 **Part 2**

I suggest all anons who have given up life to research this shit like me should read this document to completion.

I noticed the enormous amount of comparisons between "packets of data" and "bombs", dunno why probably just autistic. I looked back in the Qmap and on March 5, 2019 an anon posted how London Police "called them bombs not suspicious packages" Q responds in 2974 with "Fire".

I went into Vault 7 Projects, search for "fire"...

"Angelfire is an implant comprised of five components: Solartime, Wolfcreek, Keystone (previously MagicWand), BadMFS, and the Windows Transitory File system"

FUCKING KEYSTONE KEK

"Keystone is part of the Wolfcreek implant and responsible for starting malicious user applications. Loaded implants never touch the file system, so there is very little forensic evidence that the process was ever ran." This makes post Q 381 much easier to understand

"We Won't telegraph our moves to the ENEMY."

We will however light a FIRE to flush them out."

Q

Q is saying that they are using the Angelfire to predict the Deep State's moves without being detected. In the user files it says a key must be used to open magicwand (keystone). In Q post 270 he says that ADM R/NSA (W&W) + POTUS/USMIL = Apply the Keystone. Paint the Picture. In post 167 Q says POTUS opened the door of all doors. Expand your thinking. What is the keystone? Now this could be confirmation bias but based off of what we just read we can now infer that Q was saying trump gave Admiral Rogers permission to use Keystone and Activate malware in order to collect data on DS. Furthermore who uses a magicwand? A wizard. (W&W)

<https://pbs.twimg.com/media/D1JXvCiU8AQ585Z.png>

77) The anon remembered a recent drop with the terms "bombs" and "suspicious packages."

► **Anonymous** 03/05/19 (Tue) 14:37:07
ID: c45779 (6) No.5523830 >>5523860 >>5524217
>>5524235 >>5524258

>>5523765

Pointed this out earlier today. They specifically called them "bombs", not "suspicious packages", as per the norm.

<https://pbs.twimg.com/media/D1JZN23V4AAqTev.png>

78) This was Q's response.

► **Q** (!mG7VJxZNCI) 03/05/19 (Tue) 14:38:17
ID: 27704f (4) No.5523860 >>5523869 >>5523874

>>5523830

"Fire."

Q

<https://pbs.twimg.com/media/D1JZTiHVSAEZEEna.png>

79) The anon dug into the Vault 7 looking for the word "Fire" and came up with the "Angelfire" malware which is comprised of 5 other components one of which is named "Keystone."

I suggest all anons who have given up life to research this shit like me should read this document to completion.

I noticed the enormous amount of comparisons between “packets of data” and “bombs”, dunno why probably just autistic. I looked back in the Qmap and on March 5, 2019 an anon posted how London Police “called them bombs not suspicious packages” Q responds in 2974 with “Fire”.

I went into Vault 7 Projects, search for “fire”....
“Angelfire is an implant comprised of five components: Solartime, Wolfcreek, **Keystone** (previously MagicWand), BadMFS, and the Windows Transitory File system”

FUCKING KEYSTONE KEK

“Keystone is part of the Wolfcreek implant and responsible for starting malicious user applications. Loaded implants never touch the file system, so there is very little forensic evidence that the process was ever ran.” This makes post Q 381 much easier to understand

“We Won’t telegraph our moves to the ENEMY.
We will however light a FIRE to flush them out.”
Q

<https://pbs.twimg.com/media/D1JamkUVsAAhDDG.png>

80) Keystone allows the Angelfire malware program to operate without being detected.



WikiLeaks Vault 7: CIA's stealthy Angelfire Windows malware

Angelfire is the twenty second malware WikiLeaks has revealed since March.

<https://www.cso.com.au/article/626753/wikileaks-vault-7-cia-stealthy-angelfire-windows-malware/>

<https://www.cso.com.au/article/626753/wikileaks-vault-7-cia-stealthy-angelfire-windows-malware/>

WikiLeaks' latest Vault7 release details a multi-module piece of malware designed to spy on Windows XP and Windows 7 machines.

Dubbed Angelfire, the malware is comprised of five components, including Solartime, Wolfcreek, **Keystone**, BadMFS, and the Windows Transitory File system.

According to the Angelfire user guide, Solartime modifies the partition boot sector to load the CIA's kernel code which tweaks the Windows boot process so that CIA implant device drivers can load at the same time legitimate device drivers are loaded.

Wolfcreek is the kernel code that Solartime executes and is responsible for loading other Angelfire drivers and applications.

The Keystone component launches other Angelfire applications and is designed to leave minimal forensic evidence since Keystone implant code are loaded directly into memory and never touch the file system. The intent here was to ensure that processes created by Angelfire applications don't look out of the ordinary.

"Currently all processes will be created as svchost. When viewed in task manager (or another process viewing tool) all properties of the process will be consistent with a real instance of svchost.exe including image path and parent process," the user guide states.

<https://pbs.twimg.com/media/D1JcEPqVYAA4JBg.png>

81) The anon then makes a connection to another post from Q.

► Q !UW.yye1fxo 12/19/17 (Tue) 16:00:02
ID: 03c2f4 (13) No.127154 >>127158 >>127163

We won't telegraph our moves to
the ENEMY.

We will however light a FIRE to
flush them out.

Q

<https://pbs.twimg.com/media/D1JcYQAVsAAMY7t.png>

82) The anon begins to tie it all together making the assertion that POTUS and the Q team are using the CI_A's own Angelfire malware to track them and predict their moves without their knowledge.

Q is saying that they are using the Anglefire to predict the Deep State's moves without being detected. In the user files it says a key must be used to open magicwand (keystone). In Q post 270 he says that ADM R/NSA (W&W) + POTUS/USMIL = Apply the Keystone. Paint the Picture. In post 167 Q says POTUS opened the door of all doors. Expand your thinking. What is the keystone? Now this could be confirmation bias but based off of what we just read we can now infer that Q was saying trump gave Admiral Rogers permission to use Keystone and Activate malware in order to collect data on DS. Furthermore who uses a magicwand? A wizard. (W&W)

<https://pbs.twimg.com/media/D1Jc4fRUwAAuxtQ.png>

83) The anon takes us back to this post where Q said Admiral Rogers, the NSA (Wizards & Warlocks), POTUS and the military are all working together to apply the keystone.

► Q !ITPb.qbhqo 12/05/17 (Tue) 14:06:17 ID: 7cfe10
(8) No.38507 >>38518 >>38525 >>38531 >>38532 >>38609

Adm R/ No Such Agency (W&W) +
POTUS/USMIL =
Apply the Keystone.
Paint the picture.
Q

<https://pbs.twimg.com/media/D1Jdsi-VYAEGgmX.png>

84) Who are the Wizards and Warlocks?
The Guardians of intelligence.

Q !ITPb.qbhqo ID:/jAm9Qi+ Sun 12 Nov 2017 12:52:34 No.149140639  Report

Patriots don't sleep.
40,000ft. v. necessary to understand [US]/SA/global events.
Paint the picture.

What is No Such Agency - Q group?

Who has clearance to full picture?
Important.

+++Adm R+++

What agency is at war w/ Clowns In America?
Who does [i]t hurt?
Who control[s] the MSM?

Why was Sarah A. C. attacked (hack-attempt)?
Why was Op[e]ration Mockingbird repeated?
Why was Jason Bourne (CIA/Dream) repeated?
Think social media platforms.
Who are the Wizards & Warloc[k]s?

What council do the Wizards & Warlocks control?

Think Snowden (inside terms dropped).

Q

<https://pbs.twimg.com/media/D1JeR67UYAEjp1M.png>

85) The anon highlighted this post where Q said POTUS opened the door of all doors.



Q !ITPb.qbhqo ID:Qwfs7lfI Mon 20 Nov 2017
11:12:14 No.150214731 

POTUS opened the door of all doors.
Expand your thinking.
What is the keystone?

Q

<https://pbs.twimg.com/media/D1JeWngU8AEi8qG.png>

86) The anon wrote:

We can now infer that Q was saying trump gave Admiral Rogers permission to use Keystone and Activate malware in order to collect data on DS. Furthermore, who uses a magic wand? A wizard. (W&W)

87) Without confirming his theory, Q commended the anon for his work and encouraged him to keep digging.

► Q **!!mG7VJxZNCI** 03/07/19 (Thu) 20:59:58

ID: f9e971 (2) No.5568629 >>5568637 >>5568641

>>5565314 (/pb)

Something you should explore
further.

Impressive, most impressive.

Q

<https://pbs.twimg.com/media/D1JgJkfVAAAZj-5.png>